THOMSON
MEDSTAT

Implementation Planning Study for the Integration of Medical Event Reporting Input and Data Structure for Reporting to AHRQ, CDC, CMS, and FDA

Final Report

Volume 1 – Technical Report

Contract No. 290-96-0010

Task Order 5

Submitted to:

James Battles, Ph.D.
Center for Quality Improvement and Patient Safety
Agency for Healthcare Research and Quality
6011 Executive Blvd., Suite 200
Rockville, Maryland 20852

Submitted by:

The MEDSTAT Group, Inc.
5425 Hollister Avenue, Suite 140
Santa Barbara, CA 93111

June 11, 2002

Table of Contents

Executive Summary

Patient safety is one of the most significant issues facing healthcare today, and touches on all aspects of care. Although efforts to measure and reduce the risk of harm to patients are underway, there is no national, centralized system for the collection and analysis of information pertaining to adverse events. Rather, an array of disparate systems collect information about different types of events (e.g., device-related, medication-related), from different sources (e.g., consumers, practitioners, manufacturers). Individually, each of these systems provides value to those who submit information and those who analyze the collected data. However, linking data or combining database offers efficiencies for the collection of data and could allow for detection of safety problems that would otherwise be impossible to detect. This report analyzes existing USDHHS data systems, select other systems, and factors affecting the potential integration of systems.

Our investigation suggests that there are several possible integration options, and details two specific candidates. Both approaches lend themselves to a phased approach, with the chief integration efforts occurring early in Phase 1 and expanding to other domains or user communities. One approach initially addresses the issue of "burden of reporting" for several systems, and subsequently develops rich analytic facilities. Another approach begins by integrating two systems "end-to-end," including data entry and analysis components.

Acknowledgements[1]

The MEDSTAT project team wants to thank the following people and agencies for their help and support during this project. First, the members of the Patient Safety Task Force provided support and guidance for this project at every step. They opened the way for our teams to easily and quickly gain access to the appropriate people so that we could gather the necessary information for our study. Second, the staff at each of the agencies was open and helpful at every turn. They provided requested information and answered our myriad of questions as we learned and digested the working of their agencies systems. Both the PSTF and the agencies will continue to be intimately involved in this project at it moves forward. We hope that our work has laid a strong foundation that will make their efforts easier. Third, we would like to thank the members of our External Advisory Panel. They provided valuable insights and represented their constituencies admirably, ensuring that these interests were considered and included in the options that we recommend in this plan. Additionally, we would like to thank W. Ed Hammond, Bryan Liang, and Susan Greene Merewitz for their insightful comments on previous versions of this report. Finally we wish to thank the staff at AHRQ, specifically James Battles our Project Officer. Jim's knowledge of the work of medical errors and patient safety coupled with his resolve for the goals of this vision made our project rewarding and fun. The only sad part of this project was that John Eisenberg, the Director of AHRQ, did not live to see it completed. He was there at the beginning, had high hopes for our success and wished us well. We hope that we have lived up to his expectations.

The MEDSTAT Project Team

[1] A list of the members of the External Advisory Panel are in Appendix C.

1 Introduction

1.1 Extent of Medical Errors

In 1999, the Institute of Medicine released an alarming report, *To Err Is Human*, which estimated that between 44,000 and 98,000 people die each year from medical errors in hospitals in the United States (Kohn et al., 1999). The lower estimate places medical errors as the eighth leading cause of death in the U.S. The higher estimate places medical errors as the fifth cause of death.

These results shocked the American people. The President of the United States directed Federal agencies to devise a plan to reduce the number of medical errors. The IOM called for leadership from the U.S. Department of Health and Human Services (USDHHS) in reducing medical errors and identified one of its components, the Agency for Healthcare Research and Quality (AHRQ), as the Nation's lead organization for patient safety research. The USDHHS Secretary immediately organized the Quality Interagency Coordinating (QuIC) Task Force of 11 Federal agencies or offices involved in health care and appointed AHRQ to lead the QuIC. The QuIC described actions that its agencies would take to reduce medical errors (QuIC, 2000). One of those steps was the genesis of a four-agency coordination project to collect data in order to understand and stimulate a reduction in the risk of errors and adverse events in health care.

The wide range of the IOM estimates of death from errors reflected the impossibility of determining the extent to which medical error affects American society. There is no national reporting system, and systems mandated by State legislatures only collect rates of catastrophic events, such as deaths and life-threatening events from medical mismanagement. They record the tip of the iceberg – the most egregious errors – and under-reporting is an endemic problem.

Estimates of the size of the problem come from research. Three landmark studies, two American and one Australian, have estimated medical errors in relation to populations. All three studies, the Harvard Medical Practice Study (Brennan et al., 1991), the Colorado and Utah Hospital Discharge Study (Thomas et al., 2000), and the Quality in Australian Health Care Study (Wilson et al., 1995), found surprisingly high rates of medical error and error due to negligence. The Harvard study was the basis of the estimate of 98,000 U.S. patients that die from medical errors each year. The Colorado/Utah study was the basis of the 44,000 deaths.

The Harvard study examined medical injury and malpractice litigation from a sample of New York hospitals and thirty thousand medical records at those institutions. The study found that adverse events[2] occurred in 3.7 percent of hospitalizations and that 27.6 percent of those were due to negligence. Although 70.5 percent of the adverse events caused disabling injuries that lasted less than six months, 2.6 percent caused permanent disability and 13.6 percent led to death. The study conducted in Colorado and Utah found that adverse events, defined as "injury caused by medical management that resulted in either a prolonged hospital stay or disability at discharge", occurred in 2.9 percent of hospitalizations and that 6.6 percent of adverse events led to death (Thomas et al., 2000). Over half of adverse events could have been prevented according to the Colorado/Utah study. The Australian study, modeled after the Harvard study, found that 16.6 percent of hospital admissions involved adverse events with half of those considered preventable. Furthermore, a higher 13.7 percent of adverse events resulted in permanent disability, with 4.9 percent of adverse events resulting in death.

In addition to these studies, the Commonwealth Fund asked about medical errors in their 2001 Health Care Quality Survey, a telephone interview of 6,700 households (Davis et al., 2002). Twenty-two percent of respondents reported that they or a family member (who may live elsewhere) had experienced a medical error of some kind at some time. This was translated to 22.8 million Americans who have

[2] Defined as "an unintended injury that was caused by medical mismanagement and that resulted in measurable disability"

experienced a medical error at some time (or about 8 percent of the resident population). Eight million (or 3 percent of the population) judged that the error created a very serious problem. It is not possible to relate these “ever experienced” serious error estimates to the estimates of 44,000 to 98,000 deaths in hospitals from errors each year.

In addition to the mortality attributable to medical error, the IOM study compiled information on the financial and economic consequences. The total costs associated with medical error (lost income, lost household production, disability, health care costs) were estimated to be in the range of $37.6 billion to $50 billion for adverse events. Preventable adverse events, or those due to negligence, were estimated to cost the nation between $17 billion and $29 billion. “Even when using the lower estimates, the total national costs associated with adverse events and preventable adverse events represent approximately 4 percent and 2 percent, respectively, of national health expenditures in 1996. In 1992, the direct and indirect costs of adverse events were slightly higher than the direct and indirect costs of caring for people with HIV and AIDS” (Thomas et al., 2000). An Australian study also showed that the cost of adverse events arising from health care management might be as great a burden on society as all other forms of injury together.

In revealing medical error as an epidemic, the IOM report described the difficulties inherent in studying medical error and the limitations (circa 1999) of our knowledge:

“We do not yet have a complete picture of the epidemiology of errors. Many studies focus on patients experiencing injury and provide valuable insight into the magnitude of harm resulting from errors. Other studies, more limited in number, focus on the occurrence of errors, both those that result in harm and those that do not (sometimes called "near misses"). More is known about errors that occur in hospitals than in other health care delivery settings.” (Kohn et al., 1999)

1.2 Reasons for Medical Errors

Researchers conclude that adverse events in medicine arise from human fallibility, negligent care, limits of medical knowledge, risks inherent in medical practice, and biological variability among individuals (Fischer et al., 1997). Furthermore, medical personnel have great difficulty dealing with error on a personal level, and view any medical error as a personal failure of character and a shortcoming (Leape, 1994). In comparing the practice of medicine to aviation, Leape notes that any system that relies on error-free performance, as medical institutions do, is doomed to fail from the start. Leape called for sweeping cultural and systemic change, noting that if medical professionals "are going to succeed in reducing errors in hospital care they will need to fundamentally change the way they think about errors and why they occur."

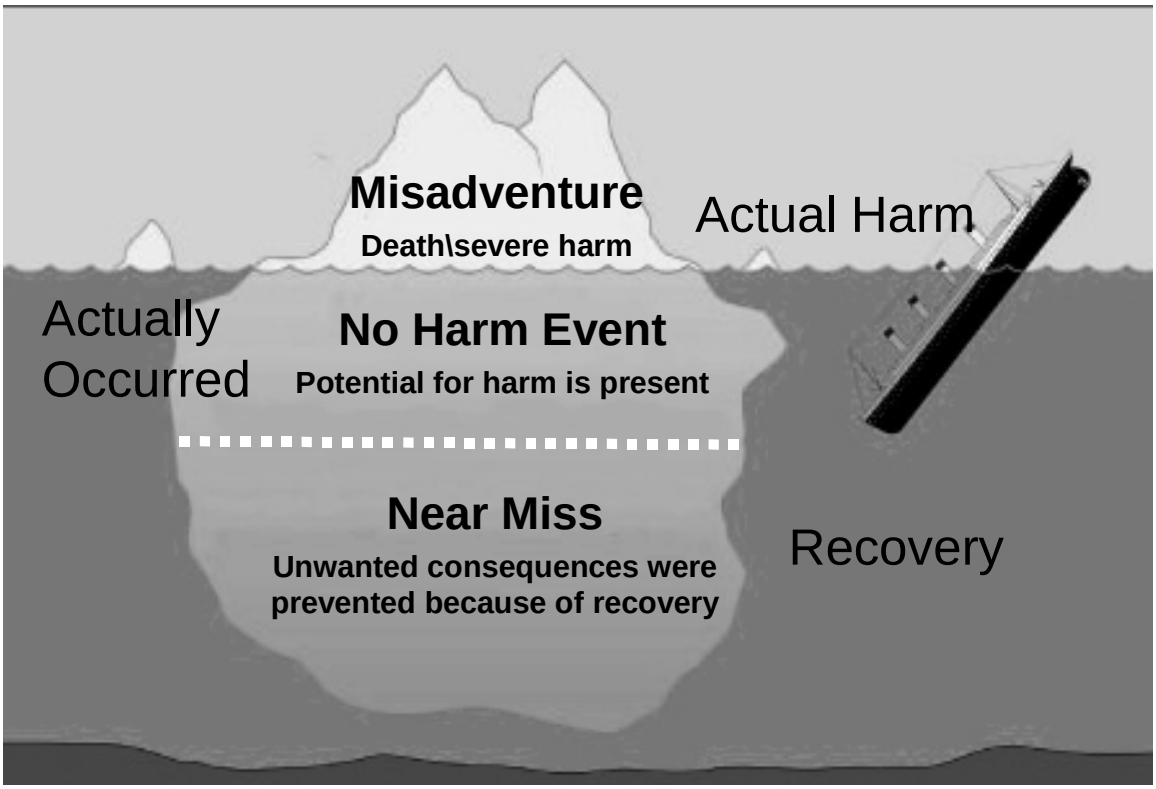
Other work supports Leape’s argument that medical professionals encounter cultural and psychological barriers to dealing with error. In surveys comparing the attitudes of doctors, nurses, fellows, and residents to cockpit crew on error, stress, and teamwork, Sexton and colleagues (2000) reported that denial of error in medicine is pervasive. Medical staff view error as “important but difficult to discuss and not handled well in their hospital.” Furthermore, medical staff denied the effects of stress and fatigue on performance, frequently did not accept their own susceptibility to error, and tended to play down the effects of anxiety and exhaustion.

To focus the issue on the underlying causes of error, multidisciplinary teams looked for causes of adverse drug events in 13 institutions, hypothesizing that system failures would be the overriding culprit (Leape et al., 1995). Sixteen major systems failures were uncovered, and "seven systems failures accounted for 78 percent of the errors; all could be improved by better information systems.” For example, lack of dissemination of drug knowledge was the most common system weakness related to adverse drug events, accounting for 29 percent of the drug-related errors.

1.3 A Conceptual Framework for Medical Errors and Events

A conceptual framework, known as the iceberg model of accidents and errors (see below), helps explain the dimensions of medical errors and related events. The "iceberg" model indicates that what is documented and recognized as serious error or severe harm (death or disability) of the patient is "the tip of the iceberg." Besides errors that result in actual harm to patients, everyday in health care facilities, numerous adverse events occur that do not result in harm to patients, either because the patient was treated and the harm reversed or because the harm was prevented by someone who observed and corrected a mistake before it reached the patient. These are "no harm events" and "near misses" where there was potential for harm to the patient but a professional recovered from a "slip" or an error was caught in time to prevent harm to the patient.

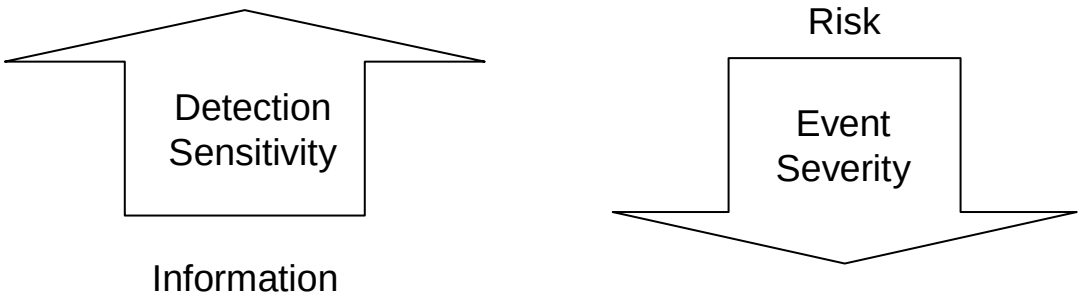
Figure 1: Conceptual Model of Accidents and Errors



Source: Battles, 2002a.

One of the consequences of tracking unplanned medical events and errors in order to eradicate them and improve patient safety is the paradox of reported events. A successful, data-driven patient safety program experiences an increase in the number of reported events (errors, no-harm events, and near misses), simply by instituting a program. This occurs because numerous problems exist that have never been documented, and the number of reported events will increase as the culture of safety spreads through an organization. The goal of an error management program should be to increase the "detection" (or number of reported events), so that the "event severity" (or risk of patient harm) can be reduced (Heinrich, 1941; OS, 2000, Battles, 2001; Battles, 2002). A successful program should see an increase in the former and a decrease in the latter as root causes of errors are discovered and actions are taken to eliminate the most egregious and obvious flaws in the processes of care. Over time the ratio of the number of minor and no-injury events to the number of major errors should rise, while the number of serious injuries to patients should decline (OS, 2000, Battles 2002).

Figure 2: Relationship of Detection Sensitivity to Event Severity



Source: Battles, 2002a

1.4 Initiatives to Reduce Medical Errors

Given that there appears to be so much to do to reduce medical errors, one strategy is to target research and patient safety initiatives on areas that have the most common and serious adverse medical events. A few studies have examined the nature of adverse events of all types (Thomas et al., 2000; Bhasale et al., 1998; Leape et al., 1995; Leape et al., 1991). The results vary with study scope and definitions of error, but generally, surgery, drug-related errors, and errors of diagnosis were the most common types. One study attributed 58% of adverse events to errors in management, and almost half of those to negligence (Leape et al., 1991).

The General Accounting Office (GAO) reviewed knowledge on adverse drug events (ADEs) in response to a Congressional request (GAO, 2000). The GAO report described the types and causes of ADEs, discussed the evidence on incidence and costs associated with ADEs, and explored what remedies the industry uses to reduce the severity and frequency of ADEs. The report concluded that little is known about the incidence of ADEs, ADEs are difficult to identify, data collected on ADE incidence are not comprehensive, knowledge of overall incidence is fragmentary, mortality estimates are uncertain, and data on associated costs are limited. What's more, suggestions for reducing ADEs and their severity are limited. The authors suggest "expanded surveillance programs to gather information about marketed drugs." They also suggest a "culture change" within medical institutions to encourage ADE reporting that would demonstrate to clinicians that the causes are systemic and not individual.

Another study of medication errors noted that there are "no incentives to reduce errors" (Newcomer, 2000). Newcomer concluded by calling for Federal intervention: "[A] computerized physician order-entry system as a condition of participation in Medicare is perhaps the simplest government approach to this problem." The LeapFrog Group, a coalition of health care purchasers (including Medicare) now rates hospitals on three evidence-based criteria, one of which is the use of a computerized physician order entry system for prescribing medications (Weber, 2000).

Focusing on another iatrogenic problem in hospitals, the Centers for Disease Control and Prevention (CDC) recently announced a new campaign aimed at hospital-caused infection. According to the American Hospital Association (AHA), the CDC "launched a new campaign to reduce the rates of hospital-acquired infection that the agency says affects nearly 2 million patients in the U.S. each year," (AHA News Now, March 27, 2002). This represents about 6 percent of hospitalized patients each year.

1.5 Obstacles to Reducing Medical Errors

While initiatives are growing, reporting on medical error is not without peril. Despite strong privacy laws to protect Federally collected data, there are no global privacy protections in the U.S. for information assembled on medical errors, and the HIPAA Privacy Rule will not solve this problem. Laws that exist to protect such reporting do so in a patchwork fashion, leaving many reporting systems exposed to legal discovery through normal court proceedings in the U.S. (Pritts et al., 1999; Liang, 2000).

For example, peer-review or quality assurance laws in some States protect information on medical mistakes from legal discovery as long as the information stays within the walls of the institution. Liang reviewed the vulnerability of the Joint Commission on Accreditation of Healthcare Organizations' (JCAHO) Sentinel Event Policy, which initially was set up to allow hospitals to report catastrophic events (e.g., deaths from medical mismanagement) to the JCAHO and to analyze the root causes of those errors. Liang concludes: "Absent a privilege, by reporting a sentinel event and delivering an RCA [root cause analysis] to the JCAHO, an entity may be compiling, and may need to deliver to the opposition without request, very damaging materials that were intended for safety rather than legal use." Anecdotal evidence suggests that institutions simply choose not to report adverse events. Even more worrisome, Liang expresses concern that State peer-review/quality-assurance (PR/QA) statutes that protect information within PR/QA committees may not protect sentinel event reports from discovery.

The HIPAA Privacy Rule, slated to go into effect April 14, 2003, does not fully protect error reports from legal discovery. The rule heightens the protections of health care data but it permits such data to be provided to law enforcement when required by law. The only way to fully protect medical error reports from legal discovery is through legislation. Many researchers (Liang, 2000, Pritts et al., 1999; Leape, 1994; and Newcomer, 2000) have recommend national legislation to protect medical error data and to encourage reporting and learning from medical mistakes.

These warnings have not gone unheeded. On June 5 and 6, 2002, bills were introduced in the U.S. Senate and U.S. House of Representatives to protect information voluntarily reported to medical event reporting systems from legal discoverability. The bills also require assembly of a national adverse medical event database and analysis to learn from errors and reduce medical errors in the United States. Tripartisan political support of the bill has made the health care industry hopeful that 107th Congress may finally pass effective legislation for assembling and learning from medical errors.

1.6 Definitions and Scope

Common language is the foundation of communication, learning, and understanding. Shared concepts and standard definitions are a necessary foundation for the field of patient safety, whether for research or for operations of health care providers. Differences in definitions can make inferences across studies impossible, and can make communication across operating departments difficult. For example, medical error has been defined as:

- The failure of a planned action to be completed as intended (i.e., error of execution) or the use of a wrong plan to achieve an aim (i.e., error of planning) (Reason, 1990; IOM, 1999; QuIC, 2000); or
- An unintended act, either of omission or commission, or an act that does not achieve its intended outcome (JCAHO, 2001).

The former definition excludes unplanned acts, while the latter includes them. Conflicting definitions are confusing in an operational setting and preclude meaningful comparisons across studies. Many related concepts and definitions have arisen in the literature on patient safety: close call, near miss, slip, mistake, latent error, active error, knowledge-based failure, rule-based failure, skill-based failure, adverse event, preventable adverse event, adverse reaction, sentinel event, error of omission (or planning), error of commission (or execution), no-harm event, accident. Nearly all connote different meanings. The same term can be defined differently across organizations. Appendix A contains a list of more than 70 terms that relate to patient safety, many with multiple definitions. The Institute of Medicine currently has a project underway to advise AHRQ on how to develop standards for definitions and classifications of medical error concepts.

A related issue for patient safety is how to define the scope of what is considered patient safety versus health care quality. For example, failure to prescribe beta blockers following myocardial infarction could be labeled an error of omission or it could be called poor quality of care. Two leading organizations on patient safety define patient safety slightly differently. The National Patient Safety Foundation defines

patient safety as: “the avoidance, prevention and amelioration of adverse outcomes or injuries stemming from the processes of health care” (NPSF, 1999). The Institute of Medicine defines patient safety as “freedom from accidental injury” (IOM, 1999). Under the NPSF definition failure to prescribe beta blockers could be considered an error in “prevention” of a future “adverse outcome stemming form the process of health care” (or lack thereof). Under the IOM definition, failure to prescribe beta blockers would not be considered an “accidental injury.” Health care quality, on the other hand, refers to the “degree to which health services for individuals and populations increase the likelihood of desired health outcomes and are consistent with current professional knowledge” (IOM, 1999). Failure to prescribe beta blockers would be considered a health care quality problem. Patient safety (as freedom from accidental injury) is clearly a subset of health care quality.

For this study of integration options for medical event reporting across USDHHS agencies, we define patient safety as “freedom from accidental injury,” the subset of health care quality. Thus, we are confining the scope of this project to obvious errors in the practice of health care which result in injury, rather than the broader array of decisions and interventions which reflect medical judgment about the diagnosis, treatment, and prevention of clinical conditions and which, in turn, is influenced by current clinical knowledge.

1.7 Enabling Reporting Systems for Medical Errors and the Benefits of Integration

A number of Federal systems of records on adverse medical events exist. The Food and Drug Administration (FDA) collects information on adverse events related to medical products. The CDC conducts surveillance on adverse events related to public health concerns – nosocomial infections, vaccines, and dialysis. The Centers for Medicare and Medicaid Services (CMS) monitors the quality and safety of care provided to beneficiaries. AHRQ is responsible for assessing the quality and safety of health care nation-wide. The Department of Veterans Affairs (VA) has a progressive program to reduce medical errors in the Veterans health care system. The Department of Defense and the Indian Health Service also are focusing on the quality and safety of their health care systems. The Health Resources and Services Administration (HRSA) assembles the National Practitioner Data Bank of malpractice liability claims.

In addition, the private health care sector has undergone a transformation in the last five years, using the Internet as an avenue for medical error reporting. Some error reporting (if only internal to the facility) is required for accreditation. Broader private reporting systems usually assemble error data only after it has been stripped of its patient, provider, and institutional identifiers.

All of these systems were started and have evolved for different purposes. They generally exist as separate islands of information with no bridges between them and few mechanisms for connecting findings across them. One important benefit to integrating such information would be better understanding of the causes of medical errors.

To take one example, a reportable event identified by the National Quality Forum is hyperbilirubinemia of more than 30 mg/dl in neonates, which can lead to death or mental retardation if not treated effectively. Many problems can cause hyperbilirubinemia, including infection acquired during delivery or during routine testing. The treatment may involve drugs (antibiotics), devices (phototherapy with blue wavelength lights) and constant monitoring (sometimes with central vascular catheters for very sick newborns). Imagine a scenario where neonate infection rates are higher at one institution than others. That institution is not aware of their infection rate problem, or if aware, attributes their higher rates to mothers with higher risk of complication. Imagine at the same time that a device such as a brand of bilirubin light is defective and that it manifests problems in 5 of 100 products. The institution experiences only one bilirubin light malfunction. Imagine further that a central line catheter shears off in the neonate during insertion, necessitating surgery to retrieve the catheter (see insert on problems with central line catheters). The consequence of these problems can be catastrophic – increased complications and death for a neonate. How many times does that scenario play out before it is recognized that infection rates are

problematic and common treatments for the problem might create further hazards? Linking pieces of information together can expose systemic problems not considered otherwise and can foreshorten time to discovery and resolution.

Case Study: Central Line Catheters

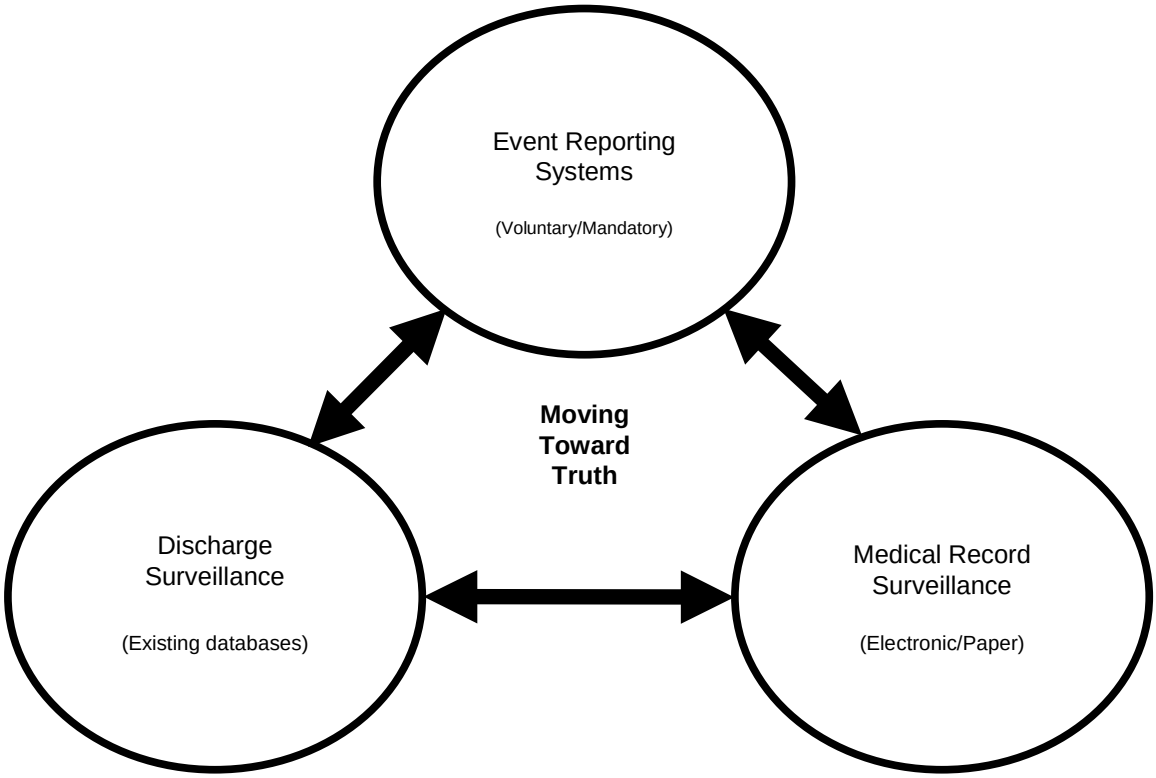
Insertion of central line catheters can be a hazardous process at best and, under emergency or training circumstances or with squirming babies, can lead to disaster. An institution may know that catheters can be sheared off inside the body by the cannula when a clinician inadvertently "backs up" a catheter during insertion. However, institutions may admonish and/or retrain clinicians in hopes of decreasing the risk, when the answer might be a better design of the catheter insertion device. Through assembly of experiences across multiple institutions with the FDA product monitoring systems and the CMS patient safety monitoring system, these and other hazards can be assessed and ideas for redesign can be generated. These databases will be invaluable for identifying processes for improvement among the thousands of medical products and processes in use in medical practice.

In this particular hypothetical example, neonate infection rates by institution could be identified from an AHRQ nationwide discharge database; statistical process control techniques could identify institutions with high infection rates, controlling for high risk mothers; institution-specific information would be shared with the individual institution only (honoring existing privacy agreements). More specific studies of the causes of neonatal infections could be conducted with a CDC hospital sample on nosocomial infections. Rare product defects in bilirubin lights should be apparent in FDA reporting systems. And in the future, systemic problems with central line catheters will be visible through a new CMS database that will be collecting detail on central vascular catheters (among other safety concerns) for a sample of medical records abstracted by the CMS Quality Improvement Organizations. Put together such information should trigger internal investigations in organizations with a high risk of error. Manufacturers would undoubtedly redesign devices to reduce hazardous processes, once aware of them. These processes should result in new insights into problems and actions to improve processes of care, better designs for equipment, increased safety, and decreased disability and death. Joining data from different perspectives (product defects, rates of infection, epidemiology of infection control, and medical record review) should expand patient safety knowledge tremendously.

However, improved safety through Federal information sources requires integrating those systems and databases so that information can be retrieved and assembled easily. Today, many of the pieces exist but are rarely put together or are too difficult to put together on a large scale. A few stories surface from time to time, which document the value of assembling information from multiple sources to create safer practice. For example, information from the CDC and FDA was responsible for detecting the cause of fatalities and impairments associated with contaminated cadaver tissue used in knee grafts throughout the United States (Marchione, 2002). Another example is an in-depth analysis of CDC and CMS data that uncovered the effect of re-use of dialysis device membranes after sterilization on outcomes of Medicare patients (Held et al, 1994). Institutions that sterilized and re-used the membranes had significantly higher death rates for dialysis patients. However, such examples are relatively rare given the thousands of procedures performed in caring for patients. There is currently no systematic process for identifying clinical processes that can be made safer.

Figure 3 shows the aim of a Federal USHDDS integration process. By integrating the parts of monitoring systems that exist today (both specific event reporting systems and more general surveillance data systems), the Federal government can aid and stimulate the movement toward a safer health care environment.

Figure 3: Components of Integrated USDHHS Event Reporting



Source: Battles, 2002b.

The integration of Federal reporting systems and related databases is not an ultimate solution or "the truth" of safety knowledge. Rather integrated information would move us toward true knowledge and stimulate a process that is inherently a local process. Patient safety is learned, practiced and improved only at the local level or "sharp end" of patient care. Information from integrated existing databases would target further work that must occur at local institutions.

Understanding patient safety as a local responsibility makes it clear that any integration of existing Federal databases must provide feedback to health care providers. That feedback mechanism must be accessible to health care providers and reporters of events in an immediate, "real time" context. It must be easy to navigate with an executive decision support framework that allows customized queries. It must link to analyses of the data conducted by experienced researchers and to other scientific evidence. It must be a kind of "one-stop-shopping" for information that can address the patient safety issues that arise in the practice of medicine. With such a design, practitioners would see the value of reporting, benefit from immediate information, and be more likely to become "willing reporters" to an integrated information system. With success, such a system of integrated Federal USDHHS information might expand to incorporate other data systems. Later in this report, we explore other systems that one day might choose to become a part of a national patient safety information system.

One immediate benefit of integrated USDHHS data systems would be addressing the concern of health care providers and purchasers that reporting systems, especially mandated ones, are proliferating and are confusing and burdening health care providers. An integrated USDHHS reporting system should eliminate the multiple processes required of institutions to report events and errors to multiple Federal agencies. A concern of policy makers is that reporting is uneven and plagued with problems. By comparing reports from different sources (for example, reports from practitioners and institutions against those from manufacturers), the FDA knows that events are grossly underreported at the point of care

(FDA, 1999). A system can and must be designed to stimulate reporting by showing reporters how reporting and the resulting information benefit them.

This section had attempted to explain how enabling and integrating reporting system would improve patient safety. In the process, this section has ignored one crucial barrier to realizing such Federal integration – the absence of full Federal protection of reported information from legal discovery. We discuss the issues of privacy protection later in this report and conclude that Federal law must be enacted to fully protect the information that is shared and collected to improve patient safety in the United States. Such legislation is a necessary condition for any of these dreams to become reality.

1.8 Project Background and Organization of the Report

Four USDHHS agencies, the AHRQ, CDC, CMS, and FDA, were given the mission by the Secretary to plan integration of their data systems that relate to medical errors or adverse medical events. These agencies have been collaborating through an inter-agency group, the Patient Safety Task Force, led by AHRQ. In 2001, AHRQ contracted with The MEDSTAT Group, Inc. to develop a plan for integrating the four agency's systems. This project was initiated as a result of that work.

Within the four agencies, approximately 24 data systems (some existing, some under development, some being merged, some being retired) are relevant. The goal of this project is to provide recommendations for integrating these medical event reporting systems, and as a preliminary step toward achieving that objective MEDSTAT conducted a detailed investigation of the four agency's relevant data systems. An overview of our approach to reviewing these systems is presented in Section 2 of this report. The results of the investigation - abstracts of the salient characteristics of the 24 systems - are presented in Section 3. Table 1 below shows the level of activity in 17 of the USDHHS systems, which are fully functioning . The level of activity – in the tens and hundreds of thousands per year – varies considerable among the reporting systems. The administrative data systems developed for purposes other than medical error reporting (HCUP and OASIS) amass millions of records per year.

Table 1: Purpose and number of events per year for selected DHHS medical event reporting and related systems.

System Name	System Purpose	Approximate number of records per year
Adverse Event Reporting System (AERS)	The Adverse Event Reporting System (AERS) is an information workflow system designed to support the FDA's post-marketing safety surveillance program for all approved drug and therapeutic biologic products. The ultimate goal of AERS is to improve the public health by providing the best available tools for storing and analyzing safety reports. One major function of AERS data is to ensure that a product's labeling information correctly captures the adverse events associated with the product. This data can also be used to re-evaluate an approval decision on an established product.	174,500
Alternative Summary Reporting (ASR)	The Alternative Summary Reporting system replaces individual mandatory reporting from manufacturers for those devices where documented problems with the devices are well understood and there is diminished return in the evaluation of individual event reports for these devices.	37,000
Biological Product Deviation Reporting (BPDR) System (BIODEV)	The Biological Product Deviation Reporting system is one method CBER uses to monitor product deviation in manufacturing of products, including testing, processing, packing, labeling, and storage, or with the holding or distribution of a licensed biological product, blood or a blood component, in which the safety, purity, or potency of a distributed product may be affected.	25,000
Dialysis Surveillance Network (DSN)	DSN is a voluntary surveillance system-monitoring bloodstream and vascular access infections and includes adult/pediatric outpatient dialysis centers caring for chronic hemodialysis patients. The purpose of the DSN is to provide a method for individual hemodialysis centers to record and track rates of vascular access infections, other bacterial infections, hospitalizations, and intravenous antimicrobial starts. The DSN also provides a method to aggregate, compare and distribute data to cooperating dialysis centers and the public health and medical communities. The data are used to prevent infections and slow the spread of antimicrobial resistance. A secondary purpose is to record rates and syndromes prompting use of IV antimicrobials in hemodialysis centers.	14,000
End Stage Renal Disease (ESRD) Network	The ESRD Networks provide a cost effective mechanism to ensure the most efficient use of Medicare dollars for dialysis treatment and kidney transplantation through monitoring quality of care indicators and maintaining timely, complete data on the ESRD program. These functions are administered at the regional level, providing direct and immediate access from the treatment provider to the Centers for Medicare and Medicaid Services (CMS) through the ESRD Networks.	2,300
Healthcare Cost and Utilization Project (HCUP)	HCUP is a family of healthcare databases and related software tools and products developed through a Federal-State-industry partnership and sponsored by the Agency for Healthcare Research and Quality (AHRQ). HCUP databases bring together the data collection efforts of State data organizations, hospital associations, private data organizations, and the Federal government to create a national information resource of patient-level health care data. These databases enable research on a broad range of health policy issues, including cost and quality of health services, medical practice patterns, access to health care programs, and outcome of treatment at the national, State, and local market levels.	45,000,000

Manufacture and User Data Experience -Medical Devices (MAUDE)	The MAUDE database consists of data representing adverse event reports involving medical devices. The term Medical Device Reporting (MDR) is often used to refer to this program and is the mechanism for the FDA to receive significant medical device adverse events from manufacturers, importers and user facilities to assure the safety, effectiveness, and proper labeling of medical and radiation emitting devices.	362,000
Minimum Data Set (MDS)	The MDS is designed to collect data about an individual nursing home resident which will ultimately lead to a comprehensive, outcome-oriented care plan for that resident; it consists of specific questions about a resident in several areas. The questions cover factors that place a resident at risk for an adverse outcome.	184,000
Medical Restraints	This program was started as part of the FDA-led Hospital Bed Safety Work Group initiatives and to meet the Medicare requirement that institutions must report incidents of harm to patients involving the use of physical and other restraints as a condition of participation in the program.	12
Medical Device Surveillance Network (MeDSuN)	The goal of the Medical Device Surveillance Network (MeDSuN) is to improve the protection of the health and safety of patients, users and others by reducing the likelihood of the occurrence of medical device related adverse events and, if they do occur, reducing the likelihood that they will be repeated. MeDSuN is designed to collect data from user facilities (hospitals, nursing homes and other health care facilities required to report under the Safe Medical Devices Act (SMDA)).	315
MedWatch	MedWatch is an FDA post market surveillance program for reporting serious adverse events (death, life-threatening, hospitalization, disability, congenital anomaly, required intervention to prevent permanent damage) associated with all medical products (drugs, medical devices, biologics, and special nutritional products). It is targeted toward reporting of events by individual health professionals and consumers.	18,000
Medical Event Reporting System for Transfusion Medicine (MERS-TM)	The Medical Event Reporting System for Transfusion Medicine (MERS-TM) is an event reporting system developed for transfusion services and blood centers to collect, classify, and analyze events that could potentially compromise transfusion safety. In addition to basic reporting, MERS-TM provides the opportunity to study and monitor both actual and near-miss events to facilitate process improvement efforts.	27,450
Medicare Patient Safety Monitoring System (MPSMS)	The MPSMS is a new system, which is currently in the conceptualization phase, that is being considered for pilot stage development by CMS and its partners on the Patient Safety Task Force. The overall goal of the MPSMS is to produce rates of adverse patient events and risk factors that contribute to them among the Medicare population.	60,000
The National Nosocomial Infections Surveillance System (NNIS)	The National Nosocomial Infections Surveillance (NNIS) System is a cooperative effort between the Centers for Disease Control and Prevention (CDC) and participating hospitals to create a national nosocomial infections database. The database is used to: describe the epidemiology of nosocomial infections, describe antimicrobial resistance trends, and produce nosocomial infection rates to use for comparison purposes.	10,000
Outcome and Assessment Information Set (OASIS)	The OASIS is a group of 79 data elements that represent core items of a comprehensive assessment for an adult home health care patient and form the basis for measuring patient outcomes for purposes of outcome-based quality improvement.	10,800,000
Vaccine Adverse Event Reporting System (VAERS)	VAERS is a post-marketing safety surveillance program, collecting information about adverse events (possible side effects) that occur after the administration of US licensed vaccines.	12,000
Vaccine Safety Datalink (VSD)	The VSD project prospectively collects computerized medical record data under a joint protocol at HMOs on vaccinations, medical outcomes (e.g. outpatient visits, emergency room visits, hospitalizations, and deaths), and covariates (e.g. birth certificates, census data). The data are then linked under joint protocol at multiple health maintenance organizations for analysis.	500,000

Although this project's focus is to make recommendations for the integration of event reporting systems operated by the four PSTF agencies, it is clear that the agencies' efforts in this regard are inextricably linked to a number of external factors that shape the medical error event reporting landscape. These factors include the legal and regulatory environment, existing and emerging standards and parallel efforts in other agencies, other countries and the private sector. Section 4 of this document presents the results of our investigation of external factors.

Of the many options we considered, the two most promising are presented in Section 5. For each option, we describe which agency systems participate in the integration plan, present a scenario for integrating the systems and discuss the advantages and disadvantages of the plan. Our final recommendation is presented in Section 6.

1.9 This Project and the Four PSTF Agencies

Four USDHHS agencies comprise the Patient Safety Task Force: the AHRQ, the CDC, the CMS, and the FDA. AHRQ is responsible for conducting and disseminating research in order to improve the quality and safety of health care in the United States. The CDC investigates threats to the public health and institutes policies to control and prevent outbreaks of infectious disease and adverse events from public health treatments. CMS is responsible for purchasing quality health care for its Medicare beneficiaries and funding quality care through the States-administered Medicaid Program for low-income people, while the FDA is responsible for monitoring and protecting the safety of medical products, including pharmaceuticals, medical devices, and biological products produced by manufacturers.

The Centers for Disease Control and Prevention (CDC) conducts surveillance on adverse events related to public health concerns – nosocomial infections, vaccines, and dialysis. The FDA collects information on adverse events related to medical products. The Centers for Medicare and Medicaid (CMS) monitors the quality and safety of care provided to beneficiaries. Thus, while the CDC may be focusing on diseases, FDA is monitoring products, CMS may be observing payments, patients, or providers, and AHRQ is studying multiple dimensions of the health care system. These divergent foci must be considered in any integration effort.

The Patient Safety Task Force developed a short-range and long-range vision for the integration of USDHHS systems. There are three near-term goals :

- To reduce the burden of existing reporting systems for those on the front-lines of medical care,
- To improve the level of reporting to USDHHS systems, and
- To improve the information and learning from existing USDHHS systems.

The long-term goals of this project are to foster integration of medical event reporting with other Federal agencies, to create a model for reporting nation-wide for both public and private systems of records, and to facilitate international collaborations. All of these goals support the broader objective of learning from and reducing adverse medical events and medical errors of all types – latent and active, slips and mistakes, near misses and close calls, and preventable and unpreventable adverse events. It is with these objectives in mind that MEDSTAT approached the Medical Event Reporting Integration Planning Project for the four PSTF agencies.

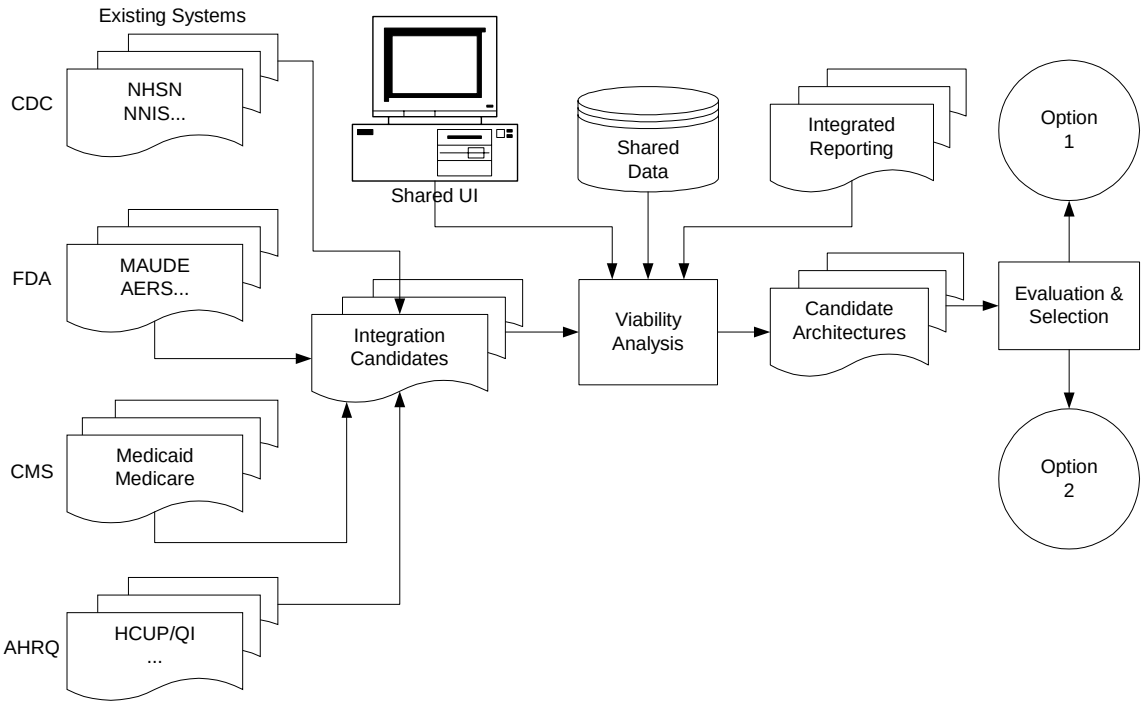
2 Approach

2.1 Introduction

In this section we describe the approach we used to conduct the project. The ultimate purpose of the approach is to arrive at a plan to recommend as the first step in integrating medical event reporting for the agencies that comprise the PSTF. Our intent was to proceed sequentially through a series of steps designed to reach that end in a methodical and comprehensive manner. We wanted to be reasonably certain when we arrived at a recommendation that we had not overlooked other promising alternatives and that we had not recommended action that had a poor chance of success due to substantive incompatibility, technological infeasibility or organizational constraints.

Figure 4 below is a diagram of the process we used. We began by investigating all of the relevant medical event systems (approximately two dozen) in operation or under development by the CDC, the FDA, CMS and the AHRQ. This step is shown at the far left of Figure 4. After we had gathered enough information to accurately portray the salient characteristics of each of these systems, we began to form subsets of the collection that we called *integration candidates*. These subsets were not chosen randomly; in order to qualify as an integration candidate the collection needed to possess at least some element of synergy; there needed to be an argument, however weak, that the integrated whole was somehow more useful than the sum of the non-integrated parts.

Figure 4: Process Used to Conduct the Project



Next, we looked at which aspects of the systems within a particular integration alternative should be merged: the user interface and/or the data store and/or the reporting engine. That is, we examined alternative system architectures for each of our integration candidates. These alternatives were subjected to a *viability analysis*, shown in the center of Figure 4. In order to be viable, an architecture must:

- Be compatible with the collection of systems it is being applied to. For example, there is no reason to specify a shared user interface for the AHRQ HCUP database, because the HCUP database has no user interface.

- Be efficient from a systems standpoint. An integrated reporting engine that must pull low-level data over the Internet is not efficient, therefore not viable.
- Be viable from the point of view of reasonably rapid implementation.

The viable alternative architectures for the integration candidates form the set of *candidate architectures* shown in Figure 4. Finally, these candidate architectures are evaluated and the best are selected. The evaluation is performed with respect to a set of solution criteria developed by the Project team and its advisory groups. These solution criteria are presented in Section 5.2 of this document.

2.2 Investigating the Existing Systems

Our approach is based around four distinct teams. Three of the teams are each assigned a well-defined domain of the overall information system environment and a fourth is tasked with external factors. The domains of the four teams are:

- *Acquisition of medical event data*. This aspect of the process is also sometimes referred to as medical event data entry, data collection, data capture and medical error or event reporting.
- *Storage of medical event data*. This is sometimes referred to as "data structure" or "data warehousing." We prefer the general term "data storage" and use it to encompass all aspects of the mechanisms used to store data subsequent to its input.
- *Use and analysis of medical event data*, the final step in the process in which event data are collated, selected, listed, statistically summarized or otherwise displayed for analysis. This is referred to variously as data mining, data analysis, and reporting.
- *External factors*, comprised of legal and regulatory issues, standards, and non-Federal and non-US systems.

It is clear that these areas involve separate constituencies and require different areas of expertise to understand. Thus our approach was to assemble four teams with distinctly different expertise and to assign each team the relevant aspects of all the systems we investigated. The input of medical event data often occurs in a clinical setting, and clinicians and medical technicians are in the best position to determine and evaluate the variety of ways in which medical events are best characterized, completely and accurately defined, and ultimately differentiated from each other. How the medical event data are stored subsequent to its capture and transformed for reporting purposes is typically the province of Information Systems personnel. Evaluating data storage methods and the potential for system integration is best accomplished by computer scientists and IT professionals specializing in database technology. The users of medical event data are the general public as consumers of health care, practitioners and members of the provider community who determine policy, and healthcare researchers and analysts. Investigating the ways medical event data are analyzed requires knowledge of data presentation methodologies, institutional benchmarking practices, general statistical inference, and a practical understanding of privacy and confidentiality constraints. A fourth team explored systems and standards as they relate to the USDHHS systems. This "external systems" team was tasked with issues such as what lessons can be learned from similar databases in foreign countries and whether information from an integrated system could usefully be combined with proprietary and private-sector databases.

Each of our four teams had separate responsibilities, corresponding to their domain of expertise. Each team was responsible for two sets of activities:

- The data inquiry phase into each of the medical event systems, as appropriate to their domain of expertise and
- The synthesis and evaluation of integration alternatives, as they apply and overlap into the team's domain.

The first set of activities corresponded to fact-finding on all the medical event systems investigated. To do this we created a standard information-gathering framework, or template, of characteristics to be

abstracted from each of the data systems. We then researched and documented those characteristics for each of the systems being studied (see Appendix B).

2.3 System Architecture

A plan for integrating event reporting systems is more than an enumeration of the existing systems that will comprise the integrated system. The plan must also specify which aspects of the systems will be merged and which, if any, will remain separate. Finally, the plan must provide a high-level blueprint, or architecture, of the computer systems, servers, databases, software and telecommunications that can most efficiently implement the desired alternative.

To describe an architecture, we decomposed systems into (at most) three areas: the user interface, the data store and the reporting engine(s). Each of these subsystems can either be implemented *locally*, that is uniquely for each system (as they are now in the existing separate systems), or *centrally*, from one shared facility that serves all the systems, or *both* locally and centrally as appropriate. Although this approach helps us be comprehensive in our search for architectural alternatives, its drawback is that it generates too many possibilities. In theory this approach yields 3 x 3 x 3 = 27 unique architectural configurations, but in practice some of the combinations are nonsensical and can be effectively eliminated from consideration. For example, while it might make sense to store data both locally and centrally and to perform reporting both locally and centrally, it makes no sense to store data only locally and perform reporting only centrally.

Just as some architectural combinations might not be intrinsically appealing, the combination of a particular architectural configuration with certain existing systems might not make sense. For example, any integration candidate that includes the CMS Medicaid and/or Medicare research databases with a shared data store is probably impractical for a Phase 1 implementation because of the vast quantities of data that would need to be housed at the shared data warehouse.

It is this combination of validating the internal consistency of a particular architectural configuration and assuring the appropriateness of applying the architectural configuration to a particular set of systems that constitutes the viability analysis step shown in Figure 4. This is the primary method we used to narrow down what at first blush appears to be an overwhelming number of possible architectures for a particular integration candidate to an acceptably few actual candidate architectures.

Finally, the solution criteria are used to evaluate the remaining candidates and rank them accordingly. The solution criteria are divided into two groups: required criteria that must be met and optional criteria, which are desirable but not necessarily required. It should be noted that the criteria are not applied in a true/false manner. Rather, an alternative typically falls somewhere on a continuum between completely failing the criteria and completely meeting it.

2.4 Guidance from the Expert Panel

The External Advisory Panel (EAP) was composed of representatives from health organizations who would have a stake in integrated medical event reporting (i.e., health care professionals who would be reporting to or using an integrated medical event reporting/data system for medical event tracking and research). Specifically, EAP members were selected from the following groups:

- providers of health care services,
- producers of health care products,
- policymakers in the patient safety arena, and
- researchers in patient safety and related fields.

These representatives guided the work of the Task Order so that it met the needs of relevant constituencies. In addition, organizations with a mission focused on patient safety or healthcare quality were included to influence activities that would result in support of a national reporting and data system.

We used the list of faculty and participants of the 2001 National Patient Safety Summit on Data Collection and Uses and a list of board members of the National Quality Forum to identify individuals that represented some of these groups. We recommended the formation of a twelve-member panel and that the TOO and PSTF select from our candidates as well as identifying additional members not listed among our candidates. Appendix C lists the members who were chosen and accepted a position on the panel.

Two meetings were planned to obtain input from the EAP members - an initial meeting held prior to the start of work with the reporting agencies, and a final meeting held after the work team produced a preliminary version of the draft report and recommendations. The major expectations of the EAP were to:

- review and comment on the study design, and
- review and comment on the draft report and recommendations for an integrated national medical event reporting system.

2.4.1 Meeting 1: Planning

An initial meeting was held December 18, 2001. Ten panel members attended the meeting, which included members of the Patient Safety Task Force (PSTF) and the Task Order Officer, James Battles. Six MEDSTAT project team members were in attendance including the principal investigator, project manager, and members of the data acquisition, storage, use and external work teams.

The purpose of the meeting was to introduce panel members to PSTF and MEDSTAT staff, provide project background information, and obtain their feedback on the project scope, system goals, identification of users, solution criteria and desired outcomes. Appendix D contains a list of goals that panel members decided were important for this project. Appendix E lists user groups that would be affected by and/or report to an integrated patient safety reporting system. Participants felt that each identified user could have multiple goals for the integrated system.

In meeting the goals, participants recommended that the project team be aware of major patient safety reporting initiatives currently operating external to DHHS and to incorporate the best practices from these initiatives. Particular systems to focus on during the project included those sponsored by JCAHO, the United Kingdom (noting a bi-lateral agreement between US and UK to share data), Australia, AHRQ-sponsored demonstration projects, New York's NYPORT, and the Massachusetts safety system.

Team members were advised to focus on making reporting a useful activity where input would be useful to the agencies collecting data as well as accessible to users. In this regard, the final system should act as a two-way tool for all users, not just meet the regulatory needs of the individual agencies. Members suggested that inclusion of near miss data, standardization of terminology, coding and classification systems, and an aggregation and expansion of collected information could all be helpful to improve the usefulness of the new system. However, improving the current system should be accomplished with a minimal negative impact on current reporters (e.g. manufacturers, distributors, health care professionals) who, in some cases, have developed elaborate processes to meet present reporting requirements.

Privacy and de-identification of data were also seen as major issues to be addressed. In particular, the team was directed to determine when to de-identify data and how to link data for the same adverse event without compromising patient privacy or subjecting healthcare organizations to undo potential for litigation. The team was cautioned to be up-to-date on current privacy laws (e.g., HIPAA) and to review HHS regulations that might need to be changed to improve linkages between systems.

2.4.2 Meeting 2: Review

The second meeting of the Executive Advisory Panel was held May 16, 2002. Nine panel members, two DHHS staff, six MEDSTAT project team members and the Task Order Officer (TOO) attended this

meeting. All attendees received a preliminary version of the draft report prior to the second meeting with the expectation that they would review the report prior to their arrival.

The purpose of the second meeting was to obtain feedback from the panel on the draft report and to provide members with more details on the two recommended options to allow for further discussion of these alternatives. After an overview of the agenda, members were asked to provide their initial impressions of the draft report. The majority of the panel felt that the report was comprehensive and met the goals of the project, but did not address issues of data usefulness and whether the options would actually improve patient safety.

MEDSTAT staff used the second half of the meeting to provide the EAP members a detailed overview of the two options. Following the overview, members were encouraged to discuss the advantages and disadvantages of these two alternatives. Several members pointed out the need to map a single type of event under the two options to determine how each option would offer an improvement over the existing systems. Suggested scenarios to map included dialysis therapy, use of catheters, and any of the practices listed in the National Quality Forum 'Serious Reportable Events' report. The meeting concluded with staff members comparing each option against the solution criteria.

3 Findings and Implications

This section begins with a brief overview of each DHHS system, and subsequently outlines the implications for integrating some or all of these systems. It is important to note that even though our analyses are deemed to be complete and accurate, several of these systems are either under development, in the process of being phased out, or otherwise subject to change. Thus, these findings represent the state of the systems at the time of our research. Where possible, we have tried to note which systems are in flux.

3.1 AHRQ System

3.1.1 HCUP

The Healthcare Cost and Utilization Project (HCUP) is a family of healthcare databases and related software tools and products developed through a Federal-State-industry partnership and sponsored by the Agency for Healthcare Research and Quality (AHRQ). HCUP databases bring together the data collection efforts of State data organizations, hospital associations, private data organizations, and the Federal government to create a national information resource of patient-level health care data. HCUP includes the largest collection of longitudinal hospital care data in the United States, with all-payer, encounter-level information beginning in 1988. These databases enable research on a broad range of health policy issues, including cost and quality of health services, medical practice patterns, access to healthcare programs, and outcomes of treatments at the national, State and local market levels.

AHRQ is committed to developing databases suitable for a broad range of health care studies that may be released to public and private users. HCUP databases are constructed with data from State data organizations, hospital association, and private data organizations. At present, HCUP received inpatient data from 29 States, institutional outpatient data from 11 States, and emergency department data from four States. These data are processed and placed into a uniform format with safeguards included to protect the privacy of individual patients, physicians, and hospitals. Many of the HCUP databases are available through restricted access, public release from AHRQ. HCUP data users must agree to certain conditions: the database can be used only for research and statistical purposes; patients and institutions cannot be identified in publications.

3.2 CDC Systems

3.2.1 The National Healthcare Safety Network

Prompted by the recommendations of the Patient Safety Task Force, the CDC is spearheading the creation of the National Healthcare Safety Network (NHSN). Key goals are to minimize the burden of reporting adverse events by developing integrated computer networks, flexible and user-friendly reporting systems and standards for coding the content of adverse event reports. NHSN data will support development of national benchmarks as well as facility-specific information and quality assurance functionality.

The NHSN model will enable electronic reporting of adverse events at the point of occurrence, provide a standardized IS architecture for CDC systems, use a centralized web-based system and create a uniform user interface.

The NHSN will replace the following systems, all of which collect information associated with adverse events. These data are collected from hospital facilities/dialysis centers that voluntarily participate in related programs:

- National Nosocomial Infections Surveillance System (NNIS)
- Dialysis Surveillance Network (DSN) and

- National Surveillance System for Hospital Healthcare Workers (NASH) - not including Tuberculosis-related events

The NNIS and DSN systems are included within the scope of this project and are described in the following pages. NASH is not included as part of the project.

The NHSN is distinct from, but related to National Electronic Disease Surveillance System (NEDSS). NEDSS is a CDC-developed public health initiative that provides a standards-based, integrated approach to disease surveillance and supports connection to developing clinical information systems. Where appropriate, NEDSS standards have been adopted by the NHSN. The NEDSS infrastructure consists of a Base System, which provides for basic data collection, reporting and system services, and Program Area Modules (PAMs), for program-specific data collection. NEDSS-compliant systems will accept, route and process electronic HL7 messages, and can accommodate LOINC and SNOMED coding standards. GIS COTS products, statistical packages and other visualization tools will support display and mapping functions. The interface will be implemented through industry standards (e.g., ODBC and JDBC).

Key users are expected to include CDC professionals, infection control practitioners, nurses (e.g., dialysis, utilization review), researchers, employee health managers and epidemiologists.

The application will be rolled out initially to existing participants in the three programs. Implementation is expected to begin by the Fall of 2002. While the system may only be partially completed with the current fiscal year, expectations are that the NHSN will be available, at least in beta, during the summer of 2002.

3.2.2 Dialysis Surveillance Network (DSN)

The Dialysis Surveillance Network (DSN), a voluntary national surveillance system monitoring bloodstream and vascular infections, was initiated by CDC in August 1999.

The purposes of the DSN are as follows:

- To provide a method for individual hemodialysis centers to record and track rates of vascular access infections, other bacterial infections, and intravenous antimicrobial starts.
- To provide a method to aggregate, compare and distribute data to cooperating dialysis centers and the public health and medical communities.
- To use these data to prevent infections and slow the spread of antimicrobial resistance.

Both adult and pediatric dialysis centers treating outpatients are invited to participate. Data collected include incident type (hospitalization, in-unit IV antimicrobial start or both), problems that led to hospitalization or IV antimicrobial start, treatment and blood culture information. Incident forms include standardized coding used to describe the event and record information. A unique feature of the system is the fact that data collectors record the presence or absence of criteria for infections, not the infections themselves. A computer algorithm determines whether the infection case definitions are met.

Several rates are reported to characterize the situation at any given center and comparisons to benchmarks are provided. Summary descriptive statistics and trending information are also available for analytical and research purposes. Participating centers may enter data on paper forms provided by CDC or they may use an Internet-based system for data entry and analysis. However, the data from individual centers are confidential and cannot be released to anyone other than the dialysis center reporting it.

3.2.3 Vaccine Adverse Event Reporting System (VAERS)

In 1990, the Vaccine Adverse Event Reporting System (VAERS) was established under the joint administration of the Centers for Disease Control and Prevention (CDC) and the FDA to accept reports of suspected adverse events after administration of any U.S. licensed vaccine. The CDC's focus is the detection of unusual epidemiologic trends or associations. The FDA uses VAERS primarily as a tool for

post-marketing research and surveillance, necessary to identify safety issues that may only be detected following vaccination of a much larger and more diverse population.

VAERS accepts reports of adverse events that may be associated with U.S. licensed vaccines from health care providers, manufacturers, and the public. Consistent with AERS reporting criteria, manufacturers are required to report serious and unexpected adverse events within 15 days. Non-serious or expected adverse events are reported quarterly or annually. The Reportable Events Table (RET) reflects what is reportable by law (42 USC 300aa-25), including conditions found in the manufacturers package insert. Reporting is voluntary for health professionals and consumers, although the National Childhood Vaccine Injury Act requires providers to report any event listed by the vaccine manufacturer as a contraindication to subsequent doses of the vaccine and any event listed in the Reportable Events Table that occurs within the specified time period after vaccination. VAERS is consumer driven and by design there are no limits/restrictions for deciding what constitutes adverse event.

VAERS receives 12,000 reports per year, approximately 15 percent of which describe serious adverse events. Data captured includes product, patient demographics, location of vaccination, prior vaccinations, contraindications/allergies, other medications, diagnostic/laboratory data and patient outcome. During processing, coding is added to describe adverse event. The coding system is transitioning from COSTART to MedDRA.

Reports can be received by mail, fax or telephone. Development of web-based submission facilities is currently underway. De-identified VAERS data can be downloaded from the Internet or obtained from the National Technical Information Service for use by researchers or other interested parties. Copies of published reviews are also available from VAERS.

3.2.4 Vaccine Safety Datalink (VSD)

The Vaccine Safety Datalink began in 1990 as a collaborative effort involving the CDC and several large health-maintenance organizations. The VSD project prospectively collects computerized medical record data under a joint protocol at HMOs on vaccinations, medical outcomes (e.g. outpatient visits, emergency room visits, hospitalizations, and deaths), and covariates (e.g. birth certificates, census data). The data are then linked under joint protocol at multiple health maintenance organizations for analysis. Approximately 6 million persons (2 percent of the U.S. population) are members of the HMOs that participate in the VSD. The standardized LLDB (Large Linked Database) and infrastructure created for the VSD have provided opportunities to address vaccination coverage and cost effectiveness related to immunization. The VSD enables large epidemiological studies of vaccine adverse events, captures information on less commonly occurring types of adverse events, and helps determine whether an event is linked with a vaccine or with some other cause.

All vaccines administered within the study population are recorded. Available data include vaccine type, date of vaccination, concurrent vaccinations (those given during the same visit), the manufacturer, lot number and injection site. Medical records are then monitored for potential adverse events resulting from immunization.

While there are no links to other databases, VSD and VAERS are complementary methods of monitoring data. Based on analysis of individual reports, VAERS is a signal generator, designed to identify problems with specific vaccine lots and to identify adverse events that were not uncovered through the pre-marketing process. VSD supports population-level analysis including hypothesis testing via formal research methods to identify causal relationships between adverse outcomes and vaccination. VSD focused its initial efforts on examining potential associations between immunizations and 34 serious neurologic, allergic, hematologic, infectious/inflammatory, metabolic conditions. The VSD project allows for planned vaccine safety studies as well as timely investigations of hypotheses. At present, the VSD project is examining potential associations between vaccines and a number of serious conditions. The database is also being used to test new vaccine safety hypotheses that result from the medical literature,

VAERS, changes in the immunization schedule or from the introduction of new vaccines. At this time VSD does not make its data available to the public.

3.2.5 National Nosocomial Infection Surveillance System (NNIS)

The National Nosocomial Infections Surveillance (NNIS) System is a cooperative effort that began in 1970 between the Centers for Disease Control and Prevention (CDC) and participating hospitals to create a national nosocomial infections database. The main purposes of NNIS are to describe the epidemiology of nosocomial infections, describe antimicrobial resistance trends and produce nosocomial infection rates to use for comparison purposes. The system involves the voluntary participation of acute care general hospitals only, with 315 hospitals participating at the beginning of 2000.

NNIS data are collected by trained infection control personnel using explicitly defined terms and surveillance protocols that target inpatients at high risk of infection. Infection data as well as "denominator" utilization data (e.g., number of ICU days) are collected. Infection data include hospital location (e.g., burn unit), infection site (e.g., urinary tract infection), any related surgical procedures, the pathogen involved and, if relevant, the contribution of the infection to patient death. The NNIS has its own standardized coding describing the type/location of infection, contribution to death and pathogen as well as a risk-based index for surgical procedures. NNIS operative procedure categories use ICD-9-CM codes that are specified and a list of ICD-9-CM that do not qualify as NNIS operative procedures. All infection sites are categorized into major and specific infection sites by using standard CDC definitions that include laboratory and clinical criteria.

Hospitals report data monthly via modem to the CDC through the IDEAS system (DOS based microcomputer system). The CDC aggregates the data to create the NNIS database. Data from each hospital is available at their site and facilities can grant other users access to their data.

3.2.6 National Center For Health Statistics

The National Center for Health Statistics (NCHS) is a part of the Centers for Disease Control and Prevention. NCHS works closely with other Federal agencies as well as researchers and academic institutions to meet priority data needs for public health.

NCHS obtains statistics through a broad-based program of ongoing and special studies, including household interview surveys, examination surveys, surveys of health care providers, and collection of statistics on birth and death in partnership with State government. NCHS data systems include data on vital events as well as information on health status, lifestyle and exposure to unhealthy influences, the onset and diagnosis of illness and disability, and the use of health care. NCHS provides mechanisms for obtaining consistent, uniform statistics that allow for comparison across population groups, types of health care providers, and States; for planning, targeting, and assessing the effectiveness of public health programs, and for identifying health problems, risk factors, and disease patterns. These data are used by policymakers in Congress and the Administration, by medical researchers, and by others in the health community. CDC has collected information on patient safety as part various provider- and patient-based surveys, and will likely continue to do so in the future.

3.3 CMS Systems

As part of its function as a payor, the CMS routinely collects claims data (including procedural and diagnostic coding) that can be applied to research studies. Data are used by the CMS and independent researchers to understand the epidemiology of disease, examine quality, and gain insights into the impact of interventions and policies on healthcare outcomes. These data are maintained by the Office of Information Systems.

3.3.1 CMS Quality Related Data Systems

The Office of Clinical Standards and Quality maintains a number of data systems specifically designed to examine quality of care across the array of CMS programs. These include the Peer Review Organization data for inpatient and outpatient care (PROs are now known as QIOs), the Minimum Data Set for nursing home care, data collection efforts related to the end-stage renal disease program, and the OASIS home health care data.

3.3.2 Quality Improvement Organization Data for Inpatient and Outpatient Care

CMS administers the Quality Improvement Organization (QIO) Program that is designed to monitor and improve utilization and quality of care for Medicare beneficiaries. The program consists of a national network of fifty-three QIOs (formerly known as Peer Review Organizations) responsible for each U.S. State, Territory, and the District of Columbia. The network of QIO data is called the Standard Data Processing System (SDPS).

SDPS is designed to standardize and facilitate the exchanges of information among QIOs, CMS regional offices (Boston, Dallas, Kansas City, and Seattle), CMS central office, and two Clinical Data Abstraction Centers (CDACs). It provides all SDPS constituents the same tools, called PROvantage, for performing analysis, data collection, tracking, and reporting. It allows users to share analysis programs and ideas and easily reproduces them in any State, region, or nationally.

3.3.3 Minimum Data Set for Nursing Home Care

The Minimum Data Set (MDS) is a uniform set of elements extracted from the Resident Assessment Instrument (RAI) which is a standardized tool for assessing the functional capacity of residents of long term care facilities and helps nursing home staff identify health problems. Long-term care facilities are required to complete and transmit MDS data to the designated State agency for all residents as a condition of participation in the Medicare and Medicaid programs.

Resident Assessment Protocols (RAPs), are part of this process, and provide the foundation upon which a resident's individual care plan is formulated. MDS assessment forms are completed for all residents in certified nursing homes, regardless of source of payment for the individual resident. MDS assessments are required for residents on admission to the nursing facility and then periodically, within specific guidelines and time frames. MDS information is transmitted electronically by nursing homes to the MDS database in their respective States. MDS information from the State databases is captured into the national MDS database at CMS.

3.3.4 End Stage Renal Disease (ESRD) Network

The End Stage Renal Disease (ESRD) Program was established in 1972 pursuant to the provisions of Section 2991, Public Law 92-603. This legislation extended Medicare coverage to virtually all individuals with ESRD who require dialysis or transplantation to sustain life.

This legislation and subsequent regulations also established health and safety standards applicable to providers of ESRD services and required the establishment of ESRD Network Coordinating Councils. Networks serve as liaisons between the federal government and the providers of ESRD services.

The ESRD Networks provide a cost effective mechanism to ensure the most efficient use of Medicare dollars for dialysis treatment and kidney transplantation through monitoring quality of care indicators and maintaining timely, complete data on the ESRD program. These functions are administered at the regional level, providing direct and immediate access from the treatment provider to the Centers for Medicare and Medicaid Services (CMS through the ESRD Networks

The Renal Beneficiary and Utilization System (REBUS) is the repository for the ESRD program data. It contains data covering the medical and demographic information for the ESRD population. Dialysis

facilities and transplant centers report patient data through the Vital Information System to Improve Outcomes in Nephrology (VISION) to 1 of 18 ESRD Network Organizations. These network organizations are connected to one another and to the REBUS through the Standard Information Management System (SIMS). The 18 Networks are currently in immediate contact with 4,153 dialysis facilities and 242 transplant centers, serving approximately 276,106 patients.

The REBUS is in the process of migration to a new system called the Renal Management Information System (REMIS). CMS is working to build an integrated ESRD system called Consolidated Renal Operations in a Web-Enabled Network (CROWN). This new system will include VISION, SIMS, and REMIS, and will be implemented about June of 2002. CROWN and REBUS will continue to work in parallel until September 30, 2002.

3.3.5 OASIS Home Health Care Data

The Outcome and Assessment Information Set (OASIS) is a group of data elements that represent core items of a comprehensive assessment for an adult home care patient and form the basis for measuring patient outcomes for purposes of outcome-based quality improvement (OBQI). Most data items in the OASIS were derived in the context of a HCFA-funded national research program (co-funded by the Robert Wood Johnson Foundation) to develop a system of outcome measures for home health care. This program, and the OASIS, have evolved over a ten-year developmental period. The core data items were refined through several iterations of clinical and empirical research. Other items were added later by a work group of home care experts to augment the outcome data set with selected items deemed essential for patient assessment. The goal was not to produce a comprehensive assessment instrument, but to provide a set of data items necessary for measuring patient outcomes and essential for assessment - which HHAs in turn could augment as they judge necessary. Overall, the OASIS items have utility for outcome monitoring, clinical assessment, care planning, and other internal agency-level applications.

3.3.6 CMS Medical Restraints

This program was started as part of the FDA-led Hospital Bed Safety Work Group initiatives and to meet the Medicare requirement that institutions must report incidents of harm to patients involving the use of physical and other restraints as a condition of participation in the program. Rather than CMS creating a new event reporting form and process, the FDA offered to accept physical restraint event reports from hospitals/health care facilities via the FDA Mandatory MedWatch Form 3500a. This information is reported through the FDA's MedWatch Program and monitored by CMS.

Beginning in April of 2001, the FDA faxes the received reports to CMS for input into a death reporting log. There is no database for this information at CMS. Each time one of these is reported, CMS sends out a field person (from the regional office) to investigate and make recommendations.

3.3.7 CMS Medicare Patient Safety Monitoring System (MPSMS)

The Medicare Patient Safety Monitoring System (MPSMS) is a medical-records-based system for monitoring the frequency and epidemiology of adverse patient events and the risk factors that contribute to them. The system is currently being designed, and will be operated through the Medicare Peer Review Organization (PRO) program. Alpha testing of the MedQuest extraction tool is scheduled to conclude January 18th of 2002. The beta testing is expected to run through June of 2002 when the actual extraction will begin.

MPSMS uses data abstracted from a nationally representative sample of 60,000 inpatient medical records and from administrative records; thus, it will capture many events not identified by voluntary reporting systems but may miss events that are not documented in the medical record. It will create a national surveillance system with State-level data for some measures. A PRO and the HCFA Clinical Data Abstraction Centers will provide administrative and data collection and analytic support. As appropriate,

CMS will assess needs for risk adjustment or stratification. The goal is to have the system producing national estimates in 2002. Over time, the system will evolve to include new categories of adverse events as well as expand to additional settings across the continuum of care.

3.4 FDA Systems

3.4.1 MedWatch – FDA Medical Products Reporting Program

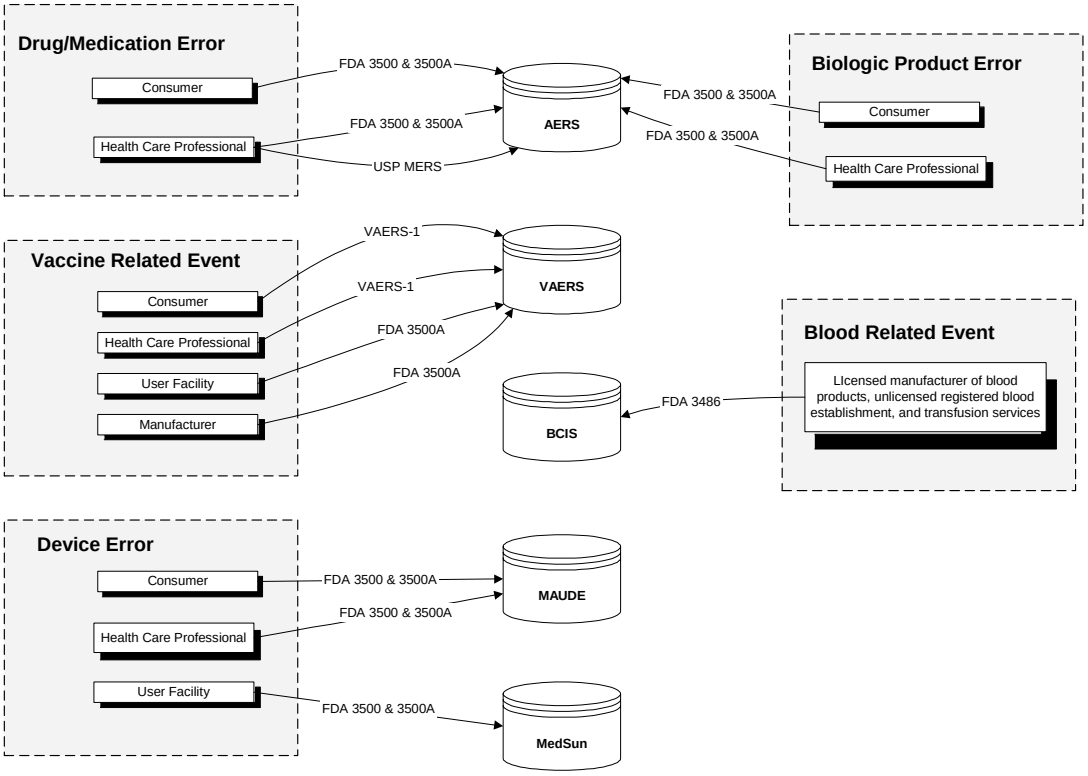
The FDA has the responsibility for assuring the safety and efficacy of all regulated marketed medical products, including: drugs, biologics, medical and radiation-emitting devices, blood products, and special nutritional products (e.g. medical foods, dietary supplements, and infant formulas).

MedWatch is a general term used in FDA publications and on their website to denote both the voluntary and mandatory surveillance programs for reporting proximal adverse events associated with the above products. Through the MedWatch website, users (primarily consumers and health care professionals) can submit voluntary reports of adverse events using an electronic version of FDA Form 3500 (Appendix F). Although encouraged to do so, consumers and health care professionals are not required to submit such reports. Once received through the MedWatch website, a paper version of the form is triaged to the appropriate FDA center (CBER, CDER, CDRH, CFSAN) for evaluation and entry into the respective FDA database (AERS, MAUDE, SNAEMS). See Figure 2 for an overview of the sources and data flow into these databases. Please note that analysis of the SNAEMS database was considered outside the scope of this project.

All analysis and data use by FDA is done from the AERS, MAUDE or Special Nutritionals Adverse Event Monitoring System (SNAEMS) databases. No regular analysis/reports are produced from the MedWatch software. However, MedWatch does send out an email alert to subscribers based upon analysis and review of problems discovered by the various centers. The MedWatch website is a public source of FDA product safety information.

While reporting is voluntary for consumers and health professionals, the FDA imposes specific mandatory adverse event reporting requirements on manufacturers and user facilities. We describe the mandatory portions of the MedWatch program (AERS, MAUDE, Alternative Summary Reporting, MedSun and BPD) in separate sections because each of these programs differs in its methods for input, storage, and reporting of information. Submission of mandatory reports is not currently supported through the MedWatch website.

Figure 5: Overview of FDA Data Submission and Data Flow



3.4.2 Adverse Event Reporting System (AERS)

The Adverse Event Reporting System (AERS) is an information workflow system (including a computerized information database) designed to support the FDA's post-marketing safety surveillance program for all approved drug, therapeutic biologic products and special nutritionals. The ultimate goal of AERS is to improve the public health by providing the best available tools for integrating, storing and analyzing safety reports. Clinical reviewers in the Center for Drug Evaluation and Research (CDER) and the Center for Biologics Evaluation and Research (CBER) evaluate AERS data to identify, serious or unexpected adverse events or an increased incidence of known drug and biologics events. A major function of AERS data is to focus on the immediate post marketing period when surveillance efforts are the most critical to ensure that a product’s labeling information correctly captures the adverse events associated with the product. These data can also be used to re-evaluate an approval decision on an established product.

Drug manufacturers of NDA and ANDA drugs and licensed manufacturers of approved biologic product license applications are required to report adverse experiences to the FDA under 21 CFR 310.305, 314.80, 314.98, and 600.80. U.S. manufacturers either report by submitting FDA Form 3500A (Appendix F) via telephone, direct mail or approved electronic filing using ICH format (discussed in External Factors section). International manufacturers may submit information by sending the CIOMS I form. Reporting may also be done (and is encouraged) on a voluntary basis from health care professionals and consumers through the MedWatch program. All reported adverse event narratives are coded into a standardized international terminology, MedDRA (the Medical Dictionary for Regulatory Activities). AERS also receives input from the USP Medication Errors Reporting Program. The appropriate fields from these forms are entered into AERS and earmarked for analysis by assigning a MedDRA preferred term of “medication error” to the record.

AERS Data Storage team matrix (Appendix B) lists the specifications for the AERS database, which was designed, developed, and is currently maintained by Booz, Allen, and Hamilton. AERS provides for the most integrative processes and storage of all the FDA systems and includes data used by CBER and CDER. AERS accepts data from MERP, CIOMS I, MedWatch, and manufacturers. Safety evaluators primarily use the AERS database to investigate specific reported adverse events. However, they also search using Medline, IMS data, and other databases with FDA cooperative agreements (e.g. Boston University, Harvard Pilgrim Health Cooperative, Johns Hopkins, United Health Group), to conduct wider epidemiological studies, assess risk and evaluate the incidence of a particular event.

3.4.3 Blood Product Deviation Reporting System (BPD)

FDA/CBER is responsible for regulatory oversight of the U.S. blood supply. FDA creates and enforces standards for blood collection and for the manufacturing of blood products, including both transfusible components of whole blood; pharmaceuticals derived from blood cells or plasma, and related medical devices. CBER works with other parts of the Public Health Service (PHS) to establish blood standards, and to identify and respond to potential threats to blood safety or supply. The Biological Product Deviation Reporting system is one method CBER uses to monitor product deviation in manufacturing of products, including testing, processing, packing, labeling, or storage, or with the holding or distribution of a licensed biological product or a blood or a blood component, in which the safety, purity, or potency of a distributed product may be affected.

Licensed manufacturers of all biological products, unlicensed registered blood establishments, and transfusion services are required by 21 CFR 600.15 and 21 CFR 606.171 to report any event associated with biologics, including blood and blood components and source plasma, that represents a deviation in manufacturing to the FDA using an online or paper version of FDA form 3486 (Appendix F). These events include deviations from current good manufacturing practices, applicable regulations, applicable standards, or established specifications that may affect the safety, purity, or potency of a distributed product. In addition, any unexpected or unforeseeable event associated with manufacturing that may affect the safety, purity, or potency of a distributed product must be reported.

Data entry clerks enter hard copy information into the Biologics Compliance Information System (BCIS) database. Manufacturers can enter information directly on the web (currently no user id/password required) via BIODEV interface. This information is stored in the FDA UUNET and transferred to BCIS one time per day. FDA analysts pull up the submitted BIODEV reports to determine whether to accept, reject, or obtain further information from the user. Quarterly and annual summary reports are prepared from accepted data, including the total number of reports submitted to FDA over a period of time categorized by the types of establishments reporting (e.g., licensed and unlicensed blood banks, transfusion services, plasma centers, other non-blood manufacturers), the types of events reported (using a standard coding system) and an analysis of the time frame in which the reports are submitted. Codes used to describe the adverse event are developed by CBER specifically for use in the BPD system. Similarities exist between BIODEV and the Medical Event Reporting System for Transfusion Medicine (MERS-TM). A recent interface feasibility study (Information Management Consultants, 2001) explained the potential for linking these two systems, but noted the difficulty in creating a single portal interface due to varying formats and input rules.

3.4.4 Manufacture and User Data Experience-Medical Devices (MAUDE)

In contrast to voluntary reporting systems, the Medical Device Reporting regulation mandates manufacturers and importers to report significant device related adverse events to the Food and Drug Administration (FDA). These reports are housed in the Manufacture and User Data Experience (MAUDE) database. Following the Safe Medical Device Act amendments, user facilities such as hospitals and nursing homes were also required to report device-related deaths to both the FDA and to manufacturers; however, the bulk of the reports come from manufacturers. Based on the information

collected from these reports, the FDA regulates and assures the safety, effectiveness, and proper labeling of medical and radiation emitting devices by sending out warnings, stopping distribution, and/or recalling devices based on the level of severity of the adverse event.

The regulation that establishes the reporting requirements for medical device reporting, 21 CFR Sec 803, outlines that user facilities, importers and manufacturers must report deaths and serious injuries and that distributors must maintain records of incidents. Reporters must complete FDA Form 3500A and send to the FDA by surface mail, fax or through phone interview. MAUDE is an Oracle based system; additional technical specifications are outlined in Appendix B.

For high priority reports such as pediatric deaths or multiple injuries for one device, the contractor who enters the data (Logistics Applications) alerts The Center for Devices and Radiological Health (CDRH) for evaluation and further action, if indicated. The reports are analyzed by medical professionals (with experience in a specific specialty) based on established criteria related to the seriousness of the event, its unforeseen nature, the vulnerability of the population affected and preventability. The process for entering the information into MAUDE includes quality control procedures and assignment of patient/device/evaluation codes. These codes have been created and are updated by CDRH. MAUDE also contains voluntary reports from consumers and health professionals received through MedWatch. Ad hoc querying and reporting is available.

3.4.5 Alternative Summary Reporting-Medical Devices (ASR)

The Medical Device Alternative Summary Reporting (ASR) offers a risk-based alternative reporting system for those devices where the malfunctions and adverse events are well documented and understood. Alternative reporting allows for reporting using means other than submitting individual reports (for economies of scale and efficiencies) to monitor possible signs of public health safety issues. Manufacturers must be approved to submit to the system. Those products approved for summary reporting require the adverse event data be periodically submitted in a tabular format. While this is a separate database from the MAUDE system, it does access MAUDE for some information. The intent of this system is to reduce the amount of time spent on entering well-documented adverse events into MAUDE, so that the FDA and manufacturers could focus on less well-known or previously undetected events.

The ASR Program was created under the authority of 21 CFR Part 803.19 and is a voluntary system that provides timesavings to the FDA and manufacturers. Each line item submitted represents a separate incident "summarized" by pertinent codes (e.g., patient- and device-related coded outcomes, dates of manufacturer awareness and evaluation) but not text. Coding is consistent with MAUDE. Information captured that relates to the medical device includes model, serial, lot and catalog numbers. ASR is an Oracle based system that is linked to MAUDE via baseline tables. See Appendix B for additional technical specifications. The aims of the software are to support the management of candidate exemptions, manage the receipt and data entry of manufacturer summary reports, manage quality control, collect, sort and perform trending calculations of data from both ASR and MAUDE, and manage data review by: supporting trended data review of variances by pre-set conditions; enabling ad-hoc query and generating preformatted reports.

3.4.6 Medical Product Surveillance Network (MedSun)

The purpose of the Medical Product Surveillance Network (MedSun) is to improve the protection, health and safety of patients, users and others by: reducing the occurrence of medical device related events, serving as an early warning system, improving the frequency and quality of user facility reporting, developing feedback and benchmarking information of reported incidents and promoting the use of aggregated adverse event reports to improve medical facilities' internal quality systems. In addition, the system will provide information on prevention and control of harms to the FDA in their device approval

process. MedSun began in response to the FDA Modernization Act, which specified establishing innovative ways to enhance surveillance reporting in medical device user facilities.

MedSun is designed to collect data, using a modified FDA Form 3500A, from hospitals, nursing homes and other health care facilities required to report under the Safe Medical Devices Act. The pilot phase of implementation includes 50 acute care facilities, with the intention of having a nationally representative sample of facilities, including other health care settings. The long term vision is that this system will replace the mandatory reporting by all user facilities of medical device related deaths and serious injuries. Participating hospitals are required to report adverse events to MedSun, but not to MAUDE. Non-participating hospitals continue to report to MAUDE. The MedSun database is separate from MAUDE, is accessible through the Internet and utilizes Microsoft IIS 5.0 (a web sever) and SQL Server Enterprise. Additional technical information is described in Appendix B. A major focus of the initiative is to create a voluntary, non-punitive reporting system, administered through a third party (contractor is CODA) rather than a regulator. Following the contractor's data review and additional collection if indicated, the FDA has access to the completed reports. Voluntary reports are de-identified, while mandatory reports are not. FDA intends to use the aggregate data to estimate national incidence of adverse events. Note that MedSun uses MedDRA codes whereas MAUDE uses codes developed by CDRH.

3.4.7 Medical Event Reporting System for Transfusion Medicine (MERS-TM)

On November 7, 2000, the U.S. Food and Drug Administration (FDA) published a final rule expanding the requirement for the reporting of errors and accidents in the collection, manufacturing, testing, storage, distribution and administration of blood and blood products. The rule, effective May 7, 2001, requires that hospitals and blood centers maintain a method to report, investigate, and track events that could potentially compromise transfusion safety. American Association of Blood Banks and JCAHO standards also include requirements to create an adverse event reporting system. MERS-TM was implemented in December, 2001 to aid in the collection and analysis of required information. The system is supported by the National Heart, Lung, and Blood Institute, in cooperation with FDA. It is primarily based at Columbia University, with Harold S. Kaplan, MD as the Principal Investigator. Facilities voluntarily participate in MERS-TM.

MERS-TM is oriented toward providing information to facilitate preventive action and a future reduction in transfusion-related adverse events and has some unique features:

- It collects both actual and near-miss events to facilitate process improvement efforts
- It tracks actions taken subsequent to the discovery of the adverse event
- It collects information to support a Root Cause Analysis
- It provides for anonymous reporting by participating facilities

There are three levels of reporting which are designed to be integrated into existing facility QA activities, without undue additional burden. The Event Discovery Report collects information on the discovery of the event and the event itself. The QA Sysop Investigation Report is completed by a trained QA staff member who classifies the event and determines the need for further review based upon a calculated risk assessment index. The Root Cause Analysis report is filled out in those cases where the organization is try to improve processes by identifying the precursors which led up to the event under analysis.

MERS-TM uses Eindhoven Classification coding system for error classification. System-specific codes have been developed to track antecedent and consequent events to support the root cause analysis. MERS-TM also provides sophisticated reporting functionality including its HAWK feature. Each field contained in computerized MERS-TM forms is given a "weight" based on its importance to the process of identifying the closest match. The HAWK software then utilizes "fuzzy" matching technology to identify similar events and to quantify the degree of similarity. By so doing, HAWK helps users assess the significance of a single event report and can prompt expanded investigations.

To support anonymity, each organization's data is stored on in a unique database. Staff at MERS-TM do not have the ability to match each database with the particular reporting organization that supplies the data.

3.5 External Factors

In this section, we describe our findings not associated with a particular data system, but as they related to cross-cutting issues such as nomenclature, classification systems, privacy, and event reporting systems outside the purview of DHHS.

3.5.1 Definitions and Classifications

With respect to the different nomenclatures used by various systems, we found a variety systems in use, virtually none of which are completely compatible. Integration of medical error reporting systems will be meaningful and useful only if certain features among systems (such as terms and definitions of events) are comparable. There are no universally agreed upon definitions for this relatively new field, although the Institute of Medicine is currently engaged in a project to develop standard definitions and classifications that can be used for medical error reporting.

Multiple classification systems exist for adverse medical events and general clinical terms, and these systems have evolved within separate disciplines or fields of study. Consortia have formed around individual classification systems and because of their large investments in maintaining their own system, will likely resist adoption of one clinical classification standard.

The NLM's Universal Medical Language System, a Metathesaurus of 60 clinical language systems, offers tools to developers for translating between different languages, including ICD-9-CM, ICD-10-CM, SNOMED, and MedDRA. However, translations between languages result in a loss of information because there is often no one-to-one match between categories or terms.

Clinical classification systems have evolved for different purposes. Some "controlled-vocabulary" systems (e.g., SNOMED) function as languages to identify preferred terms for concepts, translate between preferred and vernacular terms, but eschew numeric logic, numbering terms sequentially with entry into the system. Other "numerical-hierarchy" systems (e.g., ICD-9-CM) function principally as systems for numeric representation of clinical concepts, limit vocabularies to a fixed set of terms (without synonyms or translations), and maintain a numeric logic. Both functions are key to the coding of narrative descriptions (necessary in medical error reporting) and to efficient information retrieval.

Several key clinical classification systems are proprietary for purposes of maintaining them (e.g., MedDRA and SNOMED), and we were unable to view them completely. Proprietary fees for using classification systems will burden health care providers and may impede reporting.

Moreover, “open” standards exist but remain largely untapped. The patient safety community has not been involved in accredited standard setting. ASTM and HL7 are willing to develop standards for patient safety and are recruiting experts.

The National Center for Health Statistics, responsible for maintaining and updating the ICD-CM coding systems in the U.S. for diagnostic classification has not received proposals related to medical error reporting for improving ICD-9-CM and ICD-10-CM. Proposals can now be incorporated into the ICD-9-CM coding system within a year of submission, on October 1 of the following year.

Finally, HIPAA standards are relevant for some fields used for medical event reporting (e.g., dates, gender, race, marital status, etc.) and should be used wherever possible.

3.5.2 Error Reporting Systems Outside of DHHS

Although existing DHHS systems are the primary focus of this report, there may be important lessons to be learned from non-DHHS systems.

Error reporting systems are being adopted by many individual hospitals and hospital systems either by developing their own systems through Intranets or subscribing to proprietary Internet-based reporting system (e.g., MedMARx, UHC, DoctorQuality). Some current or developing hospital-based error reporting systems are comprehensive and cover all types of errors that can occur in the hospital (e.g., VA, UHC). While some hospital-based systems adopt definitions and classifications of errors that exist (e.g., NCCMERP), many modify them, leading to the divergence, not convergence, of data collection.

Several States now mandate hospitals to report certain types of medical errors. These State systems define sentinel events differently, usually focus on catastrophic events, classify errors differently, and have different views about the culture of blame in medical care and the role of the State.

Some error reporting systems outside DHHS have developed for specific types of errors, such as MedMARx for medication errors and ECRI's system for reporting medical device problems. These systems are more detailed in their specific area than are systems that collect data on all types of medical events.

3.5.3 Lessons from Other Countries

Several other countries have started patient safety programs in recent years. Most are in their infancy as in the United States. While patient safety systems in other countries fit different health care and accountability models and while there may not yet be an existing framework in these countries that can be copied, we feel it is important to maintain a dialog with users, analysts, and system designers who work on related systems in other countries.

3.5.4 Privacy

A major barrier to sharing data on medical errors is legal protection of such data from discovery through the Federal and State court systems.

Currently there is a patchwork of privacy laws and regulations that do not fully prevent the legal discovery of information routinely collected on medical errors in the private sector. This contributes to the development of private systems that avoid data identifying patients or institutions reporting the error.

The Federal Privacy Act of 1974 and the Common Rule governing research on human subjects are considered shields that protect some types of personally identified health information from discovery in court. The Federal Privacy Act applies only to data collected by the Federal government. The Common Rule applies only to data collected on human subjects under Federally funded research.

Some States (e.g. Georgia) have strong laws to protect data systems developed and used for peer-review and quality improvement - known as "peer review" laws. However, these laws often apply only to data collected and maintained within the walls of the peer-review committee meeting and they are by no means equally effective across all States.

The HIPAA Privacy Rule strengthens the privacy of personally identified data from the patient's perspective and applies to all organizations that hold personally identifiable health information (PIHI). However, the rule does permit plaintiffs and defendants to obtain PIHI through court order and law enforcement officers to obtain information through warrants.

The HIPAA privacy restrictions on sharing of PIHI have led health care organizations to question whether medical error reports on identified patients can be shared outside their organizations. In general, PIHI cannot be shared outside the institution except for certain purposes - for research purposes, for public health activities (e.g., preventing or controlling injury or disability), and for activities under FDA

jurisdiction (e.g., reporting adverse events with respect to food and medical product problems). Legal liability is the primary factor identified by health care providers in their reluctance to share information on medical errors.

For these reasons, the 107th Congress will be considering legislation, recently introduced, to protect voluntary reporting systems from discovery through the legal system.

3.6 Overall Findings and Implications for Integration

This section describes our general findings across teams and data system, with special emphasis on how these findings relate to the potential integration of these data systems.

3.6.1 Findings

Our most striking finding was the diversity of systems – measured in almost every dimension. While much of this was anticipated because the systems evolved for different purposes, in some cases the magnitude of the difference was surprising.

Purpose. Our review of more than 30 systems related to patient safety found that the systems exist, and data are collected, to meet a wide variety of needs. In some cases systems exist solely to collect information related to adverse events or error (e.g., AERS) whereas others represent administrative data systems (e.g., HCUP, Medicare/Medicaid) that collect information that could be used to examine issues related to patient safety. Some systems are designed around the "active" collection of event information (e.g., a consumer or health care professional takes steps to report an event), whereas others are designed to passively collect information, either through analysis of claims data (e.g., HCUP) or existing medical records (e.g., MPSMS).

These data are drawn from a variety of systems, including administrative sources, anonymous individuals, non-anonymous individuals, and in the future systems may collect information directly from laboratory equipment, as is anticipated with the NHSN.

Scale. Not unexpectedly, the volume of data processed by each system varies tremendously. At one extreme, CMS's Medical Restraint monitoring program receives approximately one record per month, whereas the Medicare/Medicaid data systems process at least one terabyte of data per year. Data storage formats vary accordingly, and range from hard copy (Medical Restraints) to high-end relational databases.

Excluding these extremes, most systems collect tens of thousands of records per year, and store these records in modern relational or object-oriented databases. From a technical perspective, a variety of mechanisms exist to link information from these disparate systems, and tools exist to allow data to be extracted anywhere from once per hour to once a quarter or year. Although this capability is a necessary condition for integration, the disparate data structures of each system pose a significant challenge to integration

Structure. Taken together, the DHHS data systems represent a wide variety of patient safety issues and concerns, ranging from consumer-reported adverse drug reactions to facility-reported occurrences of hospital-acquired infections. While it is appropriate to cover this spectrum of events, the structure and format of the various data systems reflect this diversity, and do not facilitate linking information across systems. Key issues include differences in coding schemes between systems, within systems over time, and differences in the type of information collected by various systems. For instance, some systems (FDA's BPD) update their coding scheme each year, which makes year-to-year comparisons more difficult. Some systems require patient identifiers, whereas others discourage (or even do not allow) collection of patient identifiers. Although both approaches are justified and have their own rationale, the unavailability of patient identifiers across systems makes it difficult or impossible to link records to remove duplicates of reports for the same patient and to conduct certain epidemiological and other

analyses, the results of which may ultimately improve patient care. The same case could be made for the presence/absence of facility-specific information, location, and a host of other key data elements.

Similarly, a number of different coding and classification schemes are used across the various systems, and include widely used (e.g., ICD-9-CM) to proprietary and type-specific (e.g., MedDRA). Here again, the use of any given nomenclature is no doubt appropriate within a given domain, but the lack of consistency across systems prohibits (or at least does not facilitate) analyses that may ultimately prove useful. While we do not expect a single "universal" nomenclature to exist or even to be appropriate, it would almost certainly be beneficial to reduce the number of nomenclatures so that information could be more easily mapped from one system to another.

Barriers. Although we were aware of the sensitive nature of medical event/adverse event information, we did not anticipate the extent to which this permeates every aspect of system functioning, including data collection, storage, and analysis. Design options range from "protective" (e.g., CMS) to "agnostic" (e.g., FDA). Some of the more clever and exotic architectures (MERS-TM) not only collect data anonymously, but allow system administrators and analysts to communicate with facilities "anonymously" through a "chat room" type configuration. Other systems simply collect anonymous data and do not attempt to identify either the person reporting the event or the person/facility associated with the event. Legal and regulatory protections could help overcome these barriers, as would a change in "culture" so that persons with knowledge of an adverse event would not fear reprisals should they pass that knowledge on.

3.6.2 Implications

Each of the findings outlined above have consequences for building an integrated collection/reporting/analysis system. Where possible, we provide options and alternative that should facilitate integration.

Purpose. Every system we investigated has a bona fide reason to exist. In some cases, these reasons are directly related to patient safety (e.g., AERS, NHSN, MPSMS) whereas other systems would exist whether or not safety was a concern (e.g., Medicare). The most efficient approach is likely one which identifies those systems which fulfill similar missions, and examine integration options and possibilities for those sets of systems.

Scale. Clearly, some systems are orders of magnitude more involved than other systems. Although this may seem problematic, it actually helps narrow the field of candidate systems by eliminating the larger, production systems and considering only the relatively small systems such as NHSN, MedSun, AERS. While high volume data systems will certainly play a role in the evolution of any integrated system, we feel it is unlikely they are the best candidates for early integration.

Structure. Somewhat akin to the scale issue, the path of least resistance is to integrate data systems with similar structures. Unfortunately, this is not necessarily the path of greatest value. For instance it would be relatively easy to develop a data warehouse that would include the various systems based on the FDA Form 3500*x*. However, this would not necessarily improve our understanding of the patient safety environment.

It would almost certainly be more useful to combine various aspects of information (e.g., medication adverse events, cost of care) for the same individuals and examine patterns and trends. Such and effort would require some effort to expand data collection efforts such that additional patient data was collected on medication and device reporting forms. Likewise, it would be important to allow medication and device adverse events to be reported on other forms, and allow for a common identifier across systems. This has implications for privacy and confidentiality, which are discussed in detail below.

Barriers. We believe that it is in the best interests of the nation to pass "peer review" legislation similar to that recommended by the IOM (Recommendation 6.1) in *To Err is Human* to protect adverse event

information from discovery. However, this could take some time to accomplish and even longer to implement. In the mean time, a set of other measures are worth considering.

Submitting data to a third party seems to have a positive effect, as is the case with the FDA's MedSun system and the FAA's ASRS system. In the case of an integrated reporting system, data could be submitted either to an "independent" agency (e.g., AHRQ) or a third party such as a contractor or other independent entity. The intermediary could either act as a neutral conduit of information, or de-identify the data and forward information to the appropriate destination (as is done with MedSun). Other alternatives include developing more elaborate data collection schemes, similar to MERS-TM or to collecting data that are entirely anonymous.

Definitions and Classifications. Unanimity on classification systems will be very difficult to resolve because of consortia invested in and promoting individual systems. The IOM, in its investigation of standards for classification, should examine in depth the relevance of at least five systems to medical error reporting, the relationships among these systems, and schemes for integration of them: ICD-9-CM, ICD-10-CM, SNOMED, MedDRA, and Medcin.

Work by the IOM under contract to AHRQ aims to move the field toward unanimity on definitions; that work will be completed by October 2003. Definitive guidance from the IOM on what the standards should be for definitions and for classifications would facilitate integration of patient safety systems.

To integrate medical event reporting systems effectively, integration of "controlled-vocabulary" and "numerical-hierarchy" systems would be ideal. Either vocabulary-type systems should invest in logical numerical coding auxiliary to their fixed, unchanging sequential numbering, or numerical systems should invest in translations of medical terms to their fixed terminology.

The Universal Medical Language System (and other systems) should be explored for their potential to map between alternative classification systems. These "translation engines" could sit unobtrusively behind data collection systems and data warehouses for communicating between different DHHS systems.

In order to make ICD-9-CM and ICD-10-CM helpful for medical error reporting in the U.S., AHRQ should lead an effort to propose revisions to them for adverse medical events that span all of types of errors that can occur in hospitals. And, where possible, event reporting systems should comply with HIPAA standards for relevant data elements.

Error Reporting Systems Outside of DHHS. These systems should be studied in more detail as models or bases for hospital-based DHHS integration. They might be useful tests sites for external system linkages to an integrated DHHS reporting system.

DHHS should place establishment of standards for medical error reporting as a high priority to facilitate the convergence of private information systems related to medical errors. Also, the emergence of Web-based systems makes nationwide integration as a long-run vision more feasible.

To reduce the burden on hospital systems that must report errors across States, the National Quality Forum has developed a core, uniform data set for adverse medical event reporting to States. Further work is needed to compare, contrast, and modify State reporting system definitions.

To encourage reporting at the State level, legal protections and anonymity of these data must be addressed. To achieve quality improvement through State reporting systems, the consequence of reporting must be clearly specified and the culture of blame changed.

Lessons from Other Countries. These systems should be monitored for lessons that they might offer the United States. Information such as the extent and cost of errors should be compared to the U.S. figures as reporting becomes better.

Privacy. To encourage reporting, data sharing and learning, a solution to the privacy problem for medical event reporting must be found. At present, adverse medical event reporting as part of a research project and Federally collected data are protected from discovery in court. The HIPAA Privacy Rule does not fully protect medical error reporting from legal discovery. However, the current rule does allow health care organizations to share PIHI related to medical error with the FDA, CDC, and bona-fide research projects without the fear of legally required disclosure. However, medical errors collected for operational activities by private entities and shared outside the organization (as noted below) are not protected from legal discovery. The 107th Congress can spur learning from medical errors by passing the Patient Safety and Quality Improvement Acts currently before the Senate and House.

4 External Factors

Although the focus of this project is integration of DHHS data systems related to adverse medical events, this effort will necessarily be shaped by a number of factors external to the PSTF agencies. The most important of these factors are:

- Existing and emerging standards for definitions, vocabularies, and coding systems
- Laws, regulations and mandates
- Systems that exist outside the PSTF, in other agencies, other countries and the private sector

This chapter reviews information related to all of these areas. Some findings show that considerable infrastructure has been built that will be highly useful for DHHS integration. Some findings show disarray and weaknesses that must be addressed as DHHS and other organizations move forward with medical event reporting integration.

4.1 Standards

The adoption of pervasive standards will increase the benefits of medical error reporting integration. The gradual emergence of content standards for definitions, clinical terminology and classifications of errors, near misses, circumstances and settings surrounding events will facilitate integration and the derivation of useful information from integrated systems. Unfortunately, few standards currently exist within this relatively new field of research. Consequently, medical error reporting systems have evolved without the benefit of supporting standards and each has created its own definitions, categories and labels. A growing list of patient safety publications may eventually converge on common definitions, but overwhelming heterogeneity of terms, definitions and categories for error events currently marks the field.

Existing systems of clinical classification are highly diverse. They differ not only in the breadth and specificity of vocabulary, but more significantly on the focus of underlying concepts. Some schemes classify diseases causing death and morbidity (e.g., ICD-9-CM), others classify outcomes of adverse reactions (e.g., MedDRA), while others (e.g., SNOMED) attempt to span the full vocabulary of medicine including diagnosis, treatment, prognosis, outcome, and social aspects. A standard comprehensive vocabulary is crucial at the point of care so that clinicians can minimize the number of classification schemes they must master to code and convey information. For example, MedDRA combines diagnoses, signs and symptoms, treatments, and adverse drug events to facilitate communication regarding drug manufacturing and regulation. In this spirit, several organizations are investigating ways to modify their current systems to include more terms related to medical errors.

The challenge of integration will be to resolve these differing approaches so that information collected across different event domains (e.g., across surgery, nursing interventions and drug treatment) can be combined and compared. This effort must go far beyond the four PSTF agencies. While the PSTF might agree on standards among themselves, an insular approach could be counter-productive to the long-term vision of broad integration. To encourage other organizations to model their systems on an integrated four-agency system, consideration will have to be given the to the many definitions and data classification standards in use at other public and private systems.

The PSTF will need to monitor and capitalize on efforts that are currently underway. The Institute of Medicine with support of AHRQ is developing “a detailed plan to facilitate the development of data standards applicable to the collection, coding and classification of patient safety information,” including both adverse event data and errors data (IOM, 2002). Experience has proven that an open standards development process (as opposed to closed, proprietary or mandated standards) is the key to broad acceptance. The American National Standards Institute (ANSI) fosters open processes through consensus building, but the tedious pace of that process may delay decisions needed for timely DHHS integration. Ongoing Federal participation in standards development will be required to achieve the vision of nationwide integration of medical event reporting.

Developing and issuing standards is only the first step towards their adoption and widespread use. The effort may, in many cases, require training, review of coding procedures, and consultation on use. Feedback to standard setters for updates and modifications is crucial, as systems created in the abstract do not always apply well in practice. For this reason, standard setting and classification maintenance must be ongoing. Developmental work for MedSun, which aims to integrate reporting for medical device defects, used focus groups to explore barriers to reporting. Two prominent concerns were lack of feedback from the reporting system and the burden of using the FDA coding system (Gardner & Flack, 1999). A paramount concern of institutions is that the information reported will be used beyond the intended safety purposes and instead will be used to promote lawsuits. Understanding why a standard is not being adopted or used properly may require research. A survey of users can be an effective way to uncover problems and test solutions.

The following sections on standards cover three areas:

- The standard setting process in the U.S. and internationally and the extent of ongoing standard setting activities.
- The definitions of errors and related concepts assembled by other organizations,
- The most promising candidates for classifications related to medical error reporting.

While the scope of the information we present on standards is broad, it is by no means exhaustive and it is likely that other relevant standards systems exist, particularly in the sub-specialties of medical practice, that are not well known. Appendix A lists the definitions and Appendix G lists classification systems that we found.

4.1.1 The Standard Setting Environment

Numerous organizations, public and private, national and international, are involved in or promote the development and adoption of standards for health care data, and these organizations argue that health care information systems cannot be built without uniform data elements. In the United States, the Health Insurance Portability and Accountability Act of 1996 (HIPAA) mandated the DHHS to develop national standards for electronic transactions between health care providers and third-party payers for submission and payment of health care expenses. This U.S. law was the first mandate for national health data standards in the U.S. It also mandates development of standards for the computer-based patient record.

Prior to HIPAA, standards of various types were developed and adopted voluntarily from international organizations, such as the World Health Organization (WHO) and the International Conference on Harmonization of Technical Requirements for the Registration of Pharmaceuticals for Human Use (also known as the ICH, which is an entity of the International Federation of Pharmaceutical Manufacturers Association). WHO has promoted the *International Classification of Disease* for classifying causes of mortality, which was adapted in the U.S. and elsewhere for classifying morbidity and health care. ICH has promoted the Medical Dictionary for Regulatory Activity (MedDRA), which was developed for international communications on drug development and related regulatory activity, including safety monitoring. More generally, the International Organization for Standardization (ISO) accredits organizations to establish standards for products, message formats, and knowledge content in many domains, one of which is health. A related organization in the United States is the American National Standards Institute is the organization with the authority to create U.S. national standards using the open or consensus process. ANSI is the U.S. representative to ISO. In many cases, ANSI also is the pathway for U.S. national standards to become ISO standards. ANSI is the secretariat for several ISO technical committees (ISO TC). For example, ANSI is the secretariat for ISO TC 215, Health Informatics (Hammond, 2002).

In addition to international activity, national standard setting organizations in many countries develop message format and content standards for health data and products. In the U.S., the American National Standards Institute (ANSI) accredits other organizations to develop standards, requiring them to follow

rules, including open processes and consensus building for standard setting. Those organizations are voluntary groups of industry experts (usually private but increasingly public) who have a business need for standards. ANSI balloting rules require the number of non-vendor voters (including providers, consultants, governments, payers, and pharmacies, for example) casting ballots to exceed the number of vendor members casting ballots.

ANSI recognizes three pathways for ANSI-approved American National Standards (Hammond, 2002). The first is when ANSI recognizes the need for a standard or set of standards and does not see a standards body doing the work to develop a standard in that area. In this case, ANSI creates an accredited body to develop a standard; ANSI ASC X12 is such a body. The second pathway is when an existing standards development organization (SDO) applies to ANSI for accreditation. If that organization meets ANSI requirements, then that organization becomes an ANSI Accredited Standards Organization (ASO); HL7 is such an organization. The third process is the canvas method, whereby an organization submits a standard to ANSI for approval and the proposed standard is then aired for comment. If no objections occur, the standard is approved as a national standard. (ASTM E31 submits its standards as part of a canvas process.) Methods one and two require a much more rigid approval process.

Because business needs are diverse and consensus is required for an ANSI-approved standard, standard setting organizations at a minimum develop standards for the message format (or envelopes) for the data and may permit individual trading partners to define the content. In other situations, standard setting organizations are defining standards for products and their interoperability (or the ability of one product to connect to or communicate with other products). Standard setting organizations and coordinating bodies for health products and data in the U.S. include:

- Institute of Electrical and Electronics Engineers (IEEE) for standards on bed-side computers and medical devices;
- American Society for Testing and Materials (ASTM) for laboratories and physiological monitors;
- Health Level Seven (HL-7) for clinical content and knowledge bases (tables, software, tools for care processes and for specific hospital departments, such as pharmacies and radiology departments);
- Digital Imaging and Communication in Medicine (DICOM) for radiological imaging;
- Health Informatics Standards Board (HISB), created to promote harmonization among SDOs in the U.S. and one of its early projects was identifying potential standards for HIPAA;
- American Standards Committee X12N (ASC X12N) for billing;
- National Council on Prescription Drug Programs (NCPDP) for retail pharmacy billing.

To understand the complexity of the standards setting world, it is important to realize that ANSI-accredited standard setting organizations are not the only organizations setting standards in health care. For example, while the ASC X12N develops standards for insurance claim transactions, historically in the U.S. other consortia such as the National Council for Prescription Drug Programs (NCPDP) for retail pharmacy bills, the National Uniform Billing Committee (NUBC) for hospital bills, and the National Uniform Claim Committee (NUCC) for outpatient bills, developed standards for their domains.

The National Committee on Vital and Health Statistics (NCVHS) was instrumental in studying and promoting the consolidation of standards setting activities in the U.S. in their role as advisors on the implementation of HIPAA. The NCVHS, which is an appointed advisory group to the U.S. Secretary of Health and Human Services, held hearings and invited related organizations to present their processes and proposed role in HIPAA standards activities. NCVHS produced several reports reviewing and recommending public-private standard setting processes for HIPAA (NCVHS 2000, 2001). In their report on *Uniform Standards for Patient Medical Record Information*, the NCVHS recommended that any additional U.S. standard setting activities be compliant with existing HIPAA standards (NCVHS 2000). This is a recommendation that should be heeded for setting standards for medical error reporting, as well.

The standards required for total interoperability in health care are many and varied, including clinical, administrative, reimbursement, reporting, quality, and audit standards (Hammond, 2002). For example, HL7 initially focused on the standards for interchange of clinical data and on the inpatient setting. The most popular and highest volume events – test orders and results – drove standards for trigger events, message types, segment types, and data types. Segments included:

- Message header -- sender and receiver, trigger event, and date/time;
- Data about the patient;
- Location and providers involved;
- Order; and
- Result.

Rather than trying to define explicitly every data element that could be used in and exchanged among institutions – a nearly impossible task – HL7 specifies classes of information to be exchanged and identifies, as far as possible, terminologies to be used (Hammond, 2002). For example, the "result" segment is essentially a name-value pair that can be used to send anything. The messaging structure of HL7 accommodates requirements of special data categories. For example, medications and diets have a more complex structure than laboratory orders and results. HL7 formats have been used for many years to exchange complete electronic health records – laboratory, medication, history, physical, and diagnosis information. Conformance agreements among business partners will always be required in health care because of the complexity of the diagnosis, treatment, and management processes. In some cases, definitions may be feasible on a national level (or even internationally). For example, one third-party payment specification with structured and pre-defined data elements is being implemented as a standard for the entire United States.

Because medical event reporting has elements of both complicated clinical observation and simple classification of errors that can be pre-specified, both open segments and pre-defined segments will be necessary in developing an integrated medical event reporting system for USDHHS. In particular, the unknown root cause factors that reporting systems will aim to capture will require open narrative data collection that cannot be pre-specified. Nevertheless, as many components as possible should be defined explicitly to insure interoperability among error reporting systems of institutions and between providers and patient safety experts.

A traditional role of standard setting organizations such as HL7 and X12N has involved development of transmission standards or message formats and in some instances segments or structures for specific clinical components such as medications, diagnoses, and laboratory data. HL7 specifies name-value pairs such as the diagnosis coding system (SNOMED or ICD-9-CM) and the code value for that coding system. It does not necessarily define one standard for diagnosis coding. Many standard setting organizations, especially those representing private business interests, have focused on the envelope and the order of data items, rather than restricting health data content, allowing business partners to define the content. While this solution facilitates trading of information, it is not a solution for standard content when the objective is to compare and analyze data from multiple information systems. When the content is not defined as part of the standard, the result is non-standard information contained in standard envelopes and standard ordering of information. This was an issue that DHHS had to tackle for HIPAA standards. The well-defined, ANSI-approved segments can contain non-standard codes sets. DHHS had to select and set permissible code sets for HIPAA-standards compliance. Without content standards in medical event reporting systems, it will be more difficult to compare information from different systems.

Keeping in mind the NCVHS recommendation to comply with HIPAA standards, consideration should be given to establishing medical error reporting standards under HIPAA rubrics and with ANSI-approved organizations. The advantage of "open standards" developed in an ANSI-appproved environment is that an industry consensus on standards will be set, better standards are likely to result, and data elements will conform to data collected for other purposes, such as claims processing and medical records, making

meaningful linkages feasible. Another advantage is that the knowledge of informatics experts can be brought to bear on classification and coding for medical error reporting. The disadvantage is that the process of obtaining consensus is very slow and substantial overhauls of medical error reporting systems are likely to be necessary to conform to HIPAA and/or ANSI-approved standards.

In any event, at least three components of the specific HIPAA standards related to claim reimbursement are relevant to medical error reporting:

- First, data elements that already have a HIPAA-standard format should be considered for revision in medical event reporting systems. Appendix H lists the obvious candidates based on the HIPAA coding standard. They include dates, gender, race/ethnicity, marital status, and a few other demographic attributes. (Note: Collection of some of these data elements would require patient authorization, according to the current HIPPA Privacy Rule (45 CRF §164.512(h) (2000); although that may change if proposed revisions to the rule currently released for public comment take effect.)
- Second, codes sets that DHHS designated HIPAA compliant should be considered standards in medical error reporting systems. These include ICD-9-CM and eventually ICD-10-CM. The top candidates for clinical language in computer-based patient records (currently SNOMED CT) should be considered for use in error reporting systems. This is a contentious area given the continuous investments and modifications of alternative vocabularies used for medical error reporting.
- Third, HL7, CMS and ASC X12N are devising claims attachment forms that will accommodate narrative text and auxiliary information needed to investigate and coordinate standard claims (HCFA, 2001). Claims attachments could be used to capture other types of data, including medical error narratives. The advantage of this approach is consensus around the message format and labeling of non-standard content. (Again the privacy rule would require patient authorization to collect data for one purpose and to use it for another.)

We know from our inquiry of ANSI-approved standard setting organizations (such as ASTM and HL7) that they do not currently have established or approved standards that would apply generally to patient safety and error reporting. HL7 (through it's Medication and Pharmacy Special Interest Group and the Vocabulary Technical Committee) has developed a data model for clinical drugs to simplify identification of potential drug-drug interactions. The clinical drug model separated drug, route, form, and administration device into structured coded forms. Both active and inactive ingredients are defined. However, ASTM is planning to develop standards for patient safety and is anxious to recruit and involve leaders of medical error reporting systems in their standards development process.

4.1.2 Standardized Terminology

Standard terminology for patient safety concepts is an essential foundation for data system integration. For example, should reportable medical events include adverse drug reactions, which may or may not be caused by medical error? The drug reaction could result from inappropriate prescribing or unknown patient allergies. Clearly, for a USDHHS integration of existing systems that include addressing regulatory requirements of the FDA, such events should be included. Also, for purposes of understanding root causes of error (which might include omitted steps to ascertain data on patient allergies), such events should be included. These are the types of issues that must be addressed in establishing definitions for medical event reporting systems.

Appendix A contains a list of terms obtained from the National Patient Safety Foundation and augmented with definitions found in reports and online resources of major organizations in the patient safety movement. These include the National Quality Forum (NQF), the Joint Commission on Accreditation of Healthcare Organizations (JCAHO), the Quality Interagency Coordination (QuIC) Task Force, Veterans Affairs' National Center for Patient Safety, the Institute of Medicine, Columbia University, the American Society of Health-System Pharmacists (ASHP), and the American Medical Association (AMA).

In addition, the NQF has developed a list of 27 serious adverse events that are largely preventable and recommends that they be reported through State medical error reporting systems (NQF, undated). JCAHO also has a list of 18 reportable events (overlapping on 13 events with the NQF) for which they require institutions to notify JCAHO when such events occur, to study the root cause, and report the results within 45 days. It is useful to examine these adverse events and determine whether the USDHHS systems will support such surveillance and where the gaps in data exist.

Appendix I lists the 31 NQF and JCAHO serious reportable events and identifies which USDHHS reporting systems might contain information related to those adverse events. This assessment results from a high-level review of the systems and requires more study to determine what specific related data might be available. For 21 of the NQF/JCAHO serious reportable events, there is some type of relevant data in USDHHS systems. For 17 events, multiple USDHHS systems may provide information. Only 9 of the 31 events could not be addressed by any of the USDHHS systems; these relate to surgery errors, criminal events, and delay of care. Some State collects information related to 19 of the NQF/JCAHO serious reportable events. Multiple States collect data for 16 of the events. Twelve of the NQR/JCAHO events are not collected by any of the States examined. These are serious events related to hypoglycemia, hyperbilirubinemia, perinatality, pressure ulcers, and spinal manipulation. Eleven of the events are addressed by both USDHHS systems and State systems. Despite some overlap between USDHHS and State systems related to these events, definitions are likely to vary enough to make comparisons problematic.

The value of the NQF effort to develop such definitions is that they have the potential to standardize reporting across systems. The NQF specifically had this in mind for State reporting systems. The reportable events were developed through a consensus process of patient safety and clinical experts.

4.2 Standard Data Model

In order to integrate various reporting systems effectively, follow-on activities to this project will need to develop a data model of the common (or perhaps the ideal) data elements for medical event reporting and will need to ask important questions. Are these elements normally available in the existing data sets or are they new elements that must be collected? For example, how will near miss events be captured in a national system of reporting, if an adverse event did not occur? What is the total set of elements reported in existing systems? Such an assessment would reveal what could be combined and what would need to be added.

Another way to assess the existing data systems is to compare them to standard data models in medical informatics. To facilitate development of electronic medical records of all types, HL7 has developed a model for structuring records in a generalized way that can be applied to many types of medical records (HL7, 2002). The HL7 Reference Information Model (RIM) is currently under review of the standard setting organization. The structure includes classifications of entities, roles, actions (clinical and financial), and document infrastructure. The components of each of these are summarized in Appendix J. For each component of the model, data element names are specified, although code sets are not. A schematic, called the RIM Billboard for Version 1.15, is available from HL7.

A data model for an integrated medical event reporting system should be evaluated against the RIM and HL7 should be consulted about any modifications that might be necessary to accommodate medical event reporting. To evaluate a data model against the RIM, alternative scenarios should be developed for various types of reporting. For example, how would hospital-acquired infections versus adverse drug reactions versus drug administration error fit a data model for medical events?

4.2.1 Existing Classification Systems

To locate existing classification systems applicable to medical error reporting, we started with documents used for determining HIPAA standards. The Health Informatics Standards Board assembled such a list in

1996 and the National Library of Medicine maintains the Universal Medical Language System (UMLS), a growing metathesaurus of common terms among medical languages. In addition, the literature on adverse medical events revealed related classification systems. Appendix G contains the list of classification systems reviewed for this report.

Data elements relevant for medical error reporting cover a broad range. However, two main types of classifications are specific to error reports – clinical language and specific error classes – and these are discussed in detail here. Other data collected in error reports (e.g., birth date, gender, race/ethnicity, marital status, and education) are more commonly collected for other purposes and HIPAA standards exist for these.

Clinical language classification systems are essential for classifying the clinical context of medical events in a form that is usable and understandable by computers. Systems of reporting based on uncontrolled natural language find it impossible to extract effective and usable information and knowledge, because natural clinical language is inconsistent and riddled with inconsistent abbreviations, unclear statements, and poor grammar. Even something as straightforward as the chief complaint of the patient defies understanding by computers (Hammond, 2002).

Clinical language systems can be used to improve narrative descriptions of the medical event and the clinical context of the event. Such systems have evolved in two main forms:

- *Hierarchies of words*, keywords, or preferred terms that reporters can use to describe events or that analyzers of reports can use to recode the event descriptions when they are written in natural, uncontrolled clinical language.
- *Hierarchies of words and numeric codes* for codifying the clinical description so that electronic analysis and grouping can be performed more easily. These are frequently used for the underlying diagnosis (and severity of illness) of the patient, treatment of the patient (procedure, drug, or device codes), and outcomes of the treatment or adverse event.

Errors and adverse events are classified in many different sets of categories. Those that describe the event are detailed and segregated by type of adverse event – drug, device, biologic, surgery, or nursing. Those that capture the circumstances surrounding the event (the who, where, when) and the cause of error (rather than the manifestation of the event) are streamlined, general lists (e.g., root causes of error). We start with the general clinical languages and then discuss error classification more specifically. We have focused on drug classifications but note other classifications that need to be explored to develop an integrated reporting system across fields of study.

4.2.2 Clinical Language Systems

Obtaining consensus on a common clinical vocabulary will be one of the most challenging tasks of adverse medical event reporting integration. There is a plethora of clinical language classification systems in use and possible as standards for clinical circumstances related to adverse medical events. Furthermore, current stakeholders such as pharmaceutical manufacturers have extensive investments in classifications developed for specific purposes such as meeting pre-marketing and post-marketing regulatory requirements for drug safety. Competing classifications entrenched in different fields may make development of a consensus on clinical classification difficult to achieve.

Specialists in medical informatics have reviewed and compared clinical vocabularies. We reviewed a few of those that focused on the clinical classifications relevant for medical error reporting and note them below. Furthermore, the National Library of Medicine has developed the Unified Medical Language System, a Metathesaurus® (NLM, 2002), which is an ongoing project to provide cross-mappings between clinical languages (among other information sources). It is a tool for system and software developers who must integrate information from multiple systems that are based on different biomedical languages. To facilitate this work, UMLS links the concepts, terms, and attributes of different vocabularies and

maintains relationships defined within those systems. The Metathesaurus 2002 contains 777,000 concepts, 2.10 million concept names, and over 11 million relationships in more than 60 different vocabularies. The UMLS is described further in Appendix K. The current version of the UMLS accommodates the three languages described below.

We cannot review here all clinical classification systems available and evaluate their usefulness for codifying medical events. However, we do describe the systems that appear to be the major contenders for clinical classification of the patient's condition and treatment. We also describe the internationally accepted language for pharmaceutical manufacturing and regulation because it is the apparent standard for clinical language of adverse drug reactions. About 300,000 adverse drug events are reported to the FDA annually and increasingly they are reported electronically (FDA TF, 1999). In addition, a relatively unknown system, Medcin, developed over the last 34 years by practicing physicians should also be evaluated as a clinical nomenclature for adverse event reporting because of its broad applicability and efficient use features.

4.2.2.1 International Classifications of Diseases and Its Modifications

ICD-9 and ICD-10 are hierarchical categories and organized numeric coding schemes for clinical descriptions of diseases, developed by the World Health Organization and used for classifying mortality throughout the world. They are parent systems of adaptations that are made by countries. The United States developed the ICD-9-CM, which has been used for many years to code causes of death and claims for medical reimbursement. ICD-9-CM is the HIPAA standard for clinical classifications on transactions between health plans and providers. ICD-10-CM is also under development for these purposes. Joint responsibility for the modification lies with the NCHS, which leads the condition and external cause classification, and CMS, which leads the procedure classification. ICD-9-CM includes over 10,000 diagnosis and 7,000 procedure codes. It is freely available and updated annually.

ICD-10 and ICD-10-CM have not yet been implemented in the US, but have been updated for content and format. It is difficult to determine the extent of changes in the ICD-10-CM system related to medical errors because changes include reorganization of categories from one chapter to another. For example, some codes in the injury and external cause chapters of ICD-9-CM have been moved into the body system chapters of ICD-10-CM. A chapter-by-chapter analysis is necessary to determine how much more specific the tenth edition is compared to the ninth edition with respect to medical errors or adverse patient outcomes (Pickett, 2002). Appendix L shows examples of new ICD-10-CM codes related to medical misadventures or adverse outcomes.

Some of the increased specificity in ICD-10-CM for medical or iatrogenic events comes from splitting concepts formerly grouped together (such as adhesions, obstructions, and perforations resulting from a foreign body being left in a wound or body cavity) into separate categories with their own numeric codes (i.e., adhesions resulting from a foreign body being left – is coded separately from – obstructions resulting from a foreign body being left, and so on). In addition to expanded specificity of codes that describe complications of diseases and treatments, the 10^{th} edition creates combinations of diagnosis/symptom codes to reduce the number of codes needed to fully describe a condition. NCHS has received a few requests for revisions of codes related to medical misadventures, which came primarily from the injury-prevention rather than patient-safety community. Requests for revisions are generally accommodated unless they are poorly justified. Requests that could not be accommodated within the ICD-9-CM numbering system generally have been resolved in the ICD-10-CM revision (Pickett, 2002). While the tenth edition adds codes for medical errors that were not in the ninth edition, it does not include the detail of systems developed specifically for error classification or for use in electronic medical records.

The ICD-9-CM has an ongoing annual update process (Pickett, 2002). The process includes two open meetings per year in April and December at which proposals are considered for changes to the coding system. Proposals must be submitted two months before a meeting for consideration at that meeting.

Approved changes take place at the beginning of the following fiscal year. For example, proposals submitted by February or October of one year are reviewed in April or December of that year and would take place in the next year on October 1. Revisions to ICD-9-CM will be considered until ICD-10-CM implementation is announced under HIPAA requirements. A moratorium on revisions of ICD-10-CM for 12 to 24 months will follow that announcement to give the industry time to modify data systems to accommodate ICD-10-CM codes.

Australia has been reviewing how ICD-9 and ICD-10 coding systems can be enhanced for error reporting. The Australian Patient Safety Foundation has collaborated with its members on developing a classification for adverse drug events that fits within the structure of the ICD-10 (Malpass et al., 1999). In addition, they have decided to incorporate a flag for each diagnosis on hospital discharge records to indicate whether a condition or adverse event was present or absent on admission to the hospital (similar to requirements of some mandated State discharge reporting systems in the United States). This is intended to reveal whether a clinical problem was pre-existing or occurred during the hospitalization.

In addition to Australia, other countries have used the ICD coding systems as a complement to adverse drug reaction classification systems. In fact, the current international standard for communication on drugs (MedDRA, see below), agreed upon by the European Union, Japan, the FDA in the United States, and other countries, incorporates some ICD terms into that classification system; however, it does not use it in its entirety. According to MedDRA developers, the specificity of the ICD-9-CM was not detailed enough to capture important adverse reactions to prescription medications.

There are drawbacks to the use of ICD codes in the error-reporting context. Patient safety experts consider the ICD classifications for adverse medical or surgical events to be incompletely specified. The draft of ICD-10-CM expands injury categories to include more terms related to adverse events. However, patient safety experts have not contributed significantly to the revision. For example, ICD does not identify types of failures and harm specific to the type of product involved, especially for devices, biologics, equipment or diagnostic tools. Furthermore, classifications are not specific enough. When classifying a drug-related adverse event it is important to have clinical outcomes specific to the event for adverse drug reactions. Similarly, when classifying an adverse-medical-device event, it is important to include physical or other effects that are likely to occur as a result of a device or implant failure.

Codes change annually and must be mapped across versions to use them with archived data or in longitudinal analyses. As with most systems, no severity indicators are included for the adverse events or patients' conditions. Some adverse event codes are organized under diagnoses, while others are organized separately in a chapter on injuries or in one on external causes (E-codes). Whether these codes are easier to use in an integrated or separate chapter format is unclear. Such codes also are not used often because there is no financial incentive to use them. No payers require the use of E-codes for reimbursement (Pickett, 2002). Moreover, there is an incentive not to use E-codes because of the legal liability of reporting errors. Twenty-three States mandate the use of E-codes for public health surveillance. Despite this, E-codes are vastly under-reported in mandated hospital discharge system of States, do not distinguish between the sharp end concerns and root causes, and may blur severity and probability of adverse events, which thwarts safety analysis.

Developers of MedDRA have expressed frustration at the inability of users of ICD-9-CM to obtain updates and additions and the time involved in the process. This frustration may pre-date current revision procedures for ICD-9-CM, although MedDRA currently releases updates every six months, rather than the year timeframe for ICD-9-CM.

Medical vernacular and synonyms are not defined in relationship to the ICD classifications. This feature of medical vocabulary systems (such as SNOMED and MedDRA, described below) helps to standardize the use of terms to describe clinical conditions and makes clear the relationship between alternative clinical terms. Building this capacity into the ICD systems would make them more generally applicable to clinical database needs.

Recommendation. In order for ICD-10-CM to be suitable for error reporting considerable attention must be paid to its modification in this regard. The ICD-10-CM workgroup and experts in patient safety should collaborate on concepts, terms, and classifications. This will require the ICD-10-CM workgroup to do a thorough analysis of the improvements of ICD-9-CM and ICD-10-CM with respect to misadventures and medical errors. This also requires the patient safety research and quality improvement communities to become involved in improving the classifications of the ICD in order to make it relevant to safety concerns. It will be a challenge to determine which aspects of patient safety can best be captured in ICD rubrics and which should remain separate data elements and separate classifications.

4.2.2.2 SNOMED® CT™(Standardized Medical Nomenclature of Medicine, Clinical Terms)

SNOMED CT (the newest available version of SNOMED) is described by SNOMED International (the organization responsible for maintaining and distributing it) as a relational classification of the entire medical vocabulary (including symptoms, diagnoses, and procedures) created to code information in the medical record into a form that can be processed by computers (SNOMED International, 2002a). It has over 960,000 medical relationships, including 325,000 specified concepts and 820,000 descriptions to cover the breath of contemporary clinical practice. It includes multiple root hierarchies of:

- Findings, conclusions and/or assessments
- Procedures
- Body structures
- Biological functions
- Living organisms
- Substances (chemicals and drugs)
- Physical agents, activities and/or forces
- Occupations
- Social context, and
- Modifiers/linkage terms and/or qualifiers.

SNOMED (through its prior mappings of either the SNOMED RT or the NHS Read Classifications V3) maps to ICD-9-CM, ICD-O-3, ICD-9, and ICD-10 disorders; LOINC laboratory investigations, OPCS-4 procedures and IUB enzymes and BNF and EAN drug classifications. In the future, SNOMED International may develop other mappings: ICD-10-CM disorders; CPT4 procedures; DRG, HRG, HBG groupers; and clinical LOINC terms (SNOMED, 2002b). The mapping usually represents more detailed SNOMED terms linking to broader terms in the other classifications.

The College of American Pathologists (CAP) and the National Health Service (NHS) of the United Kingdom collaborated to combine the SNOMED RT (Reference Terminology of the CAP) and the Clinical Terms Version 3 of the NHS thesaurus of health care terms (Read Codes v 3.0). The new work, named SNOMED Clinical Terms (abbreviated SNOMED CT), combines the strength of SNOMED RT in specialty medicine, including pathology, and the richness of Read Codes V3 in primary care (described below).

SNOMED has been recommended by the NCVHS and by the Computer Patient Record Institute as the top candidate for the standard vocabulary and data model for the computer-based patient record. SNOMED International reports that the nomenclature is widely used in electronic health records, clinical laboratory and radiology systems, infectious disease reporting, HEDIS reporting, emergency rooms, case reports for clinical research, cancer registries, literature searches, image repositories, telemedicine, autopsy databases, and web-based consumer information.

SNOMED has a number of shortcomings as a classification for integrating disparate error reporting systems. The proprietary nature of SNOMED is a drawback to its use as a national or international standard for classifying adverse medical events. The high license fee maintained for SNOMED by CAP

makes this a very expensive choice for the world. Because of the price, we were unable to examine the detail of the coding system to determine whether and how errors are handled in this system. Others have concluded that SNOMED is incomplete for adverse event reporting (Hammond, 2002). CAP is considering creating a subset of terms specifically designed for adverse events. Additionally, the lack of a hierarchical numeric coding scheme, although not crucial when a standard vocabulary for narrative descriptors is the prime purpose, is inefficient for information retrieval and manual assignment of discrete codes.

Recommendation. Because of the recognized prominence of SNOMED in computer-based patient record development, it should be evaluated as a system for classifying adverse event data. In particular, it should be compared to MedDRA and Medcin (see below) to determine the similarities and differences between them and whether one or the other could satisfy the requirements for adverse event reporting. Selecting and modifying one system as a medical vocabulary rather than maintaining two or more, will reduce the resources that must be allocated to maintaining classification systems.

4.2.2.3 MedDRA™(Medical Dictionary for Regulatory Activity – A Hybrid of Clinical Language and Medical Error Coding

MedDRA (TRW, 2001; Revelle, 2002) is a controlled clinical vocabulary developed to code adverse event information in the registration, documentation, and safety monitoring of drugs throughout their regulatory cycle, from Phase I clinical trials through post-marketing surveillance when products are FDA-approved for distribution to consumers. While MedDRA was developed to track adverse events related primarily to drugs, it is being expanded to include adverse events associated with other medical products such as medical devices. A MedDRA autocoder is available that can identify standard terms and codes for concepts described in narrative text strings. MedDRA is a single system for combining information on symptom, sign, disease, diagnosis, therapeutic indication, name and qualitative results of investigations (i.e., laboratory result and adverse reaction), surgical and medical procedure, and medical/social/family history. These concepts are combined into one classification system to simplify the number of coding schemes needed to describe information about effects of clinical trials and marketing of medical products. MedDRA is a coding system, which is hierarchical (i.e., ordered conceptually) and relational (i.e., single terms or adverse reactions map into multiple system organ classes (i.e., body systems) in a standard way), but it is not numerically hierarchical. The numeric codes are sequential and non-expressive (i.e., contain no imbedded logic or knowledge) and are never changed. The codes are never changed because archived clinical trial data cannot be analyzed easily when codes change. There are over 14,000 preferred or recommended terms for clinical descriptions and over 51,000 lower level terms that help relate common vernacular to preferred terms; higher level aggregations are also part of the coding system.

MedDRA is being supported internationally as a standard terminology for electronic transmission of adverse event regulatory information. It has replaced other adverse reaction terminologies (e.g., Japan's Adverse Reaction Terminology (J-ART). MedDRA is currently recommended by several entities: the AERS program at FDA/CDER, VAERS at CDC, MedSun at FDA/CDRH, the International Conference on Harmonization of Technical Requirements for the Registration of Pharmaceuticals for Human Use (also known as the ICH), and the regulatory authorities of Europe and Japan. MedDRA and ICH are both entities of the International Federation of Pharmaceutical Manufacturers Association. Within the United States, MedDRA is ANSI compatible but not a standard adopted by ANSI-accredited organizations. The ICH does not depend on or require ANSI accreditation of standards.

There are several weaknesses of MedDRA that are important from the perspective of finding a classification system for integrating disparate systems. The proprietary (rather than public) access to MedDRA inhibits its use as a broad standard. Mandated standards should be readily and freely available. Use of MedDRA under the current subscription arrangement would burden hospitals and clinicians who would have to pay a license fee to MedDRA for reporting adverse events.

MedDRA currently excludes equipment, device and diagnostic product and failure terms, but may eventually include these. The lack of a hierarchical numeric coding scheme may not be a problem for automated coding, but is inefficient for information retrieval and manual assignment of descriptors.

MedDRA incorporates relevant terminology of a few other coding systems but not all terms and not the numeric coding of those systems. For example, ICD-9-CM diagnoses and LOINC laboratory terms are sometimes incorporated. However, this does not mean that ICD-9-CM or LOINC has been subsumed wholly, nor that their numeric codes are accessible in MedDRA. MedDRA is generally applied in a limited context. For example, the AERS manual instructs MedDRA coders to exclude prior medical history except when the history was aggravated by the adverse event. As with most systems, no severity indicators are included for the adverse events or patients' conditions.

We were not able to view the complete MedDRA coding system due to its proprietary nature. MedDRA is maintained by TRW and supported through a subscription fee. Prior adverse reaction terminologies were poorly maintained and for this reason drug manufacturers worldwide agreed on a proprietary system supported by users. Full access to the system costs $2,500 to $80,000 per year depending on the profit status and size of the subscribing organization.

Recommendation. Despite the fact that MedDRA is recommended by several organizations as a standard for collection of data on adverse medical product events, several shortcomings need to be overcome for it to be an effective standard for classification of clinical adverse event data more generally. Furthermore, it may be difficult, if not impossible, for certain groups to agree to changes to make the system appropriate for other uses. For example, periodic changes in numeric coding are one of the reasons that ICD coding is eschewed by the ICH for regulatory product data.

4.2.2.4 Other Clinical Languages

Other systems exist for coding of clinical terms for various and specific purposes.

Medcin is a set of more than 175,000 clinical terms encompassing symptoms, history, physical examination, tests, diagnoses and therapy. It is used to encode the clinical encounter with patients (Medicomp, 2002). An Intelligent Prompting engine displays only clinically relevant items for rapid documentation without overwhelming the user with information. Also, the Medcin presentation engine relates medical terms through multiple clinical hierarchies for each Medcin term. For example, chest pain is related to fever in the diagnosis of bacterial endocarditis, but not in the diagnosis of angina. Medcin includes millions of these medical relationships. Each Medcin term has an associated property record containing items such as relevant value ranges, units for tests results, laterality flags, control for narrative presentation, and cross-references to external code sets. Medcin maps to other coding systems: CPT-4, ICD-9, ICD-10, ICD-O and DSM-IV. The system is available for a license of only $25 per year per facility. This system also should be evaluated as a clinical nomenclature for integrated error reporting.

While use of MEDCIN at a site may be economical, its incorporation in application programs is a different issue. With an initial license cost of $450,000 and a $100,000 annual update fee, use of the MEDCIN database, GUI and API would be a significant line item in any budget. For MEDCIN to be considered a viable option it would have to be shown that its use would have a major impact on reducing programming costs.

Drug Terminology for standard usage has been in a state of turmoil that now appears to be resolving. The National Drug Codes (developed by the FDA) were originally proposed as a HIPAA standard but because of problems – they do not capture the route, dosage, or frequency of administration; they do not have a hierarchy or classification scheme; other organizations have enhanced codes to make them more usable analytically but that impedes standardization of codes – another alternative has emerged. The FDA is adopting the VA-Drug-RT terminology set and is merging it with NDC codes. Also, the FDA proposes to use the HL7 clinical drug model and the HL7 terminology for route and form and for devices. This

terminology will be remodeled for input into UMLS. If drug manufacturers accept the revised terminology, the drug terminology problem may be solved (Hammond, 2002).

LOINC, Logical Observation Identifiers, Names and Codes is a set of universal names and codes for identifying laboratory and clinical test results. The purpose is to facilitate the exchange and pooling of results, such as blood hemoglobin, serum potassium, or vital signs, for clinical care, outcomes management, and research. The problem has been thatlaboratory results are sent electronically from producer laboratories to clinical care systems in hospitals identifying tests in these messages by means of internal (and idiosyncratic) code values. Receiving medical informatics systems could not fully "understand" the results they receive unless they either adopted the producer's laboratory codes (which is impossible if they receive results from multiple source laboratories, for example, the hospital, the nursing home, and the local commercial laboratory), or invested in the work to map each laboratory's code system to their internal code system. LOINC is increasingly becoming system of choice for naming laboratory data elements. The well-defined LOINC structure has strong academic input and is available to trading partners without a license fee. LOINC will be part of the clinical content modifications of ICD-10. LOINC is included in UMLS and also is proposed for the claims attachment.

ICPCS, International Classification of Health Problems in Primary Care is a modified version of ICD-9 intended for use in general practice to identify patient reason for encounter, symptoms, diagnosis, procedures, counseling services, referrals, radiology ordered, and administrative procedures. It is used in the UK and Australia. ICPC-2 Plus was released in 1998 and is specifically designed for use in computerized patient record, disease registries and secondary coding of clinical data.

ICIDH, International Classification of Functioning and Disability is a set of common terms of disability for clinical use, data collection, and research. As such it may be relevant for classifying the disabling outcomes of adverse medical events.

Canonical Clinical Problem is a clinical language that connects diagnosis to therapy, prognosis, and psychosocial issues, developed to reduce the amount of time that clinicians take to enter information into a computerized patient record.

CPT-4, Current Procedural Terminology, Fourth Edition provides descriptive terms and numeric codes for reporting medical, surgical, and diagnostic services and procedures by physicians in the U.S. All third party payers require CPT-4 codes for outpatient service claims. CPT-4 is the HIPAA standard for coding treatment in physician offices.

HCPCS, HCFA Common Procedure Coding System, is built on CPT-4, and extends it to services outside of physician’s care, such as ambulance and emergency medical technician services and for medical equipment and supplies.

ICD-10-PCS, International Classification of Disease, Tenth Edition, Procedures was developed as a replacement for ICD-9-CM Procedures (Volume 3) for reporting hospital inpatient services. ICD-9-CM Procedure Codes are the HIPAA standard for reporting institutional services. Originally recommended as the HIPAA standard to replace CPT-4 for outpatient claims, it was overthrown because of anticipated retraining costs in physician offices.

Read Clinical Classification of Medicine (Read Codes V3) is a list of terms describing the care and treatment of patients under primary care, which is intended for use by all healthcare professionals and is used extensively by family practitioners in the United Kingdom. It includes some error-related terms that might be useful for ICD-10-CM revision. Read is now integrated with SNOMED.

Nursing Classifications are likely to be important systems for reporting medical errors and unexpected events occurring during hospital, nursing home, and home care, primarily because nurses’ and aides’ have continual contact with patients and because on the health care team they observe and implement physician orders and observe outcomes of all treatments. NANDA**,** the North American Diagnosis Association

system describes patient reactions to disease. **NIC,** Nursing Intervention Classifications names and describes treatments performed by nurses. **NOC,** Nursing Outcomes Classification identifies patient outcomes influenced by nursing practices. **The Omaha System** is a problem classification system, an intervention scheme, and a problem rating scale for outcomes related to nursing and other health professionals' services. Finally, **PCDS,** the Patient Care Data Set, is a compilation of terms used in patient records to record patients' problems, therapeutic goals, and care actions.

4.2.3 Error Classification Systems

Developmental work in the collection and measurement of events related to medical error has resulted in generic classifications for errors and the environment surrounding errors, near misses, and latent problems that can lead to errors. The more widely used and readily available systems of classifying errors are described below. In addition, systems developed by organizations for their own environments (e.g., hospital-based systems) also have schemes for classification of errors. These are not reviewed here because of the difficulty obtaining documentation on those classifications.

4.2.3.1 NCCMERP Taxonomy of Medication Errors: National Coordinating Council for Medication Error Reporting and Prevention

The National Coordinating Council for Medication Errors Reporting and Prevention (NCCMERP, 1998) is a membership organization of stakeholders in safe medication practices. The FDA, the American Society of Health-System Pharmacists (ASHP), and the U.S. Pharmacopoeia (USP) currently provide leadership. It aims to foster a standard language and structure for medication-error reporting and data analysis and makes its list of categories freely available.

The NCCMERP classification specifies how to classify data elements for

- Patient identity and demographics
- Date and time of event
- Setting of the event
- Description of the event (in narrative format)
- Extent of harm to the patient
- Detailed product information (for the product given and the product intended to be given)
- Type of personnel involved
- Type of error that occurred
- Causes of error (e.g., communication, name confusion, labeling, human factors, and packaging or design)

Categories are specified (often in detail) for all of the fields above except for the "description of the event," which is specified in narrative form. NCCMERP classifications are being used primarily by organizations focusing exclusively on medication errors. At the FDA, data from the AERS is coded into NCCMERP classifications after the error is reported (i.e., current reporters do not select NCCMERP categories). The NCCMERP classification of harm (NCCMERP, 1998) to the patient has wider application. It is used by many organizations collecting information on *all* types of clinical errors. We have noticed the NCCMERP harm categories on hospital-wide error reporting systems where data on all errors is collected.

The NCCMERP categories related to harm are shown in Appendix M. NCCMERP provides a number of procedural recommendations around error reporting. NCCMERP recommend that error information be reported as soon as possible after the event and updated or corrected whenever events change. Also, that one category be reported, and that the highest severity occurring during the course of the event be selected.

For various reasons, the NCCMERP classification of harm to the patient is not universally accepted. At the first annual AHRQ Conference on Patient Safety, it was noted that the NCCMERP harm/error classification combines and confuses two dimensions of the safety problem – persistence of the harm to the patient (or probable outcome of the event) with the severity or extent of the error itself. This shows differing objectives for operations and research. One wants a minimum number of data elements collected and the other wants measures of different concepts segregated. We found two systems that work to distinguish between the severity and probability of event occurrence - the MERS-TM Risk Assessment Index and the VA Safety Assessment Code Matrix. These are described in more detail below.

4.2.3.2 Eindhoven Classification of Root Cause

A model of error classification for root cause analysis, which was originally developed for the chemical industry by Van der Schaff and then adapted for transfusion medicine (Battles et al, 1998), has the potential for wider application. This classification was designed to be used after formal root cause analysis into the event to facilitate searching and analysis of patterns of errors. The Eindhoven Classification Model, Medical Version, uses 19 categories of a root cause which are organized into three types: technical, organizational, and human causes. The categories are consistent with latent and active error theory and with the classification of human behavior into skill, rule, and knowledge factors. The table below shows the structure of the Eindhoven classification. The latent errors are technical and organizational. The active errors are human.

Table 2: Structure of Eindhoven Classification Scheme

Type of Error	Factors
Latent	
Technical	External, design, construction, materials
Organizational	External, protocols/procedures, transfer of knowledge, management priorities, culture.
Active	
Human (caregiver)	Knowledge-based errors
	Rule-based behavior (qualifications, coordination, verification, intervention, monitoring)
	Skill-based errors (a slip or tripping)
Other	Patient-related factors, unclassifiable

Source: Battles et al., 1998.

Effective use of this system requires training, especially for staff with no quality assurance or risk management background, and monitoring and guidance to ensure consistency of its application across systems. Examples of the use of this system are in Battles and Shea, 2001.

4.2.3.3 The Risk Assessment Index

One challenge of risk management is deciding on which errors to investigate in depth. Another classification system, called the Risk Assessment Index of the MERS-TM system, distinguishes the severity (actual or potential) of an event and the probability that the event will recur. For each of these two dimensions, a scale of severity or probability is selected and a value that represents the interaction of the two dimensions is identified to decide which events to study. The index also factors in an adjustment for whether or not the transfusion product was issued and the type of recovery of the patient from the event. Those events with over a 0.5 index should be investigated according to the MERS-TM manual (Kaplan, 2001).

4.2.3.4 The VA Safety Assessment Code Matrix

The Veteran's Affairs, National Center for Patient Safety, has a similar tool for assessing severity of the event from the perspective of patients or resources and the frequency of the event at a facility (NCPS, undated; Bagian et al., 2001). As shown in Table 3, the VA SAC severity score is classified into catastrophic, major, moderate, and minor events that are each defined with respect to the harm (actual or potential) to humans (patients, visitors, and staff) and equipment and facility damage. Within the severity categories, expected frequency of an event also is scored to determine what action to take with respect to an event. For "close calls," reporters are instructed to code the severity of the worse case scenario even though it might have been averted.

Table 3: Veterans Affairs Safety Assessment Code Matrix Severity Definitions

Severity	Involvement	Definition of Severity
Catastrophic	Patients with Actual or Potential:	Death or major permanent loss of function (sensory, motor, physiologic, or intellectual) not related to the natural course of the patient's illness or underlying condition (i.e., acts of commission or omission). This includes outcomes that are a direct result of injuries sustained in a fall; or associated with an unauthorized departure from an around-the-clock treatment setting; or the result of an assault or other crime. Or any of the following: • Suicide (inpatient or outpatient) • Rape • Hemolytic transfusion reaction • Surgery/procedure on the wrong patient or wrong body part • Infant abduction or infant discharge to the wrong family
	Visitors:	A death or hospitalization of 3 or more visitors.
	Staff:	A death or hospitalization of 3 or more staff.
	Equipment or facility:	Any fire larger than an incipient stage. A incipient fire is smaller than a burning waste paper basket, easily extinguishable with a portable fire extinguisher, and does not require evasive action (e.g., stooping) when approaching the fire to avoid heat or smoke.
Major	Patients with Actual or Potential:	Permanent lessening of bodily functiong (sensory, motor, physiologic, or intellectual) not related to the natural course of the patient's illness or underlying conditions (i.e., acts of commission or omission) or any of the following: • Disfigurement • Surgical intervention required • Increased length of stay for 3 or more patients • Increased level of care for 3 or more patients
	Visitors:	Hospitalization of 1 or 2 visitors.
	Staff:	Hospitalization of 1 or 2 staff or 3 or more staff experiencing lost time or restricted duty injuries or illnesses.
	Equipment or facility:	Damage equal to or more than $100,000.
Moderate	Patients with Actual or Potential:	Increased length of stay or increased level of care for 1 or 2 patients.
	Visitors:	Evaluation and treatment for 1 or 2 visitors (less than hospitalization.

	Staff:	Medical expenses, lost time, or restricted duty injuries or illness for 1 or 2 staff.
	Equipment or facility:	Damage more than $10,000 but less than $100,000.
Minor	Patients with Actual or Potential:	No injury, nor increased length of stay nor increased level of care.
	Visitors:	Evaluated and no treatment required or refused treatment.
	Staff:	First aid treatment only with no lost time, nor restricted duty injuries nor illnesses.
	Equipment or facility:	Damage less than $10,000 or loss of any utility (e.g., power, natural gas, electricity, water, communications, transport, heat/air conditioning) without adverse patient outcome.

4.2.3.5 Other Error Classifications

There are a number of systems for identifying known adverse drug reactions. Most are proprietary.

MediSpan GPI Code is a proprietary software product of drug-drug and drug-diagnosis adverse interactions that can be used for checking potential interactions. Hierarchical drug codes are available for identifying drugs down to manufacturer and pill size.

MicroMedex makes proprietary software products on known adverse drug reactions (Drug-Reax) and poisonings (Poisindex), and other related information products. Drug-Reax allows users to search for drug-drug, drug-food, drug-disease, drug-ethanol, drug-tobacco, and drug-laboratory test interactions, along with known allergic reactions. It provides information on dosage, pharmacokinetics, cautions, interactions, clinical applications, adverse effects, comparative efficacy, drug of choice information, and orphan drug status.

CIOMS I. The Council for International Organizations of Medical Sciences (CIOMS) developed a terminology for adverse drug reactions (ADRs) in 1990. CIOMS is an international, nongovernmental, non-profit organization established jointly by WHO and UNESCO. Its members are international and national medical scientific societies of various countries. The CIOMS adverse drug reaction form is accepted by AERS for reports of ADRs. The group developed an ADR terminology, because the meaning of terms can vary significantly from country to country.

The **ICH E2B** provides a publicly available format for classifying and transmitting data elements for assessing adverse event reports (including adverse drug reactions). It was created by IFPMA, the Association Of The International Pharmaceutical Industry. The purpose is to standardize data elements for transmission of individual case safety reports, regardless of source, destination, and whether they relate to pre- or post-approval drugs. The approximately 300 E2B data fields include only four that are required (in *italics* below), one required term that calls for MedDRA coding (in ***italics and bold*** below**)**, and 13 optional terms that require MedDRA terms (in **bold** below**)**.

- Information about the report (*sender*; country; date of transmission and receipt; type of report; seriousness of report related to whether it results in death, is life-threatening, requires inpatient hospitalization, prolongs hospitalization, results in persistent or significant disability, is congenital/birth defect, or other medically important condition.
- Primary source of report (identifier, address, country, and qualifications of reporter, qualifications of physician, pharmacist, other health professional, lawyer, consumer, reference to literature, etc.)
- Sender and receiver information and type of sender and receiver of case safety report (drug company, regulatory authority, health professional, regional pharmacovigilance center, WHO collaborating center for drug monitoring, other).

- Patient characteristics (*identifier*, name, medical record number, or other, age, weight, height, gender, **relevant medical history**, **concurrent conditions, relevant past drug history, and reported cause(s) of death, autopsy-determined cause of death,** and parent information, if relevant.
- Reaction/event (narrative, *MedDRA preferred term*, MedDRA lower-level term, indication for use of drug in this case, which reactions(s)/events(s) occurred, relatedness of drug to reaction/event, sender's diagnosis of reaction/event, seriousness of event, dates, duration, outcome).
- Results of tests relevant to adverse event investigation.
- Drug product (drug identifier, dosage, route of administration, start date, relation of drug to event).
- Narrative case summary and further information (clinical course, reporter comments, sender comments).

This system includes categorical lists for many of the data elements. For example, ICH E2A has classes for seriousness of event, duration, outcome, time intervals, and route of administration, among others.

In addition to the systems described above, other systems might be useful for developing standards for classifying data elements used in medical event reporting. The American College of Radiology has a classification for MRI hazards. The American Society of Anesthesiologists has a classification for the severity of illness of patients who are slated for surgery and anesthesia.

Devices have at least two alternative classification systems – the Universal Medical Device Nomenclature System (UMDNS) developed by ECRI and the General Medical Device Nomenclature (GMDN) CR 14230 developed by CEN - Comité Européen de Normalisation or European Committee for Standardization. According to the CEN Website many GMDN terms incorporate or have a cross-reference to other vocabularies – for example the UMDNS system and the FDA nomenclature in the USA and medical languages of other countries. The FDA MedSun program has selected the GMDN as the standard for reporting events related to medical devices. This program will begin using GMDN as soon as MedSun obtains the rights to use the product.

4.2.4 Summary of Issues of Standards for Integration

Standards development is one of the most challenging issues for developing a national infrastructure for health data in general and medical error reporting in particular. Agreement on standards will undoubtedly be a difficult issue for DHHS integration. Minimizing the number of classification systems that reporters must understand and use is crucial to reducing the reporting burden on those who are at the front lines of health care delivery and reducing the confusion and incompatibility in data that are collected.

Despite the obvious benefits of minimizing the number of classification systems involved, the reality is that different systems have evolved for different specific purposes. For example, MedDRA was created because ICD-based systems did not provide the specificity of coding needed for understanding the consequences of adverse drug events and because the process for changing the ICD systems was too slow and cumbersome from the drug manufacturer's perspective. SNOMED may also have benefited from the ICD systems inflexibility.

In the interest of simplicity either one system should be selected as the standard or a behind-the-scenes translation between systems should be developed. The latter idea is attractive because it could enable the terminology-focused systems (without meaningful numerical coding) to map into the numerically designed systems that are efficient for information retrieval.

Are wholesale translations between clinical vocabularies for error reporting systems feasible? The National Library of Medicine (NLM) has developed a tool that can help to answer that question. The Universal Medical Language System (UMLS) provides tools for translating between medical languages. We explored briefly with medical informatics specialists (Hammond, 2002; Schoeffler, 2002; Wasserstrom, 2002) the usefulness of UMLS tools for bridging between key clinical classifications. While UMLS is probably the best translation source for clinical language systems, one difficulty of using

UMLS is the requirement of use licenses. For example, to use SNOMED or MedDRA, license fees must be paid to their vendors. This is prohibitive for many developers and could curtail adoption of error reporting systems by some facilities, if this barrier cannot be overcome (Hammond, 2002). Furthermore, while the UMLS will support translations between vocabularies, one system will map into another only as well as the underlying structure of the two relate. In other words, terms translated from a more specific language to a more general language will result in loss of some information. How much information will be lost will depend on the relationships between the two systems; determining the extent of the degradation would require study. It may be more reasonable to translate from the original narrative into two languages, than to translate from one controlled vocabulary into another (Wasserman, 2002). We can envision this process of translating narrative into both MedDRA and ICD-9-CM, for example, to tap the detailed clinical terminology of MedDRA and the efficiencies of ICD-9 (or 10)-CM numeric coding for retrieval and analysis of data.

Another issue is the relative infancy of classifications specific to describing the error itself. A number of organizations and individual hospital systems have been developing "home grown" error reporting systems. A mechanism needs to be instituted for providing guidance to those systems. Such coordination could go a long way toward standardizing classifications and variations that currently exist.

Medical error classification is frequently performed subsequent to data collection, not as part of the data collection process. In other words, the reporter is asked to "Describe what happened *in your own words."* Then skilled coders translate those reports into standard terms. Reporting "in your own words" is encouraged because the ultimate purpose is to determine the root cause of the error, which may be unknown even to the party reporting the error. In the Aviation Safety Reporting System (ASRS), narratives are captured along with specific classification to verify consistency in categorization of errors (similar to application of MedDRA or ICD-9-CM by skilled professionals) and to diagnose the underlying cause (NASA, 1999). ASRS, which was started in 1975, is a mature error reporting system. Medical error reporting can learn from the best practices in other industries such as aviation and nuclear energy. Error reporting through narratives is in contrast to data systems based on pre-specified lists, which have been devised for known, ongoing purposes, such as claiming reimbursement.

The National Committee on Vital and Health Statistics argues forcefully that uniform standards are a pre-requisite to broadening the investments in computer-based patient medical record information that someday can serve as the basis of a national health care information infrastructure (NCVHS, 2001b). The Health Insurance Portability and Accountability Act of 1996 set in motion the development for the first time of nationally required standards for transmission of health insurance claim transactions; such standards are expected to reduce the cost and confusion of hundreds of different systems that providers contend with to file claims for reimbursement. Medical error reporting can also learn from the history of inefficient claims reimbursement. Categorized reporting along side narrative reporting can increase the efficiency of gaining information from error reporting systems. Pre-specified categories and coding (such as for the clinical condition of the patient) is important not only for comparable data in integrated error reporting systems, but also for efficient retrieval of knowledge from reporting systems. Whether this is done by the reporter of the event or by trained coders who receive reports centrally, it will need to be done consistently and quickly to make reports accessible in a timely manner.

In the 1999 Report to the Commissioner, an FDA task force on risk management recommended continuing to integrate existing systems so that data is uniform and accessible to all (FDA TF, 1999). FDA has made efforts in this regard by moving data from separate databases (Medication Error Reporting System, Drug Quality Reporting System, MedWatch) into the AERS database. As discussed earlier, the FDA is also working collaboratively with international agencies to identify and incorporate naming and coding standards into their reporting systems.

If experiences of other data systems are any guide, error reporting systems must aim to remove the barriers to a common language for reporting in order to foster knowledge that will improve the safety of patient care.

4.3 Privacy Requirements as Constraints to Integration

The external factor most likely to constrain and discourage medical error reporting nationwide is the absence of effective protections for health care data, in light of the legal liability that health care providers can face from acknowledging mistakes. Similarly, limitations of privacy laws, privacy rules, and common laws privacy mandates (for example, breach of confidentiality, invasion of privacy) can influence the collection, transmission, storage, and, in particular, the willingness of organizations to share personal health care data. Both Federal and State laws affect the collection and use of "personally identifiable" health information (PIHI). At the Federal level, both general privacy and disclosure laws and laws specific to the authorization of particular agency activities are relevant. At the State level, a myriad of laws that differ by State is involved. The implications of these laws and rules (and their limits) for DHHS integration and beyond are considered here.

Health data privacy can be viewed from many angles. Three angles relevant to the reporting of data related to adverse medical events are:

1. Safeguarding and sharing PIHI – safeguarding the individual's right to the privacy of their personally identifiable health information (PIHI) and sharing such data for research and learning.
2. Shielding PIHI from legal discovery – protecting data from the discovery process in the courts so that data can be collected feasibly in the first place; and
3. De-identifying PIHI – collecting only de-identified data or removing identifiers so that data can be shared whenever possible.

Each of these angles is reviewed in the context of laws and regulations that affect the collection and handling of health data. In addition, we discuss the implications of these laws and rules for handling PIHI in an integrated medical error reporting system.

Warning: Definitive legal advice should not be inferred from this section. MEDSTAT researchers, not lawyers, have assembled the information in this section. Despite the fact that two outside lawyers also have reviewed this section, the complexity of the issue, the myriad related laws, and the diversity of legal opinion argue for further review and critique by legal scholars. In particular, lawyers who are familiar with specific agency statutes and with Federal and State privacy laws should be consulted for legal opinions on these matters.

4.3.1 Safeguarding PIHI and Sharing It with Other Entities

The health care community has a moral and ethical duty to protect the privacy of PIHI. It is the inflexibility of laws and rules designed to protect this privacy that has researchers worried, reasonably or unreasonably. Especially under the new HIPAA Privacy Rule (see below), researchers are concerned that providers and health plans might not be willing to share data in the future for learning nationwide (HCFO, 2002). In particular, small health care entities may be dissuaded from participating in research and medical error reporting, because of the cost of implementing the requirements of the HIPAA Privacy Rule and the significant penalties for noncompliance with the Rule (up to $250,000 per violation in civil fines and up to 10 years in prison for criminal penalties). HIPAA agreements and affirmations of compliance will be necessary before data sharing can occur, increasing the cost of medical error reporting (Liang, 2002). The impact on an integrated Federal reporting system may be substantial, if a significant number of providers concerned about privacy compliance – especially small community providers – decline to participate.

A patchwork of privacy laws and regulations affect the privacy of PIHI. Current Federal laws affect data collected by Federal agencies and supported with Federal research funds. The HIPAA Privacy Rule (to

become effective April 2003) relates to health information held by any health care provider, health plan, and their business associates. State laws address privacy of health data in specific circumstances, but generally States do not have comprehensive privacy laws regulating the use and disclosure of PIHI.

The Federal laws affecting the privacy of PIHI include the following. Each law applies to the following respective domain and will continue to do so even after the new privacy rule takes effect next year. Each of these laws is described in more detail in the next sections.

- The Federal Privacy Act of 1974 (5 USC 552a and 5 CFR Part 1302) applies to Federal systems of records, specifies limits on disclosure, and specifies some permitted uses. (A separate and more stringent set of rules applies to mental health and substance abuse client records.)
- The Federal Policy for the Protection of Human Subjects – referred to as The Common Rule (45 CFR §46) – applies to data on human research subjects funded by the Federal government.
- The HIPAA Privacy Rule (45 CFR Parts 160 and 164) – mandated under the Health Insurance Portability and Accountability Act (HIPAA) of 1996 (Public Law 104-191) applies to electronic transactions between health care providers and their business partners and is scheduled to take effect April 2003.

Beyond these current laws, on June 5 and 6, 2002, two bills were introduced to the Congress (Senate Bill 2590 and House of Representatives Bill 4889) to promote the voluntary reporting of medical events for learning and research, to stimulate development of a national medical errors database, and to protect information that is shared voluntarily for quality improvement from legal discovery.

4.3.1.1 The Federal Privacy Act of 1974

The Federal Privacy Act requires that any and all personal data collected by the Federal government may be used only for the purposes for which they were collected. The purpose of the data collection is always stated on a data collection instrument (e.g., survey questionnaire) or in a data collection agreement.

In general, the Federal Privacy Act as reflected in the Administrative Procedures Act (5 USC 552a and 5 CRF 1302) affects all Federal agencies maintaining systems of records on individuals and specifies privacy protections for those records. This act requires that: “No agency shall disclose any record which is contained in a system of records by any means of communication to any person, or to another agency, except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains” with exceptions. The exceptions include

- routine uses for which the record was collected;
- statistical research and reporting, with a written request, appropriate assurances, and de-identification of the transferred data;
- circumstances affecting the health or safety of an individual;
- censuses and surveys of the Bureau of the Census, record keeping of the National Archives, and duties of the General Accounting Office; and
- pursuant to a court order or for a civil or criminal law enforcement activity provided the latter request is in writing from the head of the agency and explains the uses of the record.

This law demonstrates two relevant issues. First, exceptions to general prohibitions on data sharing across agencies can be made, but for other than the safest, general uses (for example, de-identified data transmission for statistical reporting) such sharing must be codified in law. Second, Federal administrative records are not protected from access by the court system or law enforcement agencies.

This Federal privacy provisions have been interpreted in some circumstances to mean that personally identified data collected by one Federal agency for one purpose may not be shared with another agency, even between different parts of the same agency, or outside of the government. Thus, for example,

personally identifiable household data collected by AHRQ may not be shared with the FDA for purposes of linkage with any personally identifiable MedWatch reports (if MedWatch reports identified patients).

4.3.1.2 The Common Rule on Protection of Human Research Subjects

The Common Rule addresses the confidentiality of PIHI collected for the purpose of research on human subjects, although some think the applications of the Common Rule have serious flaws. Under the Common Rule, all Federally funded research must have the approval of an Institutional Review Board (IRB), which can be set up by any organization involved in medical research. The Common Rule requires IRBs to approve research provided that 1) processes are in place to protect the confidentiality of PIHI and 2) subjects are informed of how their data will be kept confidential as part of the informed consent process.

The requirement to inform subjects can be waived when the data 1) already exist at the time of the research or 2) are either publicly available or not identifiable 45 CFR §46.111 [7]). Also, the waiver process can be expedited by review of less than the full IRB, if the data to be used or collected present no more than minimal risk to the patient, even if personally identifiable, and the research cannot be carried out without PIHI (45 CFR §46.116 [5].).

The General Accounting Office (GAO) has investigated how medical records are protected in the U.S. and concluded that the IRB process "does not ensure the confidentiality of medical information used in research." The GAO draws this conclusion because "records-based research is often subject to an expedited review process," the members of an IRB often rely on "the existence of general organizational confidentiality policies," or the IRB simply does not have time or adequate motivation to conduct thorough reviews when competing against their other professional demands (GAO, 1999, P. 12-14). The recent spate of patient deaths in clinical trials has exacerbated these concerns. Thus, in the future IRBs may have more difficulty in attracting IRB members and may become more stringent in their requirements for describing research protocols and data protections (Liang, 2002).

Despite these concerns, an IRB could be established as a strong, oversight process for reviewing the confidentiality of medical error reporting data in the U.S. and establishing guidelines for protecting and disclosing event data for mandated reporting and for research. An advantage of this avenue is that under 42 USC §241(d), the privacy of individuals who are research subjects is specifically protected from legal discovery: "The Secretary may authorize persons engaged in biomedical, behavioral, clinical, or other research (including research on mental health, including research on the use and effect of alcohol and other psychoactive drugs) to protect the privacy of individuals who are the subject of such research by withholding from all persons not connected with the conduct of such research the names or other identifying characteristics of such individuals. Persons so authorized to protect the privacy of such individuals may not be compelled in any Federal, State, or local civil, criminal, administrative, legislative, or other proceedings to identify such individuals."

4.3.1.3 The HIPAA Privacy Rule

The HIPAA Privacy Rule was published on December 28, 2000. Also, DHHS released a Notice of Proposed Rule Modification on March 27, 2002, requesting comments that will be reviewed before changes in the rule are made. Deadline for implementation of the HIPAA Privacy Rule as proposed December 28, 2000 is currently April 14, 2003 for nearly all covered entities.

The HIPAA Privacy Rule applies only to covered entities (health plans, health care clearinghouses, and health care providers who conduct financial and administrative transactions electronically), but the provisions related to research apply to public and private research. Also, the Rule has been interpreted by DHHS to apply widely through contracts of covered entities with their "business associates."

The HIPAA Privacy Rule requires entities engaged in treatment, payment, or other health care operations to obtain written consent or authorization of the patient before disclosing the patient's PIHI for any

purpose, with few exceptions (45 CFR §164.506, §164.508, and §164.510). Exceptions include disclosures required by law – for example, State or Federal laws related to reportable public health events (activities related to preventing or controlling injury or disability) and FDA-required adverse event reporting. Other research activities, such as sharing of reported adverse event information among multiple Federal agencies would require patient authorization.

The proposed changes to this rule, which are currently available for comment, recommend that HIPAA patient consent requirements be replaced with some form of notice to the patient regarding the provider's privacy policies and procedures. Given that the research paradigm referenced most in the Privacy Rule and its proposed modification is the clinical trials protocol (where consent of the patient is required for enrollment and treatment in the trial),[3] application of patient authorization to non-treatment or records-based research is not entirely clear (Liang, 2002). Legal opinion by USDHHS lawyers will be necessary to determine procedures needed to establish an interagency information system on medical errors and near-miss events under the Privacy Rule.

The special exception for FDA reportable events suggests that facilities and providers of health care will be able to report product defects with PIHI to manufacturers, where FDA regulations require such reporting, and manufacturers will be able to report such data to the FDA, all without patient consent. Further, the reporter will not be required to de-identify the data, strictly under the Privacy Act for FDA reportable events. However, most of the data elements considered "directly identifiable" are not routinely captured in current adverse event reporting (e.g., name, SSN). Some PIHI, including service dates, birth dates and device identifiers, as well as text descriptions of the adverse event may be included in adverse event reports. (De-identification protocols prescribed by the Privacy Rule are discussed below.)

While the Privacy Rule specifically permits the use of PIHI for adverse event reporting to the FDA without patient consent, it does not address the sharing and use of such data by agencies other than the FDA. Furthermore, because the Privacy Rule consistently refers to clinical trials as its prototype for research, it is not clear whether safety reporting will be interpreted in parallel with the traditional clinical trial research paradigm as an exception to the required patient authorization when approved by an IRB, thus creating a legal issue and question (Liang, 2002).

More generally, when written authorization by the patient is not specifically exempt and is required for release or use of PIHI, the authorization can apply to multiple purposes (DHHS/OCR, 2001) albeit explicitly described (45 CFR 164.508(c)). This perhaps implies that authorizations can be designed by covered entities for research and quality improvement activities in general, rather than specific to each project – an interpretation requiring USDHHS legal review and corroboration. Also, even when written patient authorization is required by the HIPAA Privacy Rule to release and use PIHI for research purposes, a waiver from that requirement can be issued by an Institutional Review Board (IRB). The IRB can waive the patient authorization requirement when there is no more than minimal risk to the individuals from release of the PIHI based on at least the following (DHHS/OCR, 2001 and DHHS, 2002):

- There is no practical ability to conduct the research without the PIHI and without the waiver.
- There is an adequate plan to protect the identifiers from improper use and disclosure.
- There is an adequate plan to destroy the identifiers as soon as possible, unless otherwise justified by health or research reasons or required by law (see acceptable "research reason" below); and
- There is "adequate written assurance that the protected health information will not be reused or disclosed to any other person or entity, except as required by law, for authorized oversight of the

[3] See, for example, 65 Fed. Reg. at 82516 (clinical trial is one authorization allowed with consent; examples of valid compound consent with authorization for clinical research; "research exception...and health care providers conducting such [clinical] trials..."); 65 Fed. Reg. at 82518 ("except for [research] authorizations requested for clinical trials..."); 65 Fed. Reg. at 82520 ("research that includes treatment...including clinical trials"; "prior to individual's enrollment in a clinical trial[] but that is now providing [the] research-related treatment....).

research project, or for other research for which the use or disclosure of protected health information would be permitted by" the HIPAA Privacy Rule.

(Note the placement of the common in the last bullet after the phrase "except as required by law," creates the impression that the disclosure of PIHI could be required under court order or law enforcement provisions, although research should be protected from such disclosure under the Common Rule.)

The modification to the HIPAA Privacy Rule currently proposed by the USDHHS Secretary would waive the requirement for destruction of the PIHI "if the authorization is for a covered entity to use or disclose protected health information for the creation or maintenance of a research database or repository" (DHHS, 2002). This change was in response to concerns that requiring a date of destruction would create a significant obstacle to the existence of research databases or repositories.

In summary, the Privacy Rule (as proposed to be amended) explicitly would allow for the creation of ongoing research databases and would allow for the use of PIHI without patient authorization, if the research is approved by an IRB or if the data collection relates to information required under FDA jurisdiction. Sharing PIHI outside of the FDA for other purpose, such as research, is not explicitly addressed in the HIPAA Privacy Rule, which raises an important question and potential obstacle for creating a shared medical errors reporting system. S. 2590 and H.R. 4889 are designed to remove this obstacle, should they pass the Congress.

4.3.1.4 State Laws

A number of State laws protect health data in specific circumstances, but generally States do not have comprehensive privacy laws regulating the use and disclosure of PIHI. One study describes the uneven terrain of State health privacy statutes (Pritts et al., 1999). Except where noted below, the review here of State laws is based on that study.

States tend to have different and distinct regulations governing hospital licensure, physician licensure, the insurance industry, and mandatory disease reporting for public health. Some State confidentiality protections are part of larger consumer protections laws. Many State regulations govern only specific medical conditions such as HIV/AIDS, mental health, cancer registries, and communicable diseases. A few States have statutes that approach a comprehensive privacy law. Hawaii comes closest, and Wisconsin and Rhode Island have laws with broad privacy protections. For many States, confidentiality is implied in the code of ethics of health care professionals, and "privilege laws" guard the privacy of patient-doctor communications. "Peer review" laws in the some States protect PIHI assembled by peer-review or quality-assurance committees in health care institutions (Kohn et al., 1999). Often, "States do not impose a duty of confidentiality, but stipulate a penalty for breaching patient confidentiality;" often, the injured party can bring a civil suit; and/or the party that violated disclosure prohibitions can be prosecuted, fined, and/or sent to prison (Pritts et al., 1999). This "uneven terrain" of State laws implies obstacles difficult to predict on any path to integrated reporting across State lines.

The number of laws, if not their complexity, can affect the protection and disclosure of PIHI, and this will undoubtedly affect the sharing of data related to adverse events. Furthermore, because of the preemption of State laws by HIPAA if the state laws are "less strict or inconsistent" with HIPAA, efforts by States to allow for error reporting and data sharing could be preempted. The exemption for FDA safety reports from the data-disclosure prohibition under the HIPAA Privacy Rule is an exemption that should be sought for adverse medical event reporting generally, particularly in light of unevenness of State laws that could affect reporting across State lines to a national error reporting system. This is one of the intents of S. 2590 and H.R. 4889.

4.3.1.5 Patient Safety Improvement Acts – Proposed in the 107th Congress

On June 5, 2002, Senators Jeffords (I-VT), Frist (R-TN), Gregg (R-NH), and Breaux (D-LA) introduced a bill (the Patient Safety and Quality Improvement Act) to provide legal protections for patient safety data

voluntarily submitted to patient safety improvement systems, in order to create incentives for voluntary reporting systems that are non-punitive and promote learning (Washington HealthBeat, June 5, 2002). On June 6, 2002, Representatives Johnson (R-CT) and Thomas (R-CA) sponsored a companion bill in the House of Representatives – the Patient Safety Improvement Act. A summary of the Senate Bill 2590 says, it would ensure that "patient safety information is privileged and confidential and, therefore, cannot be subjected to civil, criminal, or administrative subpoena." Such information would not be "subject to discovery in connection with a civil, criminal, or administrative proceeding; disclosed pursuant to the Freedom of Information Act; admitted as evidence in any civil, criminal, or administrative subpoena; or utilized to carry out an adverse personnel action." However, "a provider or PSO [patient safety organization] could disclose relevant information to the FDA, and share information as part of the business relationship between a PSO and a provider." (Washington HealthBeat, June 5, 2002). The House bill also contains a "conflict of interest" provision that prevents a patient safety organization that is also a regulatory body, such as a health department, from using the report to levy sanctions against health care providers. Both bills contain penalties for breach of confidentiality, but they differ on the stiffness of the penalties (Washington HealthBeat, June 7, 2002).

The Senate bill also includes authority for USDHHS to create a de-identified national database on medical errors, based on voluntary reports from patient safety organizations. Those data would be "privileged and confidential." USDHHS would be mandated to develop or adopt voluntary national standards within 36 months to promote the integration of health care information technology systems. The House bill ties some administration of patient safety improvement to CMS to improve the interoperability of computer technology for reporting errors – an attempt to avoid the proliferation of different information system approaches, which made development of HIPPA data standards for administrative simplification of claim transactions so difficult and costly.

Tripartisan support for the Senate bill and bipartisan support for the companion bill in the House engender hope that the 107th Congress might pass legislation to promote the reporting and learning from medical errors on a national level.

4.3.2 Shielding PIHI from Legal Discovery

Protecting personally identifiable health information (PIHI) in records systems from legal discovery is *necessary* to encourage reporting and enable learning from medical mistakes (Kohn et al., 1999). "Discovery" in this sense is a court process by which each party can obtain evidence in the possession of the other party and nonparties. Persons or organizations that are not parties in a lawsuit also can be compelled to provide evidence. There are two methods for shielding PIHI from legal discovery – laws and de-identification of the data. This section considers existing laws (before passage of S. 2590 and H.R. 4889) that prevent discovery; the next section describes de-identification.

4.3.2.1 The Laws

Currently, no single law explicitly protects PIHI that crosses State lines for national error reporting (Kohn et al., 1999). Some laws prevent discovery of PIHI collected for specified purposes. The HIPAA Privacy Rule strengthens the privacy of personally identified data from the patient's perspective and applies to essentially all organizations that hold personally identifiable health information (PIHI). The legal system has always had access to medical records through hospital medical records departments, and sometimes without a warrant. DHHS says that the courts will have no added access to medical provider records through the HIPAA Privacy Act and will now be required to obtain a warrant for such information (DHHS/OCR, 2001). However, the rule *does* permit the legal system to obtain PIHI through such official processes. Thus, the new HIPAA Privacy Rule will not fully protect medical error reporting from legal discovery. The ramification for reporters of medical errors is risk of discovery and malpractice suits that will discourage reporting to State or national medical error information systems.

Some States (e.g. Georgia) have strong laws to protect data systems developed and used for peer review, risk management, and quality improvement – known as "peer review" laws. However, these laws often apply only to data collected and presented within the peer-review committee meeting room. Once such data are shared beyond the peer-review body, they are no longer protected *per se* by "peer-review" privilege and thus become vulnerable to legal discovery.

Some very specific State laws protect PIHI from discovery by law enforcement (Pritts et al., 1999), for example:

- Colorado for HIV/AIDS, cancer, communicable, and venereal disease registries (Colo. Rev. Stat. Ann. '25-4-1404 and '25-1-122);
- Connecticut for mental health records from publicly funded hospitals;
- Nebraska for all patient-identified research data and specific condition registries (Neb. Rev. Stat. '81-699, '71-503.01).

More generally, peer-review privilege does not protect administrative information such as incident, occurrence, or investigation reports; documents in the possession of and information known to the hospital's board and CEO; and, more generally, information originating outside the peer- review process and available from other sources (Liang, 2002). Besides not applying to all types of administrative information, peer review privilege is highly variable among States. Some State statutes cover only information generated by particular providers such as hospitals while ignoring other provider forms such as managed care organizations; some State laws focus on the for-profit or not-for-profit status of the entity in extending peer review protections, Further, State peer review privilege coverage is subject to interpretation by multiple courts in multiple States, making predictability of its coverage uncertain (Liang, 2002).

In the context of U.S. Supreme Court jurisprudence, there has been a significant common law trend of narrowing privilege "in favor of full disclosure of relevant facts" (Liang, 2002). Broader discovery trends have also recently been extended to Medicare Peer Review Organizations. A Federal court has ruled that reviews made by these organizations regarding quality of care initiated by patients and/or their representatives, previously confidential, now must be reported to these individuals within 20 days of completion (see Public Citizen, Inc., v. Department of Health and Human Services, — F.Supp.2d —, 2001 WL 800013 (D.D.C. July 9, 2001)). Although under appeal, were the ruling to stand, then release of information could be required simply as a result of a complaint from a Medicare beneficiary or his/her representative (that is, attorney). This case has potential to allow legal maneuvering for plaintiff's attorneys to obtain sensitive information from providers that might otherwise be unavailable (Liang, 2002).

Court access does not extend to all sources or routes of information out of the institution. The Federal Privacy Act and Federal agency authorizations protect Federal data collection. The Common Rule protects data collected for Federally funded research from discovery. Research under the Common Rule is protected from legal discovery, although private research that has not been vetted by an IRB is not. The HIPAA Privacy Rule, which will require private research to be subject to IRB approval, would protect data from privately funded research from legal discovery via the Common Rule.

However, this piecemeal circumstance-by-circumstance, State-by-State, and condition-by-condition approach provides a riddled shield to protect PIHI from discovery in the courts (Pritts et al., 1999). While some State "privilege laws" protect information collected under the peer-review process, other State data protection laws include an exception for law enforcement. Those States allow discoverability of confidential data with a proper and valid subpoena, court order (criminal or civil), and/or warrant. Furthermore, due to the dual-track State and Federal court systems, privileges in State courts do not generally apply to Federal courts. Thus, if a claim is brought and a request for discovery of error reports and information is made in Federal court, Federal courts are not required to, nor would they typically, apply state peer review privilege; discoverability would generally be allowed in such cases (Liang, 2002).

4.3.2.2 Implications of Discoverability for Integrated Reporting Systems

The Federal Privacy Act of 1974 and the Common Rule governing research on human subjects are shields that protect federally supported PIHI from discovery in court. Adverse medical event reporting as part of a federally sponsored research project would be protected from discovery in court. However, medical errors collected for operational activities by private entities and shared outside the organization may not be.

Furthermore, because the Privacy Act states that data collected by the Federal government may not be used for any purpose other than the purpose for which it was collected, the purpose of each data set that is a candidate for integration must be reviewed. And, that review must evaluate whether or not and under what circumstances data from each system of records can be shared across agencies. For example, if hypothetically an agency's statute authorizes personally identifiable data collection but does not allow those data to be shared outside the agency, then it cannot be linked to personally identified data in another agency's reporting system. The integration design must ensure that data collected for one purpose is not shared with another institution, unless it is de-identified.

The absence of laws that fully protect reports of adverse medical events, particularly in the private sector, contributes to the existence of systems that exclude PIHI. For example, subscription-type medical event reporting systems usually exclude from event reports any data on the patient, provider, or reporter. This creates silos of data systems that cannot be linked to maximize understanding of the extent of, causes of, and trends in medical errors and close calls in the U.S. A solution to the problem of lack of confidentiality protections of private-sector PIHI is needed to protect and stimulate data sharing of medical event data on a national level. This is the goal of S. 2590 and H.R. 4889, described above.

4.3.3 De-identification of Personally Identifiable Health Information

A plan for a DHHS integrated reporting system must protect the confidentiality of PIHI, even when it is to be released for research purposes. Some safe approaches for doing so while integrating reporting systems across DHHS agencies are either to:

- Collect no PIHI under each system,
- Integrate only de-identified data into any data-warehouse design,
- Designate the system for purposes of research.

According to the HIPAA Privacy Rule "a covered entity may always use or disclose protected health information for research purposes that has been de-identified" (DHHS/OCR, 2001). De-identification must be in accordance with 45 CFR §§164.502(d), 164.514(a)-(c) of the Privacy Rule and §164.514[a][b]. The Secretary (DHHS, 2002) has indicated a willingness to change the strict de-identification requirements under those sections, if the research community proposes alternative specifications for de-identification that sufficiently protect PIHI in research environments. Because it is not possible to determine what those changes might be, below we describe the de-identification protocol as required under the HIPAA Privacy Rule published December 28, 2000. Because such de-identification standards would have important implications for the integration design, they are shown in full here:

- Only a technically qualified person (as stipulated in the Privacy Rule) may de-identify PIHI.
- A qualified person must determine that "the risk is very small that the information could be used, alone or in combination with other reasonably available information… to identify an individual who is a subject of the information."
- The methods and results of such an analysis must be documented.

Or,

- "The following identifiers of the individual, or of relatives, employers, or household members of the individual, are removed:

- Names
- All geographic subdivisions smaller than a State, including street, address, city, county, precinct, zip code and equivalent geocodes (except for the initial three digits of a zip code if, according to [current Census Bureau data],
  - The geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and
  - The initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000.
- All elements of dates (except year) for dates directly related to an individual,
  - Birth date
  - Admission date
  - Discharge date
  - Date of death
  - All ages over 89 and all elements of dates (including year) indicative of such age
  - Such ages and elements (of ages over 89) may be aggregated into a single category of age 90 or older
- Telephone numbers
- Fax numbers
- Electronic mail addresses
- Social security numbers
- Medical record numbers
- Health plan beneficiary numbers
- Account numbers
- Certificate/license numbers
- Vehicle identifiers and serial numbers (including license plate number)
- Device identifiers and serial numbers
- Web Universal Resource Locators (URLs)
- Internet Protocol (IP) address numbers
- Biometric identifiers (including finger and voice prints)
- Full face photographic images and any comparable images
- Any other unique identifying number, characteristic, or code

And,

- The covered entity does not have actual knowledge that the information could be used alone or in combination with other information to identify an individual who is a subject of the information."

The HIPAA standards for de-identification are extreme and would preclude the linkage of any auxiliary data, such as population denominators for geographic areas. For example, with this standard of de-identification, it would be impossible to develop population counts for carefully defined market areas (at less than the three-digit level of the ZIP code) of hospitals or nursing homes to derive indicators of patient safety that relate in an accurate way to the population that the institution draws from and serves. To share data across agencies and outside of DHHS, data will have to go through significant de-identification to be compliant with the HIPAA Privacy Rule.

Guidance has not yet been developed on how "qualified persons" will show that a project or system will result in a "very small" risk that information disclosed will not identify an individual (Liang, 2002). Further, de-identification itself may impede analysis of medical errors because of the inability to obtain and link additional information on an event. Also, the HIPAA de-identification list includes the catch-all phrase, "any other unique identifying number, characteristic, or code". Scenarios do exist where rare, serious, publicized cases, such as wrong-sided limb amputation, would by their characteristics and timing be identified regardless of HIPAA de-identification procedures. Such an event would have to be removed

from a national database under the current HIPAA de-identification procedures, and that would preclude the ability to study and learn from high-profile serious errors nationally. The process of de-identification in the context of medical errors, which are rare, may significantly restrict the content of a national medical error database (Liang, 2002).

4.3.4 Legislation and Regulations Governing Relevant DHHS Systems

Federal legislation authorizing government activities and regulations devised to implement such laws affect what data can be collected by Federal agencies and what can and cannot be done with such data. In this section, we review legislation that authorizes various activities of the four DHHS agencies that might be part of an integrated medical error reporting system and note specific limitations on sharing that information with other Federal agencies.

We assembled this overview for review by agency lawyers who are familiar with the many laws and rules that affect each agency's activities. *Those reviews have not yet been requested*. Before work proceeds on development of a DHHS-wide medical error reporting system, agency lawyers should write opinions on the legal obstacles to integrating the medical error reporting systems and related databases of the four DHHS agencies and any changes that must take place in agency regulations or authorizations. This report provides an overview of the planned system and the next section should serve as a start on the legal issues specific to the agencies.

4.3.4.1 AHRQ

AHRQ is authorized to collect data for research purposes related to health care quality among other topics (42 USC §299(b) and §299a). AHRQ is not authorized to release PIHI. According to 42 USC 299c-3 (Public Health Service Act §924(c)):

"No information, if an establishment or person supplying the information or described in it is identifiable, obtained in the course of activities undertaken or supported under this subchapter may be used for any purpose other than the purpose for which it was supplied unless such establishment or person has consented (as determined under regulations of the Director) to its use for such other purpose. Such information may not be published or released in other form if the person who supplied the information or who is described in it is identifiable unless such person has consented (as determined under regulations of the Director) to its publication or release in other form." Staff violating this statute is liable for civil monetary penalty of no more than $10,000 per violation.

Thus, all data sets that the AHRQ releases are de-identified with respect to persons and establishments or, in the case of HCUP, are restricted to research purposes under a data license agreement. Furthermore, public use data sets are being revised to be compliant with HIPAA de-identification standards.

The AHRQ Healthcare Cost and Utilization Project (HCUP) databases and software products are relevant for inclusion in a DHHS integrated reporting system. They could be useful in three ways. First, HCUP could be used to develop denominators for populations hospitalized for specific conditions or treatments, whether common or rare. Second, HCUP data could be analyzed with the HCUP Patient Safety Indicators (PSIs), a software package that calculates aggregate measures based on errors and complications coded by hospitals using the ICD-9-CM coding system. While the PSIs are not definitive measures of patient safety, they can be used to assess the trends in reporting of errors in discharge records compared to reporting to other sources. Third, the HCUP PSIs could be applied to other claims-based data sets that use ICD-9-CM coding, such as the CMS data. HCUP data use restrictions either would limit some data elements from inclusion (e.g., hospital identifiers) or would likely have to be renegotiated with State agencies and hospitals contributing the data in order to be included in a medical event reporting database warehouse.

4.3.4.2 CDC and NCHS

The Centers for Disease Control and Prevention are authorized to perform a variety of activities to protect the public health and to collect data in the process. The CDC includes the National Center for Health Statistics (42 USC §242k, §242l, §242m), which is authorized to collect data for "statistical and epidemiological activities for the purpose of improving the effectiveness, efficiency, and quality of health services in the United States." NCHS tracks the Nation's vital statistics on births and deaths, health status, and health care utilization, among other trends, and reports on these trends (42 USC §242m). NCHS is not authorized to release any PIHI. The NCHS public-use datasets could be incorporated into an integrated DHHS reporting system. They would be useful for developing denominators for the U.S. population with specific diseases. To the extent that NCHS surveys collect or are redesigned to collect information on adverse outcomes for patients, they might serve as stand-alone indicators of health care quality and safety over time. It is unlikely that they would produce definitive estimates of medical errors, because patients affected by errors or near misses may have no knowledge of them.

Other CDC authorizations are contained in various sections of the Public Health Service Act. For example, CDC must study sentinel diseases and occupations (42 USC §241); must screen for, test for, and disseminate information about lead poisoning (42 USC §247b-1 and §247b-3); improve data linkages between State and local health departments and between them and the CDC (P.L. 106-310, Sec. 2501(c), 114 Stat. 1161); study birth defects and developmental disabilities (42 USC §247b-4); promote orphan drug and biologic products with the FDA (42 USC §236); prevent and control sexually transmitted diseases (42 USC §247c); respond to public health emergencies (42 USC §247d) such as anti-microbial resistance (42 USC §247d-5) and bio-terrorism (42 USC §247d-6 and §247d-7); support research to prevent and control injuries (42 USC §280b); and study and prevent adverse reactions to vaccines (42 USC §300aa-2); among other duties. To prevent injuries, Congress requires the CDC "to promote coordination between Federal, State, and local governments and public and private entities in order to achieve a reduction in deaths from injuries."

The CDC, including NCHS, is under statutory confidentiality protections (originally pertaining to NCHS data collection) (42 USC 242m(d); and Public Health Service Act , section 308(d)). This statute, stronger than the Federal Privacy Act of 1974, provides that: "No information, if an establishment or person supplying the information or described in it is identifiable, obtained in the course of activities undertaken or supported under section 242b, 242k, or 242l of this title may be used for any purpose other than the purpose for which it was supplied unless such establishment or person has consented (as determined under regulations of the Secretary) to its use for such other purpose; and in the case of information obtained in the course of health statistical or epidemiological activities under section 242b or 242k of this title, such information may not be published or released in other form if the particular establishment or person supplying the information or described in it is identifiable unless such establishment or person has consented (as determined under regulations of the Secretary) to its publication or release in other form."

Because of this statute, all identifiers of persons or establishments (including hospitals or other health care settings) would have to be removed from any dataset that is releasable through a data warehouse pertaining to medical error reporting. Both AHRQ and NCHS/CDC statutes make no exception for disclosure to law enforcement agencies or court systems. Furthermore, USDHHS lawyers have argued that grantees funded by AHRQ have no discretion to disclose PIHI for litigation or for criminal, administrative, or legislative proceedings (Merewitz, 1995).

4.3.4.3 CMS

The Centers for Medicare and Medicaid collects personally identifiable health information (PIHI) in relation to the Medicare and Medicaid programs. Like other Federal agencies, CMS must adhere to the Federal Privacy Act (5 USC 552a). CMS also must adhere to privacy provisions of the Social Security Act (42 USC 1306) for data that it collects. The Social Security Act requires that: "no disclosure of any

such file, record, report, or other paper, or information, obtained at any time by any person from the head of the applicable agency or from any officer or employee of the applicable agency, shall be made except as the head of the applicable agency may by regulations prescribe and except as otherwise provided by Federal law." Violators may be found guilty of a felony and fined up to $10,000 per violation and/or imprisoned up to 5 years. Also, CMS as a *de facto* health plan also must comply with the HIPAA Privacy Rule (45 CFR Parts 160 and 164)**,** regarding the transfer of personally identifiable health information. Personally identifiable data may be released only to adjudicate claims, pay bills, and conduct research. Legal discovery appears possible with respect to CMS data.

For research uses, CMS has established policies that govern the "sharing" of identifiable data, which ensure that those data remain confidential. Health data release policies are explained in guides to users of CMS data (see, for example, BDMS (1993). For example, if a CMS employee wishes to gain access to identifiable data, they must complete a request for information. CMS only releases PIHI to users who have a "need to know." If the requestor intends to release the data to a contractor or grantee, then both parties must sign agreements promising to guard the confidentiality of the data. The same rules apply to other Federal employees or anyone outside government; they must submit a research protocol and sign data use agreements. The CMS determines the requestor's need for the data using criteria of the Common Rule governing research:

- The project cannot be accomplished without use of PIHI.
- The benefits of the research far outweigh any risk posed on individual privacy.
- Researchers will protect data confidentiality and PIHI will be removed from the dataset as soon as possible.
- The research protocol is reasonably defined so as to ensure a high probability of success with the use of personally identifiable data.

Thus, in general, CMS data could be released for construction of a national medical error reporting system, but CMS would likely require de-identification before any release of those data.

4.3.4.4 FDA

FDA has authority to collect information on medical products to monitor and protect the safety of those products (21 CFR Part 310 §305 (a) for MedWatch and AERS; 21 CFR Parts 803 and 807 for MAUDE; 21 CFR Part 606, §171 for blood products). Since the objective of an integrated DHHS system would be to enhance the monitoring of the safety of health care, incorporation of FDA systems in an integrated DHHS reporting system should fall within the FDA designated authority. FDA systems generally do not include PIHI because FDA data systems focus on products, not patients or providers. FDA systems sometime include information on reporters of the adverse events; those data would have to be protected with controlled access on a need to know basis and should not be part of any data shared among agencies. FDA systems also include identifying data on manufacturers, which would be considered confidential under 18 USC 1905, unless release of such is permitted by other FDA statute.

Language of 18 USC 1905 states that: "Whoever, being an officer or employee of the United States or of any department or agency thereof, any person acting on behalf of the Office of Federal Housing Enterprise Oversight, or agent of the Department of Justice as defined in the Antitrust Civil Process Act (15 U.S.C. 1311-1314), publishes, divulges, discloses, or makes known in any manner or to any extent not authorized by law any information coming to him in the course of his employment or official duties or by reason of any examination or investigation made by, or return, report or record made to or filed with, such department or agency or officer or employee thereof, which information concerns or relates to the trade secrets, processes, operations, style of work, or apparatus, or to the identity, confidential statistical data, amount or source of any income, profits, losses, or expenditures of any person, firm, partnership, corporation, or association; or permits any income return or copy thereof or any book containing any abstract or particulars thereof to be seen or examined by any person except as provided by law; shall be

fined under this title, or imprisoned not more than one year, or both; and shall be removed from office or employment."

FDA lawyers should be consulted on whether any of the FDA statutes permit release of identifying information on manufacturers.

4.3.4.5 Implications for DHHS Integration of Authorizing Regulations Governing these Databases

Based on most agencies authorizing laws, the Federal Privacy Act of 1974, and the HIPAA Privacy Rule (to take effect next year), any personal data collected by any of four DHHS agencies must be de-identified before it is released publicly. Any integration effort would have to protect each agency's PIHI carefully. (The next section describes HIPAA-compliant security rules for protecting PIHI.)

Sharing of data among agencies without public disclosure may be feasible under the Common Rule for Protection of Human Research Subjects, under special provisions of certain agency statutes, and under inter-agency agreements. Authorizing legislation of USDHHS agencies that is written as directives to the Secretary of HHS (as opposed to directives to agency heads) may overcome some inter-agency sharing limitations. However, agency lawyers must be consulted for legal opinions on what can and cannot be shared among agencies for purposes of linking information on medical errors and for whether new legislation is required to permit access to PIHI between or among agencies involved in such integration.

Beyond agency legislative constraints, the major hurdle and disincentives for reporters of medical errors is the discoverability of data that are reported to a national medical error reporting system. National legislation will be necessary to protect medical error reports from discovery so that reporting is encouraged and a program of national learning can commence. Hope for such legislation now lies with the 107th Congress.

4.3.5 Security Requirements for Integration

The goal of the HIPAA Security Rule is to provide a comprehensive framework to guide the protection of the confidentiality, integrity, and availability of personal electronic health data. In general, the Privacy Rule identifies what information should be protected. The Security Rule identifies how it should be protected.

The proposed Security Rule was published on August 18, 1998. The final Rule is expected to be released in June 2002. Depending upon their size, covered entities will have two to three years (from the date the Final Rule is published) to comply.

The proposed Security Rule identifies approximately 20 requirements across four categories:

- Administrative procedures
- Physical safeguards
- Technical security services
- Technical mechanisms

The core requirements are:

- Certification
- Media controls
- Chain of trust partner agreement
- Physical access controls
- Contingency plan
- Policy guideline on work station use
- Secure work station location
- Formal mechanism for processing records

- Security awareness training
- Information access control
- Access control (context based)
- Internal audits
- Audit controls
- Personnel security
- Authentication
- Security configuration management
- Authorization control
- Security incident procedures
- Cryptography
- Termination procedures
- Unique user identification
- Training
- Communication network controls
- Assigned security responsibilities
- Digital signature

Requirements are generally "scalable" depending on the size of the covered entity. The Security Standard was developed with the intent of remaining "technologically neutral" and does not prescribe that specific systems or software be used.

The implication of the HIPAA security standard for the DHHS integration of medical error reporting systems is that the design for the integration should comply with the HIPAA standard and must accommodate the reporting facility's obligation under HIPAA security provisions. Because reporting facilities will have varying capabilities, security features must be transparent to those reporting events to the system. However, specific issues of note include:

- The need for context-based access control will require the establishment of appropriate protocols and security regarding both reporting of events and access to the data that is created. As a practical matter, explicit designation of "adverse event reporting staff" within the user facility is likely to be required.
- Each agency that will have access to the integrated data must have written policies and plans that address the core requirements listed above, such as work station use and location; security awareness training; assigned security personnel and management; internal audit procedures, authorization control, and security incident procedures, among others.

4.4 Lessons Learned from Error Reporting Systems Outside DHHS

4.4.1 The Department of Veterans Affairs (VA) Patient Safety Program

The VA has been a leader in patient safety initiatives. Its medical error reporting programs are hospital-based programs that focus on quality improvement. Several systems in the VA health care system relate to patient safety:

- The Patient Safety Information System (also referred to as the Root Cause Analysis (RCA) System), a program of the VA National Center for Patient Safety (NCPS, undated)
- The Patient Safety Reporting System (PSRS), a joint program of the VA and the National Aeronautics and Space Administration (VA and NASA, undated; Bagian et al, 2002)
- The National Surgical Quality Improvement Program (NSQIP), a VA-wide program being extended under an AHRQ grant to 10 facilities outside the VA (Khuri, 2001).

It is important to note that legal barriers to reporting errors in the VA are less overwhelming and that privacy protections of reports are unique in the VA systems due to their status as a Federal government

health care entity (Liang, 2002). The Federal Tort Claims Act limits liability of Federal employees including VA employees; they are not subject to personal liability as standard community practice providers are; there is an administrative, workers-compensation-type scheme for injured veterans; and the patient populations are different. The VA population consists of older men with significant chronic illness compared with the broader, healthier community population including younger females with acute conditions. The latter class of patients subjects a provider to significantly higher damages in a patient injury lawsuit (Liang, 2002). These differences and the lack of malpractice liability may account for some of the success of the VA in instituting landmark safety systems in health care.

4.4.1.1 The Patient Safety Information System

The Patient Safety Information System at the VA is part of the Patient Safety Program, which aims to prevent injuries to patients, visitors, and personnel through steps to build trust in the safety system and make safety a part of all employees (NCPS, undated). The program, which is in VA facilities nationwide, is a never-ending process devoted to developing a "culture of safety." Emphasis is placed on the importance of reporting and analyzing close calls. "Close calls are important because they present opportunities to learn without the pain of an actual mistake." The building blocks are: comprehensive identification and reporting of adverse events, sentinel events, and close calls of all types that occur in hospitals; assessment of reports using the Safety Assessment Code matrix (a VA instrument described above) to determine whether to initiate an in-depth review; and review of serious or high probability adverse events, sentinel events, and close calls to identify underlying causes. Determination of cause is aimed at system changes needed to reduce the likelihood of recurrence and is not intended to punish individuals involved. In addition, patient safety alerts and lessons learned are disseminated throughout the VHA. Prospective analyses of service delivery systems are implemented before adverse events occur to identify system redesigns that would reduce the likelihood of harm.

The Patient Safety Information System contains identified reporting (on the patient, provider, reporter, and institution involved). The system is mandatory in VA facilities and encourages voluntary reporting to the JCAHO Sentinel Events Database (see below). The system uses the related JCAHO classification for sentinel events.

Privacy of the data received by the patient safety manager or obtained from root cause analyses is protected from disclosure as part of a medical quality assurance program (38 USC 5705). The Privacy Act of 1974 limits disclosure to families. The VA authority (38 USC 7332) limits disclosures of information on patients treated for substance abuse (including alcohol), sickle cell anemia, and Human Immunodeficiency Virus (HIV) (even after a patient's death).

4.4.1.2 Patient Safety Reporting System (PSRS)

In May 2000, the VA and NASA developed an interagency agreement to develop a Patient Safety Reporting System (PSRS) for the VA (VA and NASA, undated) modeled after NASA's long-standing Aviation Safety Reporting System (ASRS) (NASA and FAA, 1999). (The ASRS collects, analyzes, and responds to voluntarily submitted aviation safety incident reports (including close calls) in order to lessen the likelihood of aviation accidents. ARSA helps to identify deficiencies so they can be remedied; support policy and plan safety improvements; and strengthen the foundation of aviation human factors safety research. It is generally conceded that over two-thirds of all aviation accidents and incidents have their roots in human performance errors. ASRS has been lauded for its strict confidentiality procedures, managed reports, database created for the easy retrieval of information, creation of safety products and distribution of safety information. The ASRS is described in more detail in Appendix N. The knowledge and experience of ASRS is being applied to the PSRS.

PSRS encourages reporting of medical adverse events, sentinel events, and close calls through a fully anonymous, externally managed system that covers all types of adverse events in health care and

complements the mandatory internal reporting of the VA system. All VA medical facility staff may voluntarily report any events or concerns that involve patient safety, and NASA, not the VA, processes these reports to maintain strict confidentiality. The PSRS also is guided by principles of non-punitive reporting. As a complimentary system, PSRS will identify vulnerabilities, but will not provide detailed solutions, as in the case of events that are reported internally and subjected to the root cause analysis.

Easily the most confidential and privacy-concerned system reviewed here, it has the same statutory protections as the internal VA system, plus it de-identifies all reports. Both closed (check box) and open-ended (narrative) data are collected on the PSRS form (VA and NASA, 2001).

4.4.1.3 The National Surgical Quality Improvement Program (NSQIP)

The NSQIP is "a risk-adjusted adverse event reporting system for major surgical operations in the Department of Veterans Affairs (VA)" (Khuri, 2001) that has been in effect since 1990. Trained nurses 123 VA hospitals across the nation review records and submit adverse event reports to the system. Data are confidential and feedback is provided mainly through annual peer evaluations and through an internally distributed annual report. NSQIP collects data on all surgical procedures performed (CPT-4 codes), patient characteristics for risk adjustment (pre-surgical indicators) and patient outcomes (33 measures), as well as workload data. Reporting is anonymous and hospitals are de-identified. Patients are identified by age and postal address.

This system is currently the subject of an AHRQ grant to the VA Boston Healthcare System and the American College of Surgeons (Khuri, 2001). The study plans to apply NSQIP to ten non-Federal institutions. The study will use the ten sites to implement and evaluate the success of four interventions and assess the ability of the NSQIP to identify, manage, and reduce medical error. The evaluators plan to adapt the NSQIP and offer it as a model (at least) for a national error reporting system for all surgery programs.

4.4.1.4 Implications for DHHS Integration

The VA should be considered a crucial partner in the development of a nationwide error reporting system, especially one focused on hospital reporting, and in DHHS-wide integration. The VA inclusion of all types of errors and their classification for determining which events to explore for a root cause are specific items that could be used wholesale or adapted for a DHHS integration that supports quality improvement at the point of care. The VA experience in mandatory error reporting and its new experience in voluntary reporting modeled after the Aviation Safety Reporting System offer an important juxtaposition for comparing different approaches to adverse event reporting.

4.4.2 The Department of Defense (DOD) Patient Safety Registry (PSR)

The Department of Defense (DOD), Military Health System, Patient Safety Registry (PSR) is modeled after the VA Patient Safety Program. The goals of the DOD patient safety program are to prevent or minimize the occurrence of adverse outcomes consequent to medical care (and thus to improve patient safety and health care quality) and provide a safe environment for patients, visitors and staff. The program strives to do this through comprehensive monitoring, standardized reporting, and thorough analysis of untoward events. The Patient Safety Registry is exclusively for learning and for improving systems and processes, not for punitive or disciplinary action.

The Department of Defense Patient Safety Work Group (PSWG) was established in January 2000 to develop an error tracking and reporting process for all military health care facilities following IOM recommendations and later incorporating specific legislative mandates. The plan was to use both mandatory and voluntary reporting systems similar to the VA Patient Safety Reporting Program. The Patient Safety Center at AFIP, which became operational April 2001, collects and analyzes patient safety information from all military treatment facilities (MTFs). The confidentiality of the PSR medical quality

assurance records are protected under 10 USC 1102. The PSR also uses the VA Safety Assessment Code (SAC) Matrix scoring system and the VA Root Cause Analysis system.

4.4.3 State Error Reporting Systems

Sixteen States have adverse event reporting systems (Rosenthal et al., 2001; IOM, 1999). The States are:

- California[4]
- Colorado
- Florida
- Kansas
- Massachusetts
- Nebraska
- New Jersey
- New York
- Ohio
- Pennsylvania
- Rhode Island
- South Carolina
- South Dakota
- Tennessee
- Texas
- Washington

A few States are involved in development of new systems or are revising systems with the help of AHRQ grants. These are:

- Utah, using the Utah Hospital Discharge Database (UHDDB)
- Missouri and the Patient Abstract System (PAS)
- Georgia, through the Georgia Hospital Association's (GHA) Accountability and Health Safety (AHS) Program
- Wisconsin, using the Wisconsin Medical Injury Reporting System (WMIRS)
- Mississippi, with the Mississippi Medical Error Reporting system

The State error reporting systems vary widely in almost every attribute: how they define reportable events, what type of related data they collect, how they collect it, who must report, whether reporting is mandatory or voluntary, how data confidentiality is protected, and so forth. Many States do not support the adoption of national definitions of adverse events and standard classifications, fearing that national standards would diminish their capacity to customize reporting to local priorities and could lead to more Federal oversight.

Most State systems are based on regulatory mandates and pre-date the IOM report and the approach of developing a "culture of safety" and eschewing the "culture of blame." Most also were designed to document, sanction, and punish adverse outcomes for licensing, accreditation, and other regulatory purposes and were not designed to improve quality through learning and feedback. These systems also may be subject to legal discovery and State Freedom of Information Act Requests. As a consequence under-reporting is serious problem among State systems. In addition, State systems vary in technological sophistication: some are entirely Web-based, while others are paper-based systems.

[4] The California system, established in 1972 by the State legislature and identified by the IOM (1999) as active in 1998 with over 4,000 reports, was not identified by the NASHP (Rosenthal et al., 2001) because the response to the their survey was that California did not have a mandatory reporting system.

Coalitions for patient safety have been developing in the States to bring together various stakeholders in health care in order to reduce the risk of error to patients (Comden and Rosenthal, 2002). These coalitions include competing health care providers, insurers, purchasers, medical societies, State government, and others. Seventeen States have developed these coalitions and the National Academy of State Health Policy has summarized the experience of seven State-wide coalitions in existence for two or more years. Lessons for developing such coalitions indicate that innovative partnerships are beginning to emerge within the States to change the culture of blame and punishment into an environment of learning and safety. Some divergent views about accountability and legal liability cannot be resolved in these groups and are taken "off the table" in order to make progress on common issues that can reduce the risk of medical errors.

4.4.3.1 Implications for Integration of State Systems with a DHHS System

For State error reporting systems to be integrated nationally and useful for learning, State systems would need to be more standardized. Nevertheless, it might be feasible to incorporate a few State systems into DHHS integration. For example, New York has had a mandatory adverse event reporting system for hospitals in place since 1985 (NYPORTS); because it is now Internet-based, integration would be technically feasible. Then the DHHS system could be designed to incorporate data reported by institutions to the State, assuming any political objections at the State or provider level could be overcome. State systems that would adapt definitions, classifications, and data collection methods to fit within DHHS integration would be more easily integrated. If such changes were widespread among the States, DHHS could build on an *infrastructure* of State systems, much like the HCUP discharge database is built on a sophisticated network of State discharge data collection activities. However, State error reporting systems have not yet benefited from or coalesced around uniform definitions and classification standards. That was the keystone of State discharge data systems, which were patterned since the 1980s on the uniform hospital discharge dataset (defined by the National Committee on Vital and Health Statistics) and the uniform hospital bill.

At a minimum, lessons can be learned from the States and AHRQ is funding such studies. Finally, States without reporting systems or with systems still under development might look to the DHHS integration effort as a model for their own work.

4.4.4 Joint Commission on Accreditation of Healthcare Organizations (JCAHO) Sentinel Events Database

The Sentinel Events Database is part of JCAHO's Sentinel Events Policy (JCAHO, 2002a). The Sentinel Events Policy is two-fold. First, as a part of the accreditation process, JCAHO defines a minimum set of medical errors (sentinel events) for which institutions must devise mechanisms to identify, report, and analyze the events; institutions may expand upon this list. Reporting a sentinel event to JCAHO is described as voluntary, although it is required for accreditation, as the guidelines in the JCAHO accreditation manual make clear. Second, the Sentinel Event Policy requires that JCAHO review an organization's response to an event and the organization's root cause analysis. However, due to discoverability and other legal considerations, JCAHO reviews and validates root cause analysis during accreditation surveys and does not assemble all relevant data into a database. JCAHO developed its Sentinel Events Database specifically to exclude organization, caregiver, and patient identifiers, primarily because of legal discoverability (Crafton, 2002).

The purpose of the Sentinel Events Database is to gather information on sentinel events (catastrophic medical errors), their root causes, and remedial strategies, thus forming an evidence base of knowledge to share with the greater healthcare community. JCAHO estimates that they receive less than 1 percent of actual medical errors (JCAHO, 2002b). Although the database contains only a small number of events, JCAHO believes it is enough to identify patterns of root causes and event risk reduction (Crafton, 2002). JCAHO developed its own sentinel events taxonomy internally, the major categories of which include:

medication error, procedure complication, wrong site surgery, treatment delay, and transfusion death. JCAHO strongly advocates development of a uniform national taxonomy of medical events and would collaborate with other parties with the same intention (Crafton, 2002).

Implications for Integration: Because JCAHO captures only a small proportion of medical errors in U.S. health care institutions – less than 1 percent – it is not a strong candidate, per se, for integration with DHHS medical error reporting systems. However, some conceptual approaches of the Sentinel Events Reporting and Root Cause Analysis are appropriate for incorporation. In fact, many "home grown" hospital systems are likely to have done so. For example, the Patient Safety Network of the University Healthcare Consortium (UHC) incorporates guidelines of JCAHO related to patient safety such as anonymous reporting, de-identified collection of information, and root cause analysis categories of the JCAHO. JCAHO's Root Cause Analysis process is considered thorough and a paradigm for an evidence-based system for identifying the underlying systemic causes of medical errors. Presently, JCAHO does not use a medical error taxonomy in common with anyone else. The Sentinel Events Database is not designed be statistically representative and therefore cannot be used by individual organizations to benchmark themselves against their own or a national set of data. There is no active feedback mechanism that would give organizations valuable evidence-based data to reduce their own rate of medical errors.

4.4.5 MedMARx

MedMARx is an interesting model for hospital-based medication error reporting. It was developed in 1998 and is maintained by the United States Pharmacopoeia (USP, undated(a)). Hospitals subscribe to MedMARx and contribute drug-related error reports anonymously on actual and potential errors in their facilities to an Internet-accessible database. In return, they can access their own data and the aggregated experience of all subscribing hospitals. About 500 of the 6,200 hospitals in the U.S. currently subscribe and subscriptions have been growing rapidly. MedMARx differs from the FDA MEDWATCH in that MedMARx enables hospitals to monitor internally their progress toward error prevention, view how they compare with other institution, and learn how other hospitals devise solutions to systemic errors.

The MedMARx system requires anonymous input. Total anonymity of the program overcomes one of the major obstacles (legal discoverability) to reporting and sharing incident report information and experiences among facilities through a private entity such as USP. Legal vulnerability for MedMARx data comes primarily from State laws of "discoverability" or "privilege". Only internal peer-review or quality-improvement processes in hospitals enjoy privilege or protection from legal discovery in many States. In the view of USP, as soon as identifiable information on a case is released outside of the peer review activities of the hospital to any other entity, the information can be discovered through court proceedings (Cousins, 2002). Only anonymous reporting (with respect to the reporter, patient, and institution) fully protects the institution against discovery in court. Rep. Constance Morella (R-MD) introduced a bill (H.R. 4673) on May 7, 2002 to protect the confidentiality of data on medical errors that are based upon the MedMARx system. The Patient Safety Improvement Acts (S. 2590 and H.R. 4889) have broader protections and probably hold more promise for passage.

Total anonymity in MedMARx is achieved through the use of a secret code (similar to the PIN or personal identification number used by banks). A "PIN" number is assigned to the subscribing hospital through a PIN-based email address that does not identify the hospital. All communications are through the PIN-email address. Hospitals can alter their own records in the system (via the Web with the PIN). USP does not know the identities of hospitals, although they can communicate (through the PIN) to ask for clarifying information or corrections to reports.

MedMARx collects detailed information related to medication errors (and collects some data on devices, biologics, and vaccines). Elements include:

- Facility type – the reporter selects general facility characteristics such as "teaching facility" and provides number of beds, average length of stay, and average daily census.

- Drug information – generic and/or brand name of drug (whichever is applicable), including manufacturer, strength, therapeutic class, dosage form, type and size of container, and intended route of administration.
- Time and place of error – date of error, time of error, node in medication process at which error occurred, location where initial error occurred, and location detail for facility use only.
- Narrative description of error in the reporter's own words.
- Classification of error and harm – patient harm and level of care administered to the patient as a result of error, using modified NCCMERP harm/error categories:
    - Category A: "No error – circumstances or events that have capacity to cause error."
    - Category B: "Error occurred, but medication did not reach the patient."
    - Category C: "Error occurred, but caused no harm."
    - Category D: "Error occurred that resulted in the need for increased patient monitoring - no patient harm."
    - Category E: "Error occurred that resulted in need for treatment or intervention – temporary patient harm."
    - Category F: "Error occurred that resulted in initial or prolonged hospitalization – temporary patient harm."
    - Category G: "Error occurred that resulted in permanent patient harm."
    - Category H: "Error occurred that resulted in a near-death event."
    - Category I: "Error occurred that resulted in patient death."
- Cause of error and contributing factors – root cause analysis (narrative); root cause analysis summary.
- Follow-up to event – actions taken to avoid recurrence of an error (through a pick list and narrative).
- Patient data – age, gender and any clinical description in the narrative (at the reporter's discretion); MedMARx collects no other patient-related data.

USP published the first report on MedMARx for data collected in calendar year 1999 (USP, 2000) and the second report for year 2000 data (USP, 2002). Other MedMARx-related publications are available through the same USP Web site. Subscribing hospitals not only access their own data and aggregated data of all subscribing hospitals, but also drill down to protected record-level data of other hospitals. Hospitals can generate spreadsheets and graphs and download data sets for study at the hospital level. Besides subscribers, only USP staff has access to the full database.

Implications for Integration: MedMARx is a strong candidate for integration with a DHHS error reporting system, if certain limitations of MedMARx either are unessential for the Federal regulatory program or can be overcome. Under the current design of MedMARx, the government would not be able to follow-up with institutions or patients for more information, because MedMARx does not identify providers or patients. If such follow-up is essential, then either Federal privacy protections would have to be extended to MedMARx data or HIPAA privacy protections would have to be in effect and revised to fully protect private error reporting databases such as MedMARx from discovery in Federal or State courts; otherwise, hospitals would be reluctant to contribute data.

USP indicates that they have discussed with FDA the potential for sharing MedMARx data with the FDA reporting systems (Cousins, 2002). The Internet-based MedMARx makes it technologically easy to link and integrate with other systems through well-defined electronic transfers. USP also indicates a willingness to function as a contractor for collection of medication errors reports to the government or to establish access to the USP database for Federal staff (Cousins, 2002).

4.4.6 Medication Error Reporting (MER) Program

The MER Program is another Web-based error reporting system, which was established and is maintained by the USP and through which all health care practitioners and students who encounter actual or potential medication errors can report confidentially to USP (USP, undated(b); Cousins, 2002). Reporters can

choose to report either anonymously or to be identified. Because this system is focused on how pharmaceuticals can be improved such as through labeling and packaging, most professionals provide their identity and agree to have it passed on to others for follow-up information.

This system is a precursor of MedMARx and was established to collect information on problems with medication products in hospitals, but reports can be made from any health care setting. It differs from MedMARx in that the MER Program is not limited to subscribers only; allows for Web, mail, phone or facsimile reports; and does not provide the same feedback to reporters. The definitions and data elements are similar to those in MedMARx, including no identities of institutions.

Implications for Integration: USP already shares MER data with the FDA on a weekly basis (Cousins, 2002). USP reviews all MER reports for health hazards and sends all reports to the FDA, the manufacturer, and to the Institute for Safe Medication Practices. FDA does not, however, send reports that go directly to FDA to USP. Data sharing is in one direction in this case and is not a full integration.

4.4.7 University HealthSystem Consortium (UHC) Patient Safety Network (PSN)

The University HealthSystem Consortium (UHC) is a member-owned cooperative of not-for-profit university hospitals specializing in building databases and management solutions for member institutions. The UHC has a membership of about 80 academic medical centers and 100 affiliate hospitals – representing about 80 percent of the teaching hospitals in the United States (UHC, 2000).

To reduce the rate of medical errors, UHC assembled a workgroup of 15 institutional members to design the Patient Safety Network (PSN), an Internet-based, voluntary, point-of-care, medical adverse event reporting system for member institutions (UHC, 2000 and 2002). As of April 2002, the system was tested at one facility and soon to expand to six more. The system allows reports to be made from any computer station in a hospital and captures actual and potential (near-miss) events as well as events that affect patients, staff, and visitors. Many of the data elements of the system are specified as optional, rather than required, reporting. Text narratives are all optional fields. The system provides for detailed follow-up and root-cause analysis by a nurse manager, pharmacy manager, or quality assurance manager, depending on the type of error.

A staff member initiating a report, views a series of yes/no, and drop down menu questions. With each answer, the system presents a tailored set of follow-on questions. The systems allows for elaboration on many types of adverse events including:

- Medication errors,
- Adverse reactions,
- Falls,
- Transfusion events,
- Surgical procedural events,
- Complications,
- Equipment issues,
- Behavioral events,
- Skin integrity, and
- A non-specific “other” category.

The system uses some common classifications (such as the NCCMERP “harm score,” the VA severity assessment score, a pharmacy adverse drug reaction (ADR) classification system, a ADR severity index from the University of Colorado, and a falls reporting system from another institution). While the system allows for anonymous input, the host organization may also customize fields to identify each caregiver involved (to allow for follow-up). The system asks for the specific location in the hospital where the error occurred so that locations of error can be mapped by UHC to specific types of services and departments. Entering a report takes about 15 minutes. The system logs the user off after 15 minutes to protect integrity

of computers left in the rush of an emergency. The system "closes out" reports after 45 days, and they can no longer be accessed.

Each report may be followed-up by one or more managers from nursing, quality assurance, or pharmacy. Each manager-follow-up screen contains questions drilling into the root cause and contributing factors, such as unplanned-workload increase or temporary staff. These screens also provide an opportunity to choose an "assessment of additional costs" that includes factors such as "inconvenience, pain and suffering for patient", "visit to the emergency department", "increased length of stay", and "unplanned surgery." UHC members wanted this screen because they felt that not enough attention was focused on the cost of medical errors (Newcomb, 2002). In the future, this cost-related screen could be tied into other hospital databases such as billing records. On the back-end, the system provides reports that can be customized and that yield comparative data for benchmarking and detecting trends. Reports can be customized for submission to the JCAHO Sentinel Events Database and to State mandatory reporting systems, although standard system-wide reports for these purposes have not been developed.

4.4.7.1 UHC PSN and Privacy Concerns

The UHC PSN collects personally identifiable information (such as provider number and medical record number), while other comparable systems (e.g., the JCAHO Sentinel Events Database or MedMARx) do not. The danger is that this information could become discoverable in a court of law once it is transmitted to the UHC, and this could discourage hospitals from participating. Therefore, the PSN employs policies and electronic security to protect the confidentiality of the data.

UHC and hospitals participating in the PSN sign an agreement in which UHC promises to use the hospital's data only for the purposes specified in the agreement and not to use it for any other purpose. UHC has agreed not to share individual reports with any organization except the contributing organization. If at any time, an organization decides not to continue as a member of the PSN, UHC will return that hospital's data and purge it from the PSN system server. The hospitals have approved the use and sharing of aggregate, non-identifiable data for benchmarking purposes (Newcomb, 2002).

The PSN employs password security that members must use to log onto the UHC Website and to access the PSN. Everyone who logs onto the UHC Website and the PSN to enter or edit a report must go through an authentication process to authorize access to the Website and the PSN (Newcomb, 2002).

The PSN uses a Secure Sockets Layer-secured connection with member institutions so that data are encrypted during transmission and unencrypted for storage in the PSN database. All PSN data reside on a stand-alone server at UHC. The server includes personally identifiable information, unless the transmitting organization decides to mask such information before transfer to the UHC server (Newcomb, 2002).

Each hospital deals with the inevitable legal implications of discoverability differently. Some hospitals have protection from State laws and regulations; others consider the PSN protected as a "peer review quality improvement" activity, which is considered exempt from discoverability in most States (Newcomb, 2002).

4.4.7.2 Implications for Integration

The Patient Safety Network (PSN) is a comprehensive error reporting system that spans all types of errors that occur in hospitals. It is similar to the VA hospital system in that regard. Designed by experts from different fields, it incorporates many recent medical event-reporting developments. UHC set out to incorporate the "best practices" of many well-known systems such as the Eindhoven Error Classification system and other "homegrown" systems from the institutions of the panel that helped UHC create the PSN (Newcomb, 2002). The PSN also is a tool for root cause analysis.

The PSN is a single user-interface, thus, promoting comparability of reporting across institutions involved. It has report writing capabilities (for individual and aggregate reports), thus streamlining the burden of required reporting to multiple entities outside the hospital.

The PSN is a thoughtfully designed, albeit as yet unimplemented, system that should be studied as a base for developing or integrating a hospital-based DHHS system. It could serve the dual purpose of internal quality improvement and external reporting to DHHS reporting systems. UHC might be approached as a test site for integrating a standard DHHS reporting format into the Patient Safety Network of academic medical centers.

4.4.8 ECRI Medical Device Problem Reporting Database and Medical Device Safety Reports

Since 1968, ECRI (a nonprofit health services agency) has investigated reports of medical device failures. Since 1977, ECRI has maintained a voluntary medical device problem-reporting database. ECRI accepts reports from around the world from consumers/patients, providers, administrators, or manufacturers. Reports can be submitted through an online form, telephone, fax, or mail (ECRI, 2002a). Each report relates to an event. Once received, ECRI acknowledges receipt and checks against the historical database to determine whether the report warrants an escalation of the issue (Bruley, 2002). ECRI provides process improvement feedback (based on past reports), launches an investigation, or monitors the situation for further development. If ECRI perceives a reporting trend with a particular device, they will publish a Medical Device Safety Report (ECRI, 2002e and 2002e). ECRI has an Accident and Forensic Investigation department, which meets weekly to discuss all new reports, and "improvements" to an alerts database happen on a continuous basis as the knowledge base grows (Bruley, 2002a). If ECRI deems a reported hazard to be serious enough they will forward notification onto the FDA. The FDA and ECRI have collaborated on hazard reports in the past and used each other's resources to assist with each organization's mission (Bruley, 2002b).

ECRI has collaborated with the Food and Drug Administration (FDA) for many years. ECRI developed and managed the pre-cursor to the MAUDE database. Currently, ECRI is under contract to the FDA to develop training materials for the new MedSun database (Bruley, 2002a).

The Problem Reporting Database has a comprehensive search engine. ECRI assigns a "Cause of Device-Related Incident" to each filed report. According to ECRI, the FDA prefers ECRI search engines when searching MAUDE because they are easier and more useful than other error classifications employed by the FDA. There are five broad "cause" categories with sub-categories that are used to classify and search for reports (ECRI, 2002a):

- Device Factors – design/labeling error; device failure; device interaction; failure of accessory; improper maintenance/testing/repair/or lack or failure of incoming inspection; improper modification; invalid device foundation; manufacturing error; packaging error; random component failure; software deficiency.
- External Factors – electromagnetic or radio-frequency interference; environment/temperature/humidity/light; medical gas/vacuum supplies; power supply/including compressed medical gasses; water supply.
- Support System Failures – error in hospital policy; failure to impound; failure to train and/or credential; improper storage; lack of competent accident investigation; lack or failure of incoming and pre-use inspections; poor incident/recall reporting systems; poor pre-purchase evaluation; use of inappropriate devices.
- Tampering and/or Sabotage.
- User Errors – abuse of device; accidental spill; device misassembly; failure to perform pre-use inspection; failure to read label; improper connection; inappropriate reliance on an automated feature; incorrect clinical use; incorrect control settings; incorrect programming.

ECRI also assigns, when given permission, the clinical specialty and/or service from which the report originated (ECRI, 2002d). Finally, ECRI assigns a mechanism of injury or death, when applicable. ECRI also uses other classifications such as the Universal Device Nomenclature System (UMDNS). UMDNS, developed and maintained by ECRI, is a system to name, label, and communicate information about standard medical devices (Bruley, 2002). It is widely used nationally and internationally as a uniform classification of medical devices (ECRI, 2002a). However, FDA recently decided to support another system as the international standard for device nomenclature.

Compared to the ECRI Device Problem Reporting form, FDA requires more information in their reports. FDA collects personal patient information, information about any corresponding laboratory data, and relevant history, which ECRI does not request. While a reporter could include such information in the narrative section of an ECRI report form, those elements are not required by ECRI (Bruley, 2002), and thus, not captured consistently.

4.4.8.1 Implications for Integration

ECRI appears to be collecting device error reports that also may be submitted separately to the FDA. ECRI does not automatically submit reports to the FDA, however, due to a longstanding collaborative relationship, ECRI will alert the FDA if they deem the hazard to warrant immediate attention. ECRI supplies services to reporters that FDA does not supply – acknowledgement of receipt and process improvement feedback to the reporter based on past reports. If FDA wanted to provide feedback information to reporters, it might pattern the feedback on ECRI's approach or employ ECRI to design and provide that feedback. ECRI also does not collect patient data that FDA requires.

ECRI's approach has several strengths that would make it ideal as a paradigm (or partner) for integration. They have established and maintain two key classification systems for devices – the ECRI "Cause of Device Related Incident" groups and the Universal Medical Device Nomenclature System used by most manufacturers worldwide. They have a staff of medical device experts who read reports and develop Health Device Alerts.

A weakness of ECRI data is the absence of information about the patient using the device or on whom it is used. Another weakness (and reason for excluding patient information) is that ECRI data have not been protected legally from discovery. Because ECRI is private entity, it is not covered by the protections of the Privacy Act of 1974. However, ECRI data might become protected under the HIPAA Privacy Rule, when it goes into effect April 14, 2003, although as noted above this is not yet sufficient to protect ECRI data from discoverability in court.

4.4.9 Other Private Systems

Many hospital systems have developed custom error reporting system or are signing on to subscription services designed to automate risk prevention and management systems in their hospitals. One interesting and accessible example is the Baylor Healthcare System. Baylor has experimented with two Web-based approaches that focus on the breadth of potential problems in the hospital – a "home-grown" approach and a pilot subscription service with DoctorQuality. Baylor has reviewed these two experiences in Baylor University's medical journal (Dixon et al., 2002 and Atherton, 2002, respectively) and found substantial increases in reporting and large reductions in time from event to report (from almost 8 days to 1.6 days, in one approach). These systems have also been credited with program changes that, in at least one instance, have reduced the incidence of patient falls. Users praised the reporting systems for clarity in how to report and ease of reporting. Leadership and safety campaigns appear to make a difference in the level of reporting in the institutions. Both systems also facilitated reports to meet mandatory reporting deadlines such as for JCAHO Sentinel Events (required 45 days from event) and FDA MedWatch reports on medical devices (required 10 days from event).

4.4.9.1 Potential for Integration

Besides enhancing the ability of hospitals to report adverse events efficiently and to study and learn lessons about their safety environments, such systems make long-run integration into national reporting systems more feasible. Any of these systems can be customized to develop reports in standard formats, while maintaining the look and feel of the internal hospital reporting system. Furthermore, the common use of Web-based technology for these systems will make the electronic transfer of data to national systems relatively straightforward, if the national systems are Web-based. Moreover, Web-based systems can be designed to comply with HIPAA security and privacy standards, although Federal statutory protections will be necessary to limit the discoverability of data in these systems. With Federal protections and integration of DHHS reporting systems, AHRQ might subsequently fund pilot tests of linkages to custom hospital reporting systems to foster a full national system. Some special attention also will be required to bring small and rural institutions into a national medical error reporting system.

4.4.10 Australia Council for Safety and Quality in Health Care

In 1999, the Australian Department of Health and Aged Care established the Australian Council for Safety and Quality in Health Care (ACSQHC) to coordinate a national effort to improve patient safety and the quality of healthcare. Establishment of the council took an important step towards creating a comprehensive national patient safety database.

At present, the work of the ACSQHC is in its infancy. The plan is to look at what Australia currently has for databases that capture adverse event data. The council has completed a thorough study of existing local and specialty databases that could provide data and a model for the national prototype. The types of systems studied include coronial data, morbidity and mortality review data, chart review projects. However, these systems cannot meet all needed criteria for a national database. Some are not specifically designed to identify adverse events, not all deaths involving an adverse event are referred for investigation (and thus make it into the database), some of the coding cannot distinguish between adverse events and other conditions, and some of the review processes are resource intensive (such as medical chart review).

One system that shows promise is the Australian Incident Monitoring System (AIMS). Intended to monitor adverse events, it is a national effort and a uniform classification (coding) system was developed for it. The system contains "information on incidents from voluntary reporting by hospital staff" (ACSQH, 2001). The system relies on a combination of coding and narrative reports. A Generic Occurrence Classification (GOC) was developed by the Australian Patient Safety Foundation (APSF) to be used with AIMS. The code was developed using decision tree software and aggregate national data. Unfortunately, the coding and the system proved extremely cumbersome and ultimately too expensive to use (for the moment). APSF is completely re-engineering the system to make it easier to use and hopefully cheaper to implement.

The Australian Council for Safety and Quality in Health Care has set out some preliminary goals to create a national, integrated error reporting system, with standardized and uniform specifications:

- By January 2004, all healthcare facilities will have incident monitoring systems that are capable of contributing consistent data for [healthcare] systems improvement.
- By July 1, 2002, all healthcare services, States, and Territories will have processes in place for the review of patient deaths with a particular focus on, identifying and reviewing patient deaths which may be attributable to an adverse event, promoting appropriate referral of deaths to coroners, and improving national information on causes of death.
- By January, 2004, all health care services, States, and Territories will have processes for action on adverse events which lead to serious patient harm (ACSQHC, 2001)

4.4.10.1 Lessons from Australia

The work of the council may teach us useful lessons:

- The requirement that definitions and classification systems must be applied uniformly and nationally;
- The realization that while smaller, local efforts may be useful and successful in their own right, they inevitably are too unique to attempt to integrate; they serve better as models and paradigms for a national system;
- Designing a national system requires the participation of all stakeholders (public, private, across healthcare professions);
- There should be a dedicated, national body, to guide development.

Further study of the Australian patient safety activities is appropriate to determine which hold relevant lessons for the U.S.

4.4.11 United Kingdom – National Health Service, National Patient Safety Agency

In mid-2000, the National Health Service (NHS) launched an initiative to create an integrated, national medical errors and adverse event reporting system. The first published report from the initiative, "An Organization with a Memory," and related early presentations (DOH/UK, 2001a and 2001b) create a vision for the new system. The new system aims to:

- Develop new reporting systems to foster increased reporting.
- Protect staff who report errors and near misses, by continuing whistleblowing" laws.
- Work with stakeholders to increase the usefulness of data for monitoring and improving the outcomes of care.
- Guide the NHS on investigations and inquiries.

To achieve these goals, the National Health Service created the National Patient Safety Agency (NPSA) to support education and learning from errors, not to regulate the practice of medicine. The NPSA has identified a general scheme for responding to adverse and near-miss health care events and is establishing a central repository of such data.

NPSA's national approach for responding to adverse and near-miss events is to (DOH/UK, 2001b):

- Define adverse events and near misses;
- Ask providers to:
    - Gather information on adverse events and near misses;
    - Apply root cause analysis (RCA) to facilitate learning and minimize risk (using any published RCA method);
    - Analyze patterns and trends;
    - Report standard information on specified events and near misses to NPSA;
- Develop a central repository for standard data on adverse and near-miss health care events;
- Analyze and disseminate lessons learned from the NPSA repository; and
- Implement effective change.

The NPSA will mandate reporting to the central repository by the entire NHS (whether public or private providers of care) and will encourage voluntary reporting by the general public and other interested parties. To maintain the repository, NPSA will (DOH/UK, 2001b):

- Set reporting standards;
- Collect, code, and classify information;
- Maintain a publicly available central repository;

- Exclude identities of patient and health care professionals in the repository, but maintain identities of institutions; (Note: In the UK, the hospital or "trust" law precludes court access to an entire hospital database. Discoverability applies to individual cases with court order.)
- Provide trends and aggregate data on the NPSA Web site (early results expected April 2002)
- Analyze the data for patterns and trends
- Provide feedback to organizations and individuals
- Produce solutions to reduce risk
- Specify national goals and targets
- Promote research
- Promote a reporting culture
- Collaborate with relevant national and international bodies

NPSA will allow local NHS provider organizations (NHS Trusts) to choose their own software programs for reporting. However, each organization must have the capability to report a minimum data set of about 18 elements to the NPSA. The main elements are (DOH/UK, 2001b):

- Description of the event – severity, people involved, equipment involved
- Location of the event – medical specialty
- Date/time of the event
- Cause of the event – immediate or proximate
- Root/underlying cause of the event
- Action or proposed action taken to fix the cause and root cause
- Impact of the event – on the patient, on the organization
- Analysis of possible mitigating factors
- Patient characteristics – age, gender, ethnicity (Osborn, 2002).

A survey of current reporting forms will be undertaken to determine whether existing forms can be modified to collect the above data related to patient safety. The publicly available materials describing the NPSA system do not indicate how much of the system will be based on narratives and how much will be pre-specified categories of information.

To implement the system, NPSA has identified working definitions of adverse events and near misses (DOH/UK, 2001b). These are based on international collaboration:

- "Adverse Healthcare Event – an event or omission arising during clinical care and causing physical or psychological injury to the patient.
- Health Care Near Miss – a situation in which an event or omission, or a sequence of events or omissions, arising during clinical care fails to develop further, whether or not as a result of compensating action, thus preventing injury to a patient."
- To prove the viability of the initiative, the NPSA has set the following end-result goals (DOH/UK, 2001b):
    - "By the end of 2001, reduce to zero the number of patients dying or being paralyzed by mal-administered spinal injections.
    - By 2005, reduce by 25 percent the incidence of harm in obstetrics & gynecology, which result in litigation.
    - By 2005, reduce by 40 percent the number of serious errors in the use of prescribed drugs.
    - By 2002, reduce to zero the number of suicides by mental health patients from non-collapsible bed or shower curtain rails on wards."

Implementation goals for the NPSA are (DOH/UK, 2001b):

- "By December 2001, 60 percent of NHS Trusts will be in a position to provide information to the national system and all NHS Trusts will be working towards this goal.

- By December 2002, all NHS Trusts and a significant proportion of primary care will be providing information to the national system.
- By December 2002, levels of reporting in the NHS will have doubled."

As of February 7, 2002, the NPSA had 28 pilot sites reporting data for about 10 weeks to the NPSA central repository. In that time, about 3,000 adverse events or near misses were reported. NPSA expects to have about 140,000 incidents reported by the end of a year of reporting, March 2003 (Osborn, 2002).

Under an existing State insurance system that requires reports of catastrophic medical events, providers are required to report within 48 hours and perform a root cause analysis within 45 days. However, those data do not have standard definitions, nor do they have a common clinical language for reporting, and they are nearly impossible to interpret. (Osborn, 2002.)

4.4.11.1 Lessons from the UK

NPSA is in the enviable position of having a mandate to implement a national reporting system that applies to all health care providers in the United Kingdom (U.K.). As a result, they are in a position to realize a fully integrated error reporting system in a relatively short period of time. However, they are only beginning their initiative, so that lessons cannot yet be based on a history of experience.

It will be important to monitor the progress, successes, and failures of the NPSA. Some interesting questions will be:

- How successful will the NPSA be in gathering data, given the independence of local providers to use their own software and methods? This is similar to the U.S. situation.
- What opportunity will the NPSA lose (if any) given the apparent plan to use existing reporting forms rather than electronic reporting?
- Will the NPSA require providers to report according to some standard classifications of error, harm, clinical conditions, and other data elements? If so, what are those? If not, how difficult will it be to interpret narrative reports?

It is notable that the NPSA expects the incidence of error and near-miss reports to increase and specifically states that as a goal of their system. The result of their pilot program of 28 hospitals reporting for 10 weeks was 3,000 incidents.

The initiative of National Health Service in implementing a national patient safety reporting system is a development that will provide valuable lessons on patient safety in the future.

4.4.12 ISMP Canada – "Analyze-Err" Software

Analyze-Err is a national, voluntary medication error reporting and root cause analysis (RCA) system that allows institutions in Canada to report, record, and analyze *medication* errors (ISMP Canada, 2002a). ISMP Canada is a private, not government, organization. While ISMP Canada performs aggregate analysis on national data, each participating institution has the ability to perform data queries and root cause analysis on their own local database of reported errors. ISMP Canada developed the software in conjunction with ISMP in the U.S. and launched the package in late 2001.

The report form combines both standardized drop-down menus and narrative responses in order to capture all relevant data on the error (ISMP Canada, 2002b). With permission, Analyze-Err employs the NCCMERP error outcome classification system. The software package queries, analyzes, and graphs data for root cause analysis and for charting trends.

The software supports anonymous reporting and disassociates personally identifiable information from a report before entering it into its aggregate database (ISMP Canada, 2002a). However, the report is entered with identifying information about the patient and the reporter, in case of need for further contact or clarification. The identifiable information collected in the report includes patient name, patient number (if

applicable), patient diagnosis, service and nursing station where error occurred, and an explanation of corrective measures taken (if any). The report has space for narrative expansion of any of the identifiable information given.

Analyze-Err allows almost instantaneous analysis of the reported error against that organization's internal database. Analyze-Err offers another illustration of a database design for medication errors.

5 Options and Alternatives

In this section, we describe the proposed options and alternatives for the integrated reporting system. Our discussion begins with descriptions of high-level and specific design options and continues with an enumeration of "solution criteria." The final section includes an implementation recommendation for consideration by AHRQ and the PSTF.

5.1 High-level Alternatives

During the course of our data collection, it became apparent that all systems could be usefully partitioned into two distinct but related components: the "front end" and the "back end." Front end components of the system include the data entry components and user interface, whereas back end components include the underlying database and the collected data. While far from modular, front end components from some systems could be merged to produce a common or integrated front end. Likewise, a data warehouse could be created using information collected from somewhat diverse data systems.

Although simplistic, the possible solutions resolve themselves into no more than six, and likely three, high-level candidates. These options are the combined result of answers to the following three questions:

- Should the "front end" (data entry) components should be integrated?
- Should the "back end" (data storage and analysis) components should be integrated?
- Should of the complete data systems be integrated?

Given the diverse nature of the data systems and their broad reach, it seems unlikely that they could be efficiently integrated in a timely manner. For example, the existing Medicare and Medicaid infrastructure are well established and so broadly used that developing vastly different implementations (e.g., web-based data collection) would probably be overly burdensome for all parties, and may not lead to any significant improvement in the nature or quantity of reported medical events. Thus, we feel that integrating all data systems is an impractical option, at least in the short- and medium-term. Accordingly, the high-level design categories can be described in a 2 x 2 matrix, illustrated below.

I. No front end integration, no back end integration	II. Front end integration, no back end integration
III. No front end integration, back end integration	IV. Integration of both the front end and back end

Category I essentially describes the *status quo*, and as such does not represent a viable integration plan. The relative merits of each remaining option are discussed below.

5.1.1 Category II - Front end integration

Integrating the "front end" (e.g., user interface and data collection components) has several appealing qualities, including reducing reporting burden, standardizing data elements, and increasing reporting.

A prototypical front end integration would consist of a common web interface which routes collected information to various data systems. Reporting burden can be reduced when extent data systems collect duplicate information. Similarly, use of standard nomenclatures and formats is likely to reduce the reporting burden, as it would allow users to utilize common vocabularies when reporting various events. For example, standardizing nomenclatures would allow hospital staff to use similar terminology/vocabularies when reporting either a catheter failure or a nosocomial infection.

Patient Safety experts contend that one of the reasons medical events are under-reported is because of reporting time and complexity. Removing these barriers should increase reporting and allow policy

makers and researchers a better understanding of the nature and scope of patient safety issues across various settings.

The downside to front end integration is that it does guarantee an increase in either data analysis or linkage of events across multiple settings. Collected data could be routed to existing "stovepipe" systems and the resulting databases might look and function much as they do now.

5.1.2 Category III - Back end integration

Whereas "front end" integration is aimed at reducing the effort associated with getting data in, integrating the databases and analysis systems leverages the existing data. Such an effort might entail use of various algorithms to link information from disparate data systems. These links could provide a context for existing data (e.g., creation of rates using CDC or FDA data as a numerator and CMS or AHRQ data as the denominator) and also create "error episodes" that cut across settings and time. Such episodes might be used to analyze events that manifest themselves in one setting (e.g., outpatient visits) but can be traced to events that occur in other settings (e.g., inpatient procedures).

Strengths of the back end integration approach are minimal (if any) disruption to existing data entry mechanisms, and minimal impact to existing system performance and functionality since relatively complex analyses can be performed off-line. Moreover, system development along for this option could proceed incrementally, beginning with integration of a few databases and adding information from other databases as it becomes necessary and practical.

The chief drawbacks of this approach are:

- it does little to reduce the burden of reporting,
- analyses are likely to be temporally removed from the actual events, especially if several different databases are used for analysis, and
- common tools for online analysis are not available until the later implementation phases.

For example, it is fairly trivial (in terms of computational and processing power) to create numerators using data from CDC and denominators using data from AHRQ or Medicare. The challenge is time, waiting for appropriate denominator data to wend its way through various intermediaries and processing steps. While it may be possible to estimate denominator data, rates associated with adverse events may not be available for months or years after an event occurs.

Another potential drawback of this approach is that it would co-mingle data from various sources, which may violate existing agency agreements and regulations. Certain data efforts are supervised by Institutional Review Boards and are subject to various restrictions (e.g., use of data for purposes other than those for which the data were originally collected). In order to make full use of the data, it may also be necessary for the various agencies to sign data sharing agreements that would govern the use of these shared data.

5.1.3 Category IV - Integration of both front- and back-end

Category IV, the "complete" approach, would develop a common user interface for event reporting systems, implement a common data warehouse to store the collected data, and include a common set of tools for data analysis. This option is the sum of the two approaches discussed this far, and as such inherits the advantages and disadvantages of each approach. This option represents the most complex and potentially the most productive solution. Some specific components (e.g., data elements on specific forms, coding schemes and nomenclatures) could be re-designed to be more compatible offering a valuable opportunity to harmonize aspects of various systems, and enabling future integration efforts. Such an integrated system should ultimately include as many standalone systems as is practical, and the effort required to integrate these databases in a single step would likely extend beyond the short-term and perhaps so long that other options are more appealing.

5.2 Solution Criteria

Determining a solution requires the development of a solution criteria set. Members of the project team discussed potential solution criteria based on their knowledge of existing systems, user needs, project goals, the patient safety "landscape," and discussions with key personnel from various organizations. The result is a synthesis of these perspectives into solution criteria relevant to the current project. The criteria were further divided into two groups: required and optional solution criteria. Required solution criteria represent the subset of solution criteria that any candidate system must meet, whereas optional solution criteria represent characteristics of certain alternatives but are not necessary components of every solution. For example, all viable solutions must protect patient and provider privacy, and a solution may be considered viable even if does not collect information relating to inpatient medication errors..

Required Solution Criteria

- Facilitate a reduction in the risk of harm to patients.
- Make data collection simpler and more similar across systems.
- Return valuable information to the data source (e.g., provider).
- Allow incremental development so DHHS can address significant issues first and subsequently incorporate other systems and issues.
- Protect an individual's privacy. This applies to patients, providers, and persons who submit information.
- Accommodate the current systems of the PSTF agencies.
- Facilitate data sharing among the PSTF agencies.
- Incorporate a recommendation on a standard event-reporting format(s). This should include specification of classification systems, reporting forms, narrative versus codified entry, and related issues.
- Develop a plan for building a secure data collection, storage, and reporting system.
- Incorporate a mechanism for collecting and analyzing information associated with "root causes" of adverse events.

Facilitate a reduction in the risk of harm to patients. One of the most important functions of an integrated reporting system is to reduce the risk of harm to patients. Although somewhat obvious, it is important to bear this in mind as various alternatives are considered, since some options may integrate systems in such a way that the result does not influence patient care.

Make data collection simpler and more similar across systems. Although each existing system has a designated purpose, some systems may have similar functions that could be standardized (e.g., different login methods for various systems). Where appropriate, a solution should be parsimonious and streamline the data collection task while still preserving the essential information.

Return valuable information to the data source (e.g., provider). Several existing systems provide direct and immediate feedback to information submitters about medical events relevant to their submission. These individuals are in the best position to communicate this information and effect change. The recommended solution must also allow for aggregate information to be made available to intra- and extra-mural researchers for off-line analysis.

Allow incremental development. Given the changing nature of patient safety systems and research incremental development results in a system that is more flexible and adaptable given the number of development evolutions. With an incremental approach system designers can respond to changing standards and requirements by revising the design on a periodic basis.

Protect an individual's privacy. An essential characteristic of any system is the protection of personally identifiable information, whether it relates to a patient, provider, or someone who submits information. Protecting privacy can be accomplished either by (a) deleting or encrypting any identifiable information

or (b) obligating those who work with sensitive data to use such information only for designated purposes.

Accommodate the current systems of the PSTF agencies. Taken together, the PSTF agencies maintain a host of data systems that fulfill specific operational needs. Although some of these systems may merge in the future, we are developing a plan based on the existing systems rather than starting from scratch with an entirely new system that would likely take years to design and build. While this process is underway all of the PSTF agencies must maintain the mandated collection and reporting requirements.

Facilitate data sharing among the PSTF agencies. While we anticipate that data will continue to be submitted to distinct entities for specific needs, we also view the creation of an integrated system as an opportunity for agencies to share and combine data. Although the agencies have shared data and cooperated on several projects, many of these efforts have been "one-off" endeavors and not reproduceable. Implementation of an integrated event reporting system should reduce the effort required for staff from various agencies to cooperate on *ad hoc* and other analyses.

Incorporate a recommendation on standard event-reporting formats. Most patient safety systems are still in their infancy and are being developed to meet the needs of specific facilities, States, or agencies. It is important to establish common ground among these systems, and one such mechanism would be a standard event reporting format. Much as the UB 82 (and subsequently UB 92) facilitated efforts to analyze administrative health care data, development of a common reporting format would enable various entities to share information and would expedite development of patient safety systems.

Develop a plan for building a secure data collection, storage, and reporting system. Although related to privacy, security is a separate criterion in today's electronic age. While it is important to maintain the privacy of identifiable data, it is also important to maintain the integrity of the data repository and prevent unauthorized access to components of the site. Security can be accomplished through technologies such as firewalls, virtual private networks, and other security monitoring software applications.

Incorporate a mechanism for collecting and analyzing information associated with "root causes" of adverse events. Piecing together *why* events occurred is critical for formulating procedures so that the likelihood of future adverse events can be reduced. One of the more widely used methods for accomplishing this is through collection and analysis of the "root cause" of a given event. Since root causes transcend domains (e.g., drugs) and settings (e.g., inpatient), lessons learned from one facility can be utilized by other users. For example, a facility may note an increase in adverse events, conduct an internal analysis, and find that the increase can be attributed to insufficient monitoring of patient status or process of care (as opposed to, say, manufacturing defects). Other facilities may observe a similar trend and look at monitoring as a possible cause early on in their evaluation process.

Optional Solution Criteria

- Develop requirements for a system that includes information on inpatient medication errors.
- Increase the value of the individual pieces of information by linking them with other types of information.
- Includes a mechanism through which data standards, classifications, technical standards, and best practices can be shared.
- Make data from the PSTF agencies more accessible outside of the agencies.
- Leverage State reporting systems as a data source.
- Provide optional (user-defined) fields for custom event types.

Develop requirements for a system that includes information on inpatient medication errors. This criterion follows the practice of "picking low-hanging fruit" first, and addresses an important dimension of patient safety for which data could readily be obtained. Although there are certainly other important domains, numerator and denominator data in this area are routinely captured as part of the day-to-day functioning of many hospitals.

Increase the value of the individual pieces of information by linking them with other types of information. Although this is might seem to be a required solution criteria, we were able to conceive of potentially viable options that integrated similar data systems without incorporating other data systems (e.g., one that routes various existing data to respective systems).

Include a mechanism through which data standards, classifications, technical standards, and best practices can be shared. While noble and worthwhile, this criterion is not essential to the initial success of all possible options. We expect that any proposed approach will naturally develop a user community that shares information either formally or informally. At some point, this coordination activity may take center stage though efforts of the PSTF or by forming an independent entity.

Make data from the PSTF agencies more accessible outside of the agencies. This criterion was suggested with the aim of facilitating extramural research, and making such data available would likely further patient safety research efforts. However, the privacy and confidentiality implications of such disclosure may make it impractical.

Leverage State reporting systems as data sources. State systems represent a potential source of information and could be used to augment data reported through various Federal channels. Although attractive, there are relatively few State-based systems and those that do exist (or are being built) are designed to meet State-specific requirements and mandates that may vary over time.

Provide optional (user-defined) fields for custom event types. This criterion would enable users to submit user-specific information, possibly including other types of events and potentially sensitive information. This capability might make users more willing to enter information especially if it was easily available in their own organization as well. We feel it is more efficient to focus on the early development of key data elements, and add optional information as the system matures.

5.3 Description of Options

Based on these solution criteria, we developed approximately a dozen different design options/alternatives and compared these to a) each other, and b) the solution criteria. Not surprisingly, many of the alternatives were structurally similar, varying only in terms of user population (e.g., hospitals only) or data systems to be integrated (e.g., FDA only, CMS only) and the sequential order of integration.

After discussing each option and eliminating relatively similar candidates, the remaining options were more fully elaborated. Section 5.4 describes the two options that we feel best meet the PSTF's goals and the solution criteria outlined above.

Although each option consists of distinct activities and phases, each option requires design, implementation, and evaluation components. The design component includes not only the design of specific software and hardware modules, but also includes development of data dictionaries and standards for collecting, storing, and analyzing data.

Implementation of a given option entails the database construction and development of other technical features. This could include rollout of a web server, distribution of digital certificates, and other activities directly associated with the development of integrated data system.

Finally, it is important to develop a method for evaluating the effectiveness of a given implementation. This can include (but is not limited to) measurements of reporting burden, number of events reported, and number of analyses performed.

5.4 Option 1 – Integrating Hospital-Based CDC and FDA Event Reporting

Option 1 addresses integration in phased approach, and begins by developing a common user interface for those systems that collect adverse event information from facilities. Specifically, this approach calls for development of a common user interface for three FDA systems:

- Adverse Events Reporting System (AERS),
- Biological Product Deviation (BPD),
- Manufacturer and User Device Experience (MAUDE),

and one CDC system:

- National Healthcare Safety Network (NHSN).

Additionally, the approach recommends an adverse event data warehouse prototype, built initially from the retrospective data stores of the four named systems and transitioning to live data feeds from the common front-end as it becomes operational.

In addition to the development activity associated with data collection components of Phase 1, we foresee the following activities occurring in Phase 1:

- Formation of a "user group" consisting of staff from AHRQ, CMS, CDC, FDA, and representative facilities that will submit data to the common front end.
- Design and implementation of preliminary reports and analyses run against the prototype data warehouse
- Interviews and meetings with potential users to determine unmet needs and potential system uses
- Analysis of data gaps and recommendations for changes to data collection forms and format.

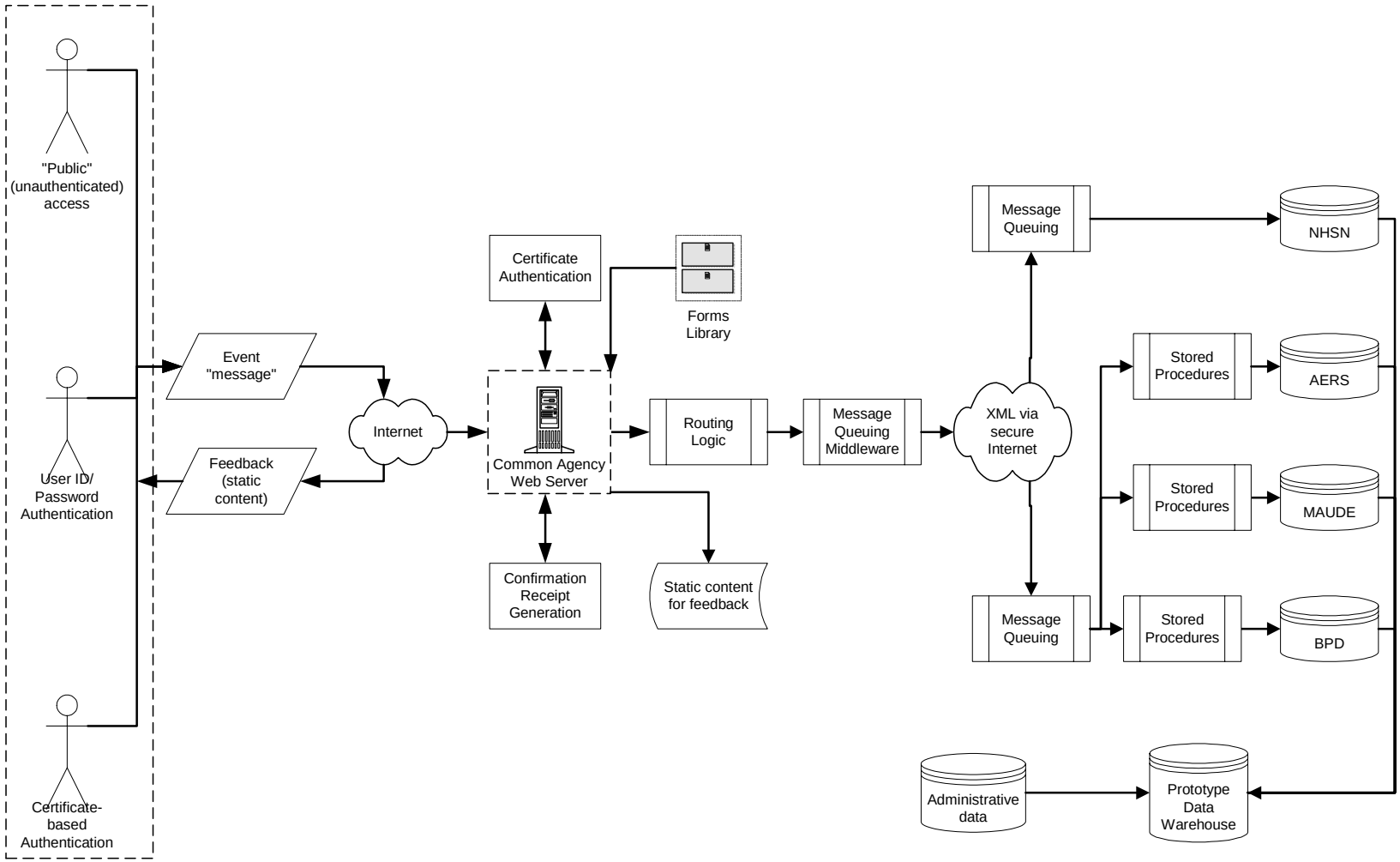
5.4.1 Development of the Integrated System

Integrating the data collection component of these systems would provide facilities with a web-accessible common user interface that allows for standardization of data elements common to each system. As part of Phase 1, a front end would be developed that collects information using a consistent look and feel, and routes information to existing data stores at the respective agencies. Initially, this approach is minimally disruptive to existing systems, while allowing for future expansion and integration.

Figure 6 is a high-level diagram of proposed integration Option 1. At its center is a "Common Agency Web Server", which will serve as the single point of contact for all hospital-based event reports to the CDC and the FDA. This point of contact will consist of a web site on the public Internet accessed by pointing a browser to a single distinct URL, although in fact the site may consist of one or more new and/or existing web server computers or processors. The new web site will prompt for and receive all of the variations of event reports that are currently being collected as part of the four systems.

In Phase 1, the common agency web server will serve only as a mechanism for eliciting event reports from users and forwarding the information to the appropriate agency systems. The permanent persistent storage of reports and the subsequent analysis and reporting will continue to take place at the systems maintained by the agencies for this purpose.

Figure 6: Overview of Option 1, Phase 1



The main functions of the common agency web server will be to:

- Authenticate users, when appropriate
- Determine the information to collect from users, present forms for this purpose and validate information in the event reports to the greatest extent possible
- Acknowledge receipt of information from users with a unique confirmation number that identifies the interaction that occurred
- Allow users to amend, retract or otherwise update reports after establishing their right to do so
- Reliably transfer the event reports and the updates to the appropriate system(s) at the FDA and CDC sites.

Note that the MedSun system (currently being implemented) is not included in the initial set of candidates for integration. As the role of MedSun and MAUDE evolve with respect to reporting of medical device-related adverse events, Option 1 would flexibly support any required incorporation or transitioning of systems and data or would support any required changes.

5.4.2 Data Warehousing Prototype

Although the initial goal of Option 1 is the development of a common front-end web site for four FDA and CDC systems, the long-term goal of the effort is true end-to-end integration of these and other systems. Ultimately, the disparate data models these systems utilize will need to reconciled into a single homogenous model that will support integrated reporting.

Rather than wait until the common front-end has been built and is operational, issues involved with data integration must be confronted as quickly as possible, so that any changes in data collection required to support integrated reporting can be discovered as early as possible and incorporated into the developing system. Building a prototype data warehouse from the existing databases behind NHSN, AERS, MAUDE and BPD can best accomplish this.

The purpose of this prototype, unlike a classic data warehouse will not be to maintain a current, up-to-date, real-time data query facility, but rather to investigate issues of data quality, data completeness, assess data linkage capabilities, homogeneity and conceptual compatibility. As such, the prototype will not have to deal with some of the standard data warehouse issues of timing and periodic update. We envision a process whereby a static “snapshot” of each database is taken encompassing approximately one year of the most recently collected data.

The four snapshots will be moved onto a single analytic platform, combined and analyzed. Based upon current estimates of data volume for the four systems involved, this platform need not be more elaborate than a workgroup or department server with 100 to 200 GB of disk storage. There are a number of commercially available software tools that could be used to facilitate the process, including ETL (“Extract, Transform, and Load”) and statistical packages that incorporate data manipulation tools.

Previous attempts to merge and analyze data obtained from different error reporting systems have met with limited success, due largely to conceptual incompatibilities of the underlying data. Similar problems may well confound the prototype proposed here. For this reason, it is important to identify these factors as early as possible and move quickly to rectify them at the point of data collection.

5.4.3 Authenticating Users

The existing FDA systems and the NHSN currently collect event reports under a variety of user authentication and identification scenarios. Some event reports to the FDA systems can be made anonymously, others are made by identified reporters. Event reports submitted to the NHSN system will be submitted by identified, registered reporters only, and with a computer certificate-based system used to

positively establish the reporter's identity and authenticity. We anticipate that the common agency web server will accommodate each of these types of event reporting.

Anonymous reports are the easiest to accommodate, as they require no additional facilities at the web server. User ID/password authentication can be performed by a number of well-known means, as this is a common method of establishing identification. Typically, this method of identification is performed with a User ID/password table in a relational database attached locally to the web server but isolated from the public Internet. Communication with the client browser is performed over the HTTPS protocol that utilizes encrypted communications to preserve the privacy of the User ID/password combination.

The NHSN system plans to use a certificate-based system to establish the identity of the reporting facility. This is the most secure of the methods employed but it comes at the cost of added complexity. There is a significant level of effort associated with obtaining and installing the software certificates on the client computers, especially as the user base expands. The NHSN system will use a software component to validate the identity of candidate reporters by verifying the existence and authenticity of the certificate on the client computer.

For both User ID/password combinations and certificate-based authentication, there are two approaches that can be used. One approach, *Certificate Authentication* is to move the databases, algorithms and vendor-provided software components to the common agency web server and perform authentication there (Figure 6). The second approach is to perform authentication at the agency web sites. Under this scenario the common front-end web site forwards the credentials presented to the relevant agency sites that in turn reply with a positive or negative acknowledgment.

5.4.4 Soliciting Information

The primary purpose of the common web server will be to elicit data on adverse events reported by facilities and are currently collected by the CDC and the FDA. The most visible aspect of this purpose from the point of view of users in hospitals will be the user interface, or set of data collection forms, that is presented to hospital staff via their web browsers.

The common web server will maintain a "Forms Library", as shown in Figure 6 attached to the web server. This library will contain all of the *static* HTML forms needed to collect information now collected as part of NHSN, BPD, MAUDE and AERS. The qualifier "static" in the previous sentence acknowledges that some of the information collected (via NHSN) will be determined by database entries that effectively customize a facility's set of forms. A different mechanism will be used to accommodate this functionality; a static forms library is inadequate.

5.4.5 User Interface Characteristics

It is a crucial, defining principle of the system that the set of information gathering forms be as simple, efficient and easy to use as possible from the end user's point of view. To this end, the design effort will look at the total collection of forms used by the four agencies and strive to remove redundancy from the collection, to streamline the process used to enter information and to introduce as much consistency as possible across the various pieces. Possible approaches to this objective include:

- Appropriate sequencing and ordering of information requests
- Organizing of information requests
- Replacing or supplementing free text entry with multiple-choice entry
- Use of appropriate default values
- Remembering, and offering to use previously entered values
- Using information already entered to constrain the choices that can be made
- Using consistent navigation mechanisms
- Using color and fonts in a consistent manner to convey information

Appropriate sequencing and ordering of the data entry form fields and controls is a critical element of usability. Fields need to be grouped in a manner consistent with the user's task so that users can move through them sequentially and contiguously in the order that they would naturally use as they move through the sources of information and thought processes relevant to the data entry task. For example, when information about a biologic product is entered, all of the associated information should be grouped together and be in the order that it might appear on a label or other identifying document. Logon and establishment of identity (for other than anonymous reporting) should always occur at the beginning of the sequence, and the user's identity can be used to determine the actions they are allowed to perform.

Organizing information requests involves looking for common data elements across the various data entry forms and putting the relevant fields in one and only one place. For example, two or more of the agency systems might request information on a location and this request might be at the beginning of one form and at the end of another. Factoring aids users by giving them a sense of familiarity with the data entry process, regardless of which type of event they are reporting.

Where appropriate, free text data entry fields should be replaced with multiple choice fields, as it is easier for users to make a choice than to type in a description. In some cases this option is not possible, such as when a narrative is required or when no appropriate taxonomy exists. In many cases, information previously entered can be used to constrain the subsequent choices a user can make. Effective user interface design results in form logic that guides the user away from entering inconsistent, incomplete or incorrect data. For example, rather than parsing form fields after the "Submit" button is clicked and generating error messages, the form logic can constrain choices and provide feedback during data entry. Some fields end up taking on identical values time after time, and these can either be set as the default for a particular user or institution, or the system can keep track of the last value(s) entered and offer to insert them.

Font styles, sizes and colors can be chosen to provide consistent information to users across all the systems. Text rendered in the color red, for example, can be restricted to feedback that points out inconsistencies or incomplete data. The labels on required fields can utilize one font style, while optional fields another, and this approach can be standardized across all four systems.

All of the methods described above are aimed at minimizing the burden of reporting for users. The burden is minimized by reducing the number of keystrokes and mouse clicks a user must make, and by reducing the shuffling and reorganizing of information, both cognitive and physical, that the user must perform to accomplish the reporting task.

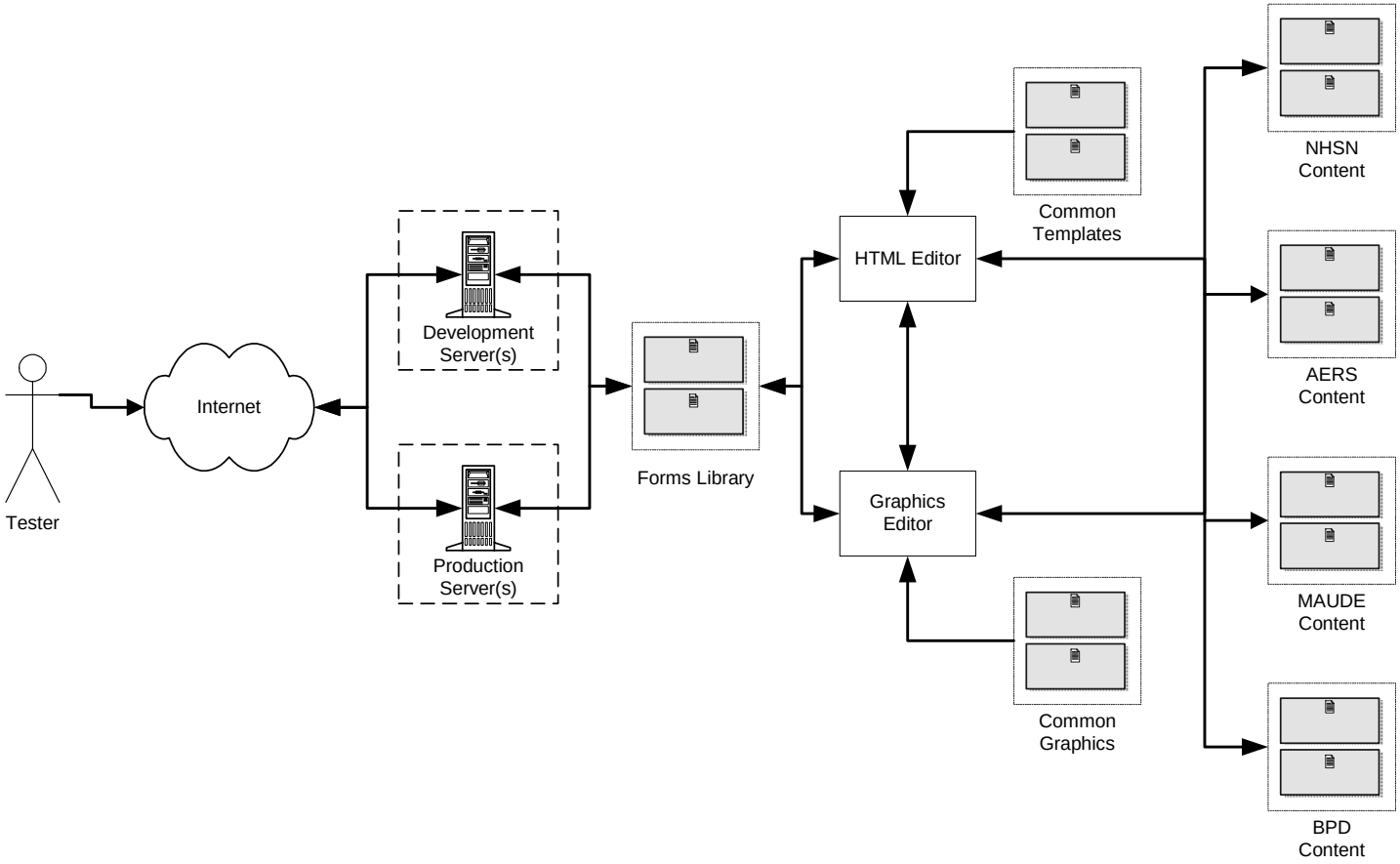
5.4.6 Confirming Report Receipt

Once the report has been received, the system will confirm its receipt. A unique confirmation number will be generated and transmitted back to the user. Confirmation numbers are often relatively short alphanumeric sequences (radix-36, case-insensitive letter-digit combinations). These confirmation number will serve as the user's receipt. The receipt can be used to track the report if necessary, and to identify the report should the user wish to amend, retract or otherwise update it.

5.4.7 Creation of the Forms Library

Figure 7 depicts information combined from a number of physical locations, including the CDC, the FDA and the site where the common agency web server will be deployed. Phase 1 of Option 1 will seek to develop a common front-end, with a consistent look and feel, to the data gathering elements of what are now four disparate web sites. Option 1 will create an environment that can be used to meld visible elements of the four sites into a single coherent site.

Figure 7: Forms Library Creation



5.4.7.1 Common Templates

The key to building a forms library with a common look and feel begins with a collection of common HTML templates containing elements such as:

- Headings, hyperlinks and logos used on every page
- Common high-level navigation bar that run downs the side or across the top
- Common footer that includes things like links to help, frequently asked questions, and a way to contact site personnel
- HTML table definitions used to divide web pages horizontally and/or vertically and to control how elements wrap or truncate as the page is expanded or narrowed in the user's browser
- Frames and borders, and their respective colors and widths
- Other common elements

Other templates might contain one or more common, pre-populated controls, such as:

- Drop-downs for identifying physical locations, such as States
- Drop-downs, list boxes or JavaScript-based hierarchical indexes for displaying common taxonomies
- Text boxes with scroll bars for free-text data entry
- Collections of patient-description information, such as ID, age, DOB, sex, weight, etc., formatted together in a standard way
- Combinations of descriptive text and labeled check boxes laid out in a standard fashion
- Mouse-over effects such as highlighting, descriptions, help text and tips
- Date capture boxes that qualify dates and optionally display calendar controls

5.4.7.2 Graphical elements

When used in conjunction with a common template library, a graphics library provides a coherent look and feel to the entire site. Whereas as a common template library provides a repository of HTML that can be shared and reused across the four sites, a graphics library can serve the same purpose for graphical elements used in the site, helping to provide a common coherent look and feel to the entire site. Graphical elements might include:

- FDA and CDC agency logos
- Program logos such as "MedWatch"
- Backgrounds
- Pictures
- Maps
- Gradients
- Curved or shaped boundaries and filled areas
- Distinctive buttons
- Text formatted as graphics to preserve a particular font and/or layout

Although HTML can be used to define much of the text on a web page, not every browser can render the same set of font styles and sizes. When it is necessary to place text on a page in a specific font style, size and layout, a common practice is to create the textual element with a graphics editor and convert it to GIF (Graphics Interchange Format) or another graphics format and place it on the web page as a picture. This technique is particularly useful when the font size, style and layout convey a sense of familiarity or authenticity to the reader, such as an agency name and address, an OMB form approval header or a US DHHS representation or certification.

5.4.7.3 HTML and Graphics Editors

Site developers will find it useful to use editing tools designed specifically for HTML editing and graphical editing to create the site. There are a number of commercial off-the-shelf (COTS) HTML editors available, ranging from very simple and inexpensive tools like Macromedia's Homesite to special purpose integrated tools like Cold Fusion and Macromedia Dreamweaver through general purpose development environments like Microsoft's Visual Studio incorporating ASP.NET. Similarly a number of COTS graphical editing tools can be utilized. Examples in this category include Adobe Photoshop, Macromedia Flash, and Macromedia Fireworks.

5.4.8 Routing Information

Phase 1 of Option 1 does not replace the four CDC and FDA agency systems. Rather, it would serve as a front end to these systems, replacing the visible aspects of the data collection processes. In some cases, such as with the NHSN system, deciding where to draw the line between functions that are clearly front-end, and those that are clearly back-end may prove difficult. Some functionality, such as rights administration and data import, falls into the gray area between. In other cases, such as the FDA's voluntary reporting under MedWatch, the distinction is straightforward, as users connect to the site anonymously, provide event description information that is input into the system, and terminate their interaction with the site.

In an ideal world, Phase 1 would simply elicit a predetermined collection of information from users and forward it to the appropriate targets, but unfortunately this is not completely possible. Determining the user's identity, what groups the user belongs to, what the user wants to do, and what information the user provides all serve to shape the interaction with the system. This information in turn determines which pages the user views, which fields they see and which options they are given.

Based upon the type of information the user is reporting, the common front-end will route the adverse event description information to the appropriate back-end web site(s). In the situation where the information might be appropriately reported to more than one site, the system can either automatically route the information to multiple sites, or give the user the option to forward the information to multiple sites.

Depending on the complexity of the interaction, however, additional types of information might need to be routed between the agency sites and the common front-end. The additional types of information that will potentially move between the front-end and back-end servers will be discussed later in the Section 5.4.11 Variations and Configuration Options.

5.4.9 Message Queuing Middleware

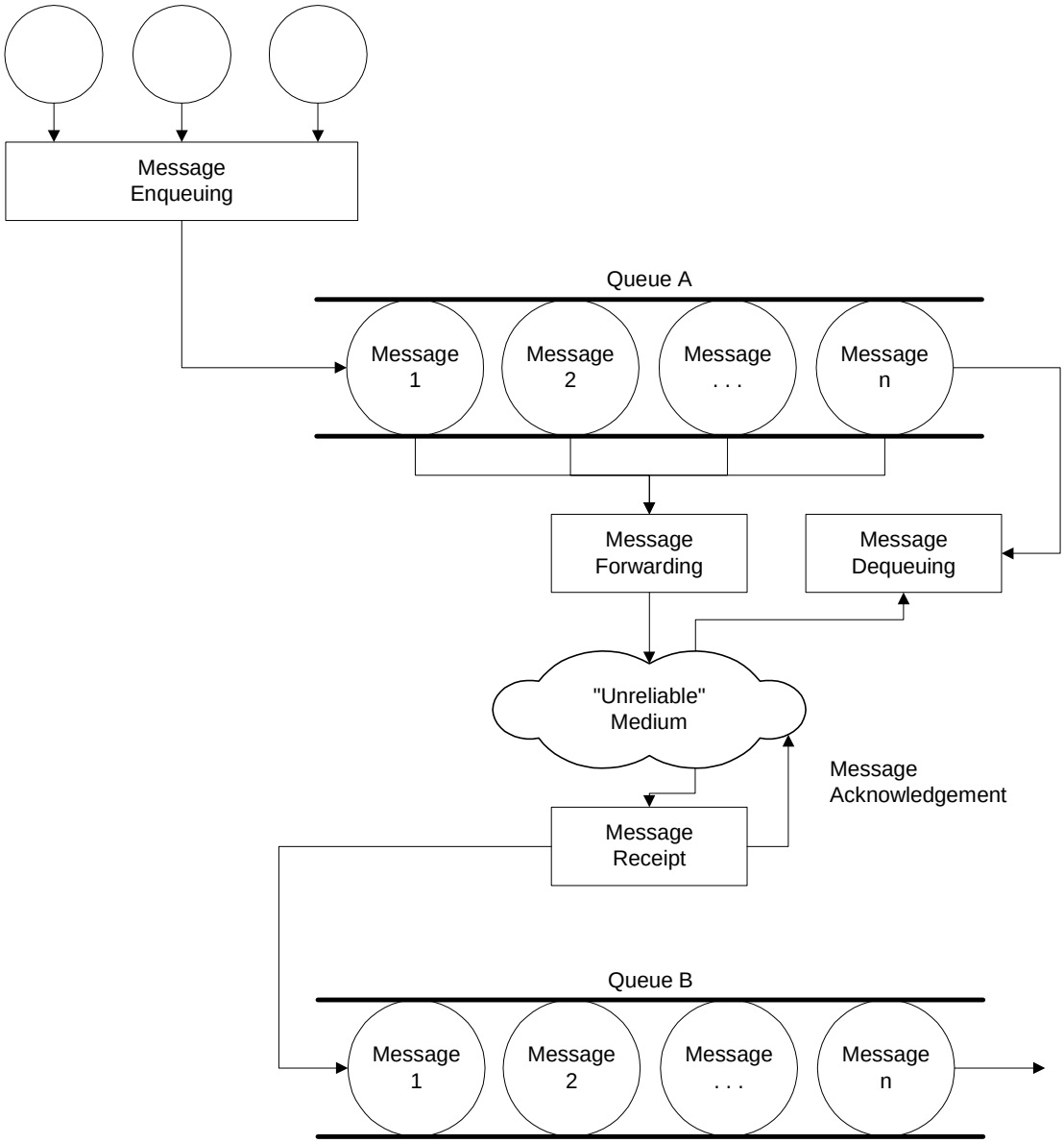
Figure 8 shows the system utilizing a tier (above the routing logic and on both sides of the Internet cloud) referred to as "message queuing middleware." This term describes a variety of commercially available products whose purpose is to implement a reliable queue of arbitrary messages spread across multiple nodes of a system. Often the multiple conceptual layers of the system correspond to geographically separate physical locations, as in the option proposing here. Message queuing software is often referred to as "middleware" because it usually occupies an architectural tier between the user interface, or business logic driven by the user interface, and the relational database back-end. Message queuing software is vital to the design: it increases the reliability and scalability of the system.

The most important consideration is system reliability. The Internet is an inherently unreliable medium, as are most networks in general including local area networks (LANs) and wide area networks (WANs). When a message departs one location on the Internet bound for a second location, it takes an unpredictable path through an unknown number of intermediate computers, routers, switches and communication lines. It will usually, but not always arrive at its destination. This is where message

queuing software comes in. Figure 8 shows a conceptual representation of a message queuing system operating over an “unreliable” medium, such as the public Internet.

The software maintains separate queues in different locations ensuring that messages placed in Queue A eventually make it to Queue B. This is accomplished by forwarding the messages to the destination queue. When the message is received at the destination location, an acknowledgement is sent to the sender, who can then remove the message from the source queue. If an acknowledgement is not received in a suitable period of time, the message is re-sent and this process is repeated until a positive acknowledgement is received. Even if the machines that host Queue A and Queue B and the communication medium that connects them are not always operational, this method will eventually get the message to its destination. Two or more queues can thus be serialized to form a reliable store-and-forward network.

Figure 8: Message Queuing Software



The second function that message queuing software provides is increased scalability. Most operations that occur in the course of serving web pages and receiving web browser post-backs occur in a synchronous fashion. Operations for a given web user occur in a strictly sequential fashion, and the next operation step cannot proceed until the prior step has executed to completion. Although such coupling is simple to design and implement, it can often create bottlenecks that result in system failure.

For example, consider the situation in which the web server has received form information from the user's browser and invokes a stored procedure in the database server to persist the information in relational database tables. If this operation is performed synchronously, the web server task that is communicating with the user's web browser is kept active but paused while waiting for the database operation to complete. Any number of things might cause the relational database to be slow in performing the stored procedure call. Scheduled backups, maintenance or partial drive failure might cause sluggish response. A system failure or communication failure can temporarily interrupt service. It is not uncommon for too many simultaneous requests to overwhelm the database server. On the web server side, more and more transactions pile up and remain open until the web server runs out of resources, causing it to fail. Not only does the web service then become unavailable, but pending transactions can be lost as well.

Message queuing software mitigates these problems. In the scenario described above, the call to the RDBMS stored procedure from the web server can be replaced with an operation to enqueue the stored procedure request. On the database server side, queuing software can serially dequeue the requests and perform them sequentially. From the web server's point of view, the database operations are now performed *asynchronously*, and although the web server cannot be sure when they will be performed, it knows they will happen eventually and can terminate service with a particular web browser much sooner. The result is that the system can scale up to handle many more users, with service degrading gracefully as the number of users increase, rather than reaching a critical threshold of users and failing all at once.

Virtually all database-connected web sites that service a large user community and/or handle a large number of transactions utilize some sort of messaging middleware. There are numerous examples of products that fall into this category, including TIBCO, Microsoft MSMQ, SonicMQ, IBM MQ Series, and others.

5.4.10 Message Formats

The key to success of this option will be negotiating and developing a set of standards for the transmission and receipt of data between the front-end site and the back-end agency servers. Although we can anticipate some of the issues involved, make suggestions and offer advice at a higher, "generic" level, the detailed standards themselves cannot be determined this early in the process. It is likely that determining the standards will consume a substantial portion of the early effort should this option be chosen.

A number of choices are obvious. The public Internet, with appropriate confidentiality protocols applied, has become a secure, reliable and affordable medium for connecting geographically dispersed computers. To this end we propose that the front-end and back-end systems communicate over the Internet using the HTTPS (secure sockets) protocol. More security, in the form of additional encryption mechanisms, might be employed on an as-needed basis.

A second obvious choice is the use of XML to format the messages moved between the systems. XML is a non-proprietary, virtually universal protocol for message syntax that can be shaped to conform to almost any variation in data structure and content. By determining and specifying the syntax and semantics of the XML messages that move between the common front-end and the CDC and FDA back-ends, we will have effectively defined the communications standards that will be used.

As part of the NHSN effort, a good deal of effort has gone into investigating and adopting data standards that are both specific enough to handle the adverse event reporting task at hand and yet general enough to ultimately encompass substantive domains outside NHSN's current context (i.e. nosocomial infections, etc.). The NHSN project team has identified HL7 as the current leading, most relevant health data standard and has used elements of HL7 to inform and shape the NEDSS data standard initiative. Consequently, NHSN will utilize, to a greater or lesser degree, a data model derived from NEDDS to structure project data.

We propose the creation of a variety of HL7/XML-based message types (e.g., NNIS message, BPD message) for transmission of information between the web server and the specific systems. To the extent possible, each message type will share common data elements and definitions, although there is every reason to expect that each message will contain types of information unique to that message type.

5.4.11 Variations and Configuration Options

There are a number of aspects of this option that are potentially problematic and will require considerable discussion with stakeholders and careful consideration in order to implement. The problems involve the issue of identification of users, and by extension, the behavior of the system as it interacts with identified users. Specifically, there are a number of alternatives around where to perform:

- Rights administration
- Identification of users
- Generation of custom pages based on identity.

Rights administration is the collection of activities performed to define who has access to the system and what each user is capable of doing. Rights administration is hierarchical in structure. For example, there might be a top-level administrator, or "super-user" who has the authority to modify all aspects of the system, followed by high-level administrators under the super-user, with facility-level administrators at the next level and finally normal users at the bottom. This is not necessarily the specific hierarchy we are recommending, it is merely an example of how rights administration might be structured. The actual structure will follow the requirements established by the administrators and users of the system.

The first issue that arises is where rights administration should be performed, either at the common front-end web site or at the CDC and FDA sites. The common front-end site offers the greatest but there are a number of reasons why this might not be the best choice, at least initially. The different agencies and programs might require different standards for establishing identity and issuing rights, and these standards might change over time. For example, the NHSN site will require that digital certificates be installed on user computers, whereas the FDA systems might not. Keeping rights administration at the agency site allows the agencies to retain more control over the process, and this might be important to them.

A second reason to keep rights administration at the CDC and FDA agencies is that it often requires substantial human involvement, with agency staff providing help and advice, restoring accounts, making determinations, changing passwords, over-riding system defaults and policies, etc. Since such decision-making can have far-reaching consequences, the individuals providing help and issuing control over the user community might best be agency personnel, as opposed to individuals operating the common web site.

Although CDC and FDA agency staff could perform rights administration remotely, over the web to the common web site, this scenario would require that all of the database infrastructure and program code for rights administration be moved to the common web site – from all four agency systems – and this task could prove more difficult and time-consuming than moving the information gathering aspects of the four systems.

The second issue that arises is where authentication of users should take place, at the common web site or at the agency sites. Once again, the obvious approach is to handle authentication at the common web site.

Like rights administration, this authentication requires that the database infrastructure that persists user names, accounts, passwords and associated rights be located at the common web site, and this in turn implies that a replication mechanism be employed to keep authentication information at the common web site synchronized with CDC and FDA agency sites. If the same database platform (Oracle, SQL Server, DB2, etc.) is in use at each agency and at the common web site, this approach is not too difficult; if different database platforms are in use it becomes much more intractable.

The other option is to perform user authentication at the agency sites. Under this scenario, the common web site prompts for identifying information, encrypts it and passes it to the agency sites. They perform the authentication process and either reject the user or issue a time-stamped electronic "ticket" that permits the ticket holder to use the system to report events to a particular system for a fixed period of time.

If both rights administration and authentication continue to reside at agency web sites, which is where they are located now, the design and implementation of the common web site is simplified. This approach leads to a partitioning of responsibilities in which the only function of the common web site is to collect event information from authenticated or anonymous users, as appropriate, and forward it to the target site. This scenario, as applied to the NHSN system, is shown in Figure 9.

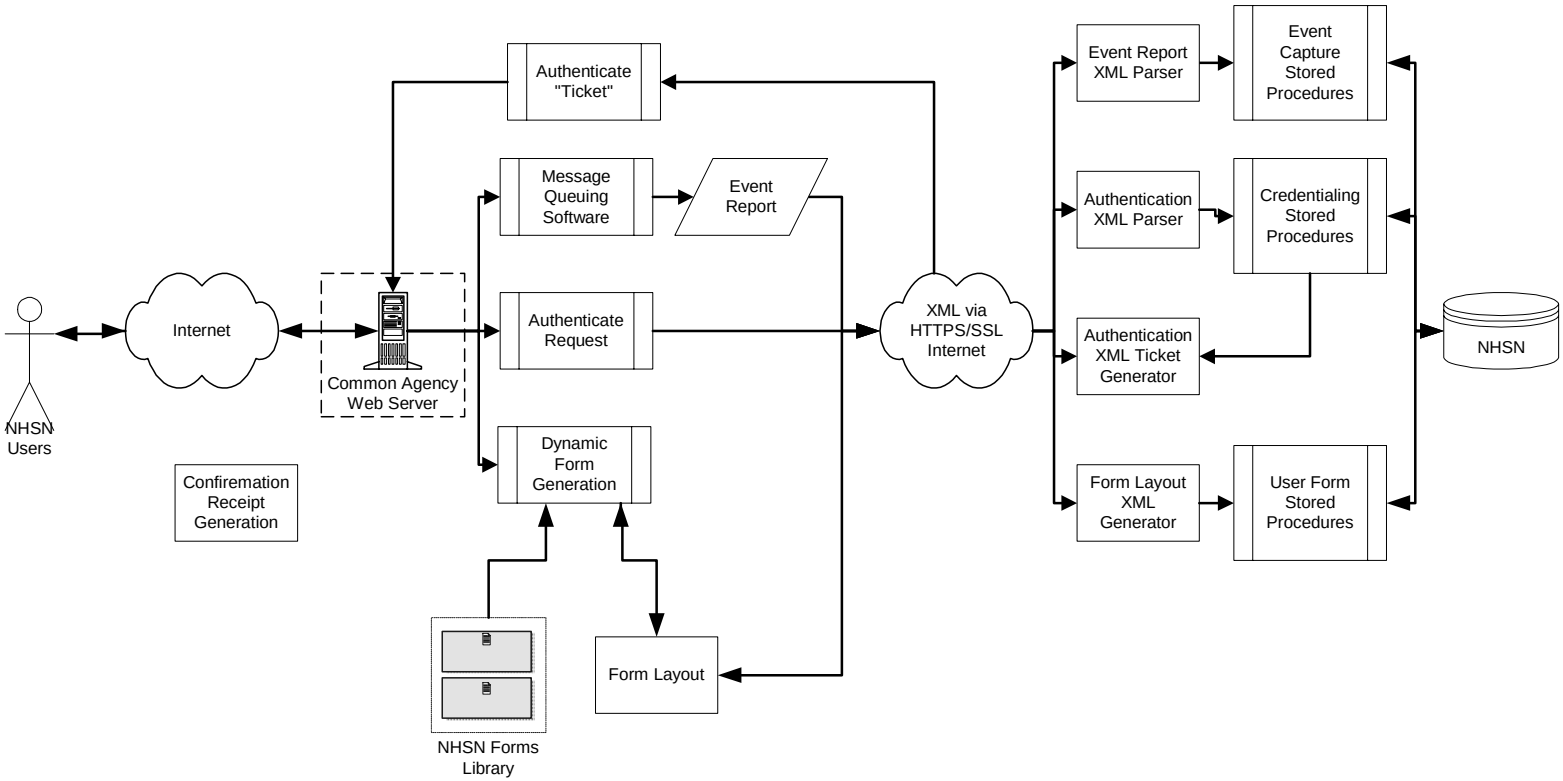
A complicating factor, for the NHSN system, is dynamic creation of differential content based on a particular user's rights and group membership. NHSN will allow facility administrators to determine which questions users at their facility see on event reporting forms. This complicating factor means that it is not sufficient for the NHSN site to inform the common web site that user X is authorized to report an error, it must also convey the set of form fields, labels and descriptive text that user X will see, and perhaps other user-specific details as well.

Although a difficult problem, there are several design options for achieving this result. Once the universe of form fields, labels and descriptive text has been defined, instead of simply authenticating a user, the agency site can respond to the common web site with XML that specifies precisely what form content a given user should see. The common web site can then use a scripting language, such as JSP, ASP or Perl, to build the pages the user sees on the fly.

The message queuing approach described previously is an excellent method for coupling the information-gathering common front-end to the agency's back-end sites, since the asynchronous queuing occurs when the interaction with the user is complete and is essentially invisible to users. It is not clear that message queuing is equally suited to handling the back and forth XML interaction required as a user moves from page to page. Message queuing middleware could introduce unacceptable delays into the page generation process; however, the alternative is reduced scalability and reliability. These are difficult engineering decisions that will need to be addressed during the implementation phase.

If substantial complexity must be introduced at both the front-end and back-end to accommodate a vertically integrated system such as NHSN, where rights administration, authentication and dynamic content are tightly coupled and inextricably woven, does it make sense to front-end it at all? Or should *standards* that define the appearance and behavior of a common web site just be pushed back to NHSN? Under this scenario, the common agency web site would either serve and solicit FDA content or redirect browsers to the standardized NHSN site. Once again, this is a complicated decision that must take into account both engineering considerations and organizational preferences and mandates.

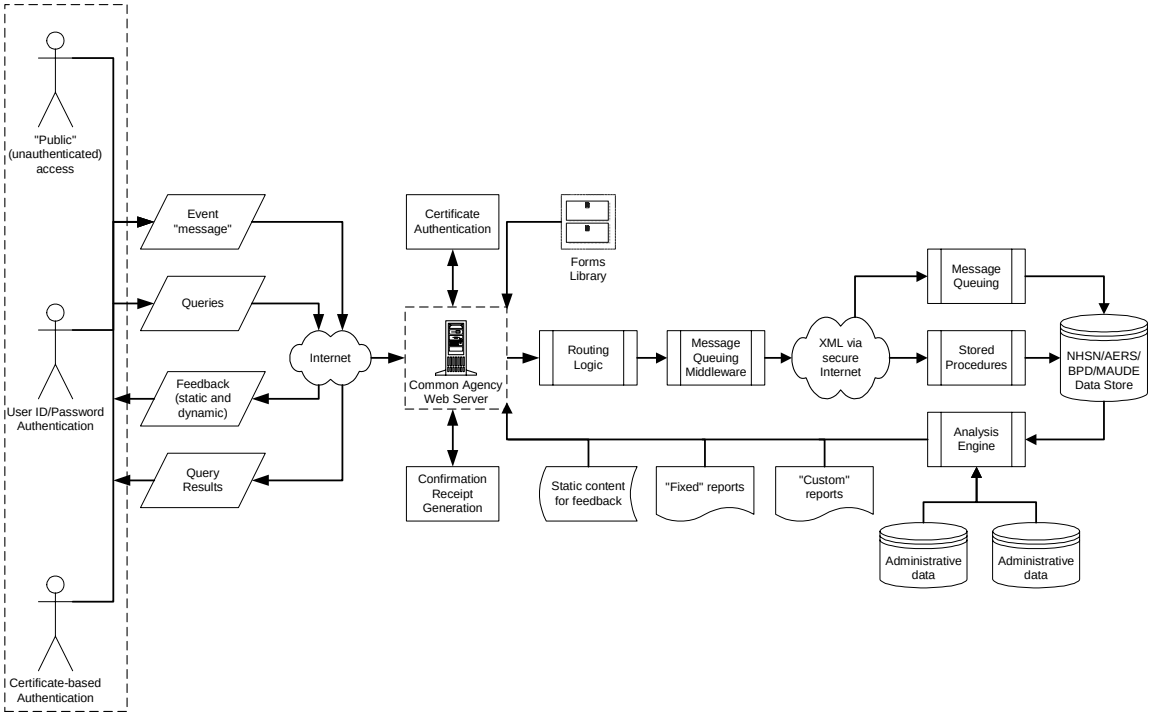
Figure 9: Overview of NHSN



5.4.12 Phase 2 Project Scope

The vision of Option 1 is to tackle breadth of scope first, integrating all four systems across two agencies - but to attempt only the visible front-end integration at first, and to extend the scope of development to the data store and analytic reporting functions later. The metaphor is *horizontal* integration first, *vertical* integration in subsequent phases. During Phase 2 of this option we anticipate working towards a common data model and migrating data from the four systems into this new model. Additionally, we advocate moving to include other data sources, derived from administrative data systems, that will assist in providing benchmarks and appropriate denominators to augment the reporting functions already in place.

Figure 10: Overview of Option 1, Phase 2



We envision the following key activities occurring in Phase 2:

- Development of a common data model and repository for collected data
- Addition of administrative data sets
- Extending scope of data collection and analysis to include other event-based systems
- Refinement of reports and analyses conducted using the common data model/repository

5.4.12.1 Integrating the Data Store

Integrating the data store will be a challenging task, but is key to developing a truly integrated adverse event capture and reporting. A number of factors that remain unknown at this time will influence the difficulty of this task including the architecture of the four proposed systems for integration. Modern system design principles encourage a multi-tiered architecture, with separate, independent "layers" that handle, in order:

1. The visible user interface
2. The logic required to present and accept data from the user interface
3. Message queuing, if it is incorporated
4. Business logic, computed values and enterprise "rules" that must be enforced

5. Stored procedures that extract and insert data from the relational database, and implicit procedures such as database triggers and referential integrity rules
6. The logical and physical structure of the underlying relational database(s)

Sometimes not all of these tiers are incorporated, and in some designs adjacent layers are merged. Effort is made to maximize connections and shared state within each layer and conversely, great effort is taken to minimize connections between the tiers. Ideally, the only communication between the tiers is via a publicly exposed interface. Although every design will deviate somewhat from this ideal structure, in general, this decomposition forms the basis of most modern thin-client (browser-based) and client-server designs. To the extent that our four systems conform to this basic web architecture the task will be simplified. If one or more of the four systems is instead structured as a monolithic whole, with connections running outside of established interfaces, the task will be more difficult.

If one or more of the systems to be integrated does not conform to the architecture above, then the first step will be to move the non-conforming systems into some measure of compliance. Most important is compliance at levels 4, 5 and 6, since these layers contain and interface with the data store.

A second factor that will influence the difficulty of merging the data storage aspects of the systems is the relational database platform they utilize. Early indications are that most of the systems use or will use Oracle. If this is the case the task will be considerably simpler. If not, a common relational database will need to be chosen and the systems that do not currently employ that platform will be migrated to it.

Although superficially it might seem that the choice of database platform has its most significant impact at tier 6 of the architecture and diminishes as you move up the tiers, this is not actually the case. There are a number of outstanding third party tools that do an excellent job of abstracting physical structure from one database platform (such as DB2 or SQL Server) and importing it to another (such as Oracle). Once the physical structure has been recreated on the new platform, the data can be migrated table by table. The tools are not perfect however, and such details of physical structure such as exotic types of indices, multi-segment keys and non-standard data types need manual reconciliation. Nevertheless, the tools are a great help.

The larger difficulty occurs at tiers 5 and sometimes 4, if business logic is embedded in SQL. The language facilities available for writing stored procedures differ greatly from platform to platform, and the worst-case scenario is that stored procedures might need to be completely re-written to conform to the target language. Any business logic encapsulated in stored procedures, a common practice, might need to be revised as well. This underscores the reason why the database platform used in the majority of the systems we seek to integrate is the most likely candidate for use in the standardized system. Oracle would be a very low-risk choice for the standard platform, but SQL Server or DB2 would meet the PSTF's needs equally well.

Once the standard platform is chosen, all physical structure, stored procedures and business logic can be migrated onto this platform. Naturally this activity can occur in parallel with the continued operation of the four systems on their original platforms. Naming conventions will need to be applied that distinguish the formerly separate systems to avoid namespace conflicts (such as two systems both containing a "patients" table). A preliminary analysis can be performed at this stage to determine whether any substantially similar tables or structures can be merged. For example, if two systems contain a patient table, those tables might be merged into a single shared patients table. Which tables should be merged will be guided, at least initially, by the standard principles of database normalization.

Next the higher tiers that communicate with the user need to be connected to the newly merged database, making the advantages of the tiered architecture apparent. Even if the underlying physical structure has been significantly modified, these details can be encapsulated in the logic at tier 5, and the stored procedures can present the (nearly) same interface to the levels above it. Significant testing will need to

be performed at this point, and this transition will need to be carefully planned and executed, as it is highly undesirable that the four actual working systems be taken out of operation.

5.4.12.2 Analysis and Reports

Concurrent with planning to transition to the common data store, decisions will need to be made about the physical location and machine resources necessary to perform analysis. Recall that in Phase 1 of this option, the data store and the analysis component for each of the four systems will continue to be at the original agency sites. Once the data store is moved to a common location, the decision will need to be made as to where analyses will occur. This decision will involve technological issues (e.g., computing resources) and almost certainly organizational and regulatory issues. For example, the FDA has policies regarding the nature and type of data that may be stored or transmitted outside their firewall. While the integrated system will be as secure as either of the current systems, it could potentially violate the policies and practices of at least one agency. There are a number of possible architectural choices, and we anticipate that active involvement from all affected entities will result in a solution that is mutually acceptable.

An obvious alternative is to move reporting to the common location as well. Summarization procedures that move through the data row-by-row, such as stored procedures that use database cursors, or statistical packages that do the same row-by-row operations, need to be executed in close physical proximity to the physical database for reasonable performance.

Planning will need to be done to determine the computing and storage resources necessary to subsume the reporting requirements of the previously separate systems into one common system. In general, it is not a good idea to use the same set of processors for analysis as is used to perform transaction processing. The reasoning behind this is well known and revolves around the fact that much less latency (wait time) can be tolerated as users entering data are interacting with forms, than can be tolerated by analysts summarizing data. In addition that summarization requires orders of magnitude more time and resources to accomplish than the small tasks normally required to post transactions against a reasonably normalized database.

5.4.12.3 Adding Administrative Data

A second reason it makes sense to migrate analytic work to the common platform is to enable integration with administrative data. As part of Phase 2, we anticipate moving some form of administrative data derived from CMS' Medicare and Medicaid research databases and AHRQ's HCUP-derived hospital patient data. Moving the patient level data is highly undesirable because of the huge size of the tables. Well-formed samples of Medicare and HCUP data are readily available, and these could prove very useful, although they are very large as well. The Medicare five percent SAF (Standard Analytic File) PUF (Public Use File) outpatient files contain tens to hundreds of millions of rows.

5.4.13 Phase 3 Project Scope

In Phase 3 of the project, we anticipate a continued expansion of the system horizontally, adding additional non-DHHS systems. These systems might be systems operated by States, by the VA or by the DoD.

Activities to be completed in Phase 3 include:

- Making de-identified data available to non-DHHS users (e.g., individual facilities, researchers)
- Incorporating additional event-based data sources
- Developing a plan to make system architecture and standards available to individual facilities for internal use

5.4.13.1 Dissemination of de-identified data

An important aspect of Phase 3 is the creation and dissemination of a de-identified research data set that can be made available to researchers outside the DHHS. This group includes facilities, hospital groups, and health care researchers. These data can be used to explore patterns and trends in patient safety, and ultimately to reduce the risk of harm to patients.

5.4.13.2 Additional event-based data sources

Phase 3 will continue to expand the breadth of the system by including other event-based data sources. These could include State-based systems and systems operated by other Federal agencies (e.g., VA, DoD). This phase will also include and investigation as to whether private systems (e.g., JCAHO, MedMarx) could and should be integrated.

5.4.13.3 Make system architecture and standards available

A final activity in Phase 3 involves developing a plan to make the core architecture (e.g., design documents, source code, data standards, and database schemas) available to facilities, health plans, and other entities. This serves two primary functions: (a) provides facilities with a starting point for internal safety improvement efforts, and (b) sets the stage for a method of inter- and intra-facility sharing of patient safety information.

While the "out of the box" system may not meet the needs of a facility, it could very well serve as a starting point for facility-based patient safety efforts. Moreover, the system could be adapted to meet specific needs and requirements of a given facility.

Should a sufficient number of facilities adopt a variant of the proposed system, this may also provide a framework for exchanging patient safety information and results. By utilizing an XML-based messaging scheme, Option 1 provides a platform that can be used to easily share information across sites. A collection of these systems could be used to share information within a given hospital group, region, or State.

5.4.14 Comparing Option 1 to the Solution Criteria

It is important to evaluate Option 1 with respect to the solution criteria developed and enumerated in Section 5.2. Some of the optional criteria are only marginally relevant to this option, but we look at each of them in turn and comment on the extent to which Option 1 satisfies the criteria.

Facilitate a reduction in the risk of harm to patients. While this goal the most important no system will "magically" reduce the risk of harm to patients. A reduction in risk can only come about as a result of human intervention and process change, and it is impossible to know how staff will use the analyses generated from the system. Progress towards this objective can only be determined empirically as the result of an evaluation study after the plan has been placed in operation and enough data has been collected to reliably assess its impact. Intuitively, there is reason to believe that when the integrated system is fully operational, the information loop is closed and findings are being fed back to practitioners, that the integrated system it will have a positive impact on the reduction of errors.

Make data collection simpler and more similar across systems. Making data collection simpler and more similar is the focus of this Option. The common forms library, composed of common controls and common textual and graphical elements, will make the four separate systems appear to be merely different aspects of the same underlying site. Through proper and judicious use of the user interface techniques elaborated earlier, the site can be made considerably simpler to use than at least some of the existing sites it will front.

Return valuable information to the data source (e.g., provider). Initially, Option 1 will only partially satisfy this criterion. Apart from the prototype data warehouse, Option 1 (during Phase 1) will not store or

contain facilities for the analysis and reporting of data; it simply routes data to existing systems, rendering the infrastructure developed under Option 1 Phase 1 incapable of returning results. It will still be possible to extract data from existing systems on a periodic basis (e.g., weekly, monthly). These data can then be used to construct the prototype data warehouse, which can then be used in the creation of user-centered reports and analyses. Moreover, at least some of the selected systems contain, or will contain facilities for returning data and aggregate results to users.

According to design documents detailing NHSN functional requirements, the system will be able to export data back to data providers and will be capable of generating numerous predefined and *ad hoc*. During Phase 2 of Option 1, facilities will be added to warehouse data and perform analyses. Then the infrastructure of the common web site will be capable of returning results directly to data providers.

Allow incremental development. Option 1 does a good job of allowing incremental development to proceed. The common web site can be developed in parallel with a number of activities, including the incremental development of the CDC NHSN system and FDA MedSun system. Additionally, the data warehousing prototype analysis can be run in parallel with Phase 1 development. The activities that are planned to be incrementally developed subsequent to Phase 1 are the common data warehouse, common reporting, the inclusion of CMS and AHRQ administrative data and integration with other systems, such as developing State or private systems. Existing systems can continue to operate and provide benefit during the development stage.

Protect an individual's privacy. Building as it does on existing systems and invoking the principle that a chain is only as strong as its weakest link, it seems safe to say that during Phase 1 of Option 1, an individual's privacy will be protected to the same extent that the existing systems do. At this phase the privacy protection of these systems cannot be increased. After review of existing FDA systems and practices (some policies and procedures were not divulged to our team by the agency in the interest of security) and the requirements defined for the CDC's NHSN system, we are convinced that these systems have strong security and confidentiality practice in place. During Phase 2 of Option 1, the control of privacy and confidentiality will be more in the hands of project developers, as data warehousing and reporting is transitioned to the common system. We expect that the resulting system will look much like the NHSN multi-tiered access hierarchy, where the providers of data have nearly unlimited rights to use, view and analyze it, but that aggregation and masking are applied as the data is disseminated to a broader audience.

Accommodate the current systems of the PSTF agencies. Option 1 does a very good job of accommodating this criterion during Phase 1. Each of the four agency systems will be required to develop and implement a secure XML-based communications component on top of their systems, and this activity will undoubtedly be considered disruptive by agency systems staff and/or their contractors. As the Option 1 front-end becomes operational, the four agencies will experience a decline in direct user web-based communication, but the remainder of system activity will be very much unchanged. The disruption the agencies experience will be small compared to the dismantling and reconstitution of the four systems that would be mandated by an end-to-end integration. However, this is precisely what is expected to occur during Phase 2 of Option 1. The extent to which this activity will be disruptive will be determined by the difference between the existing systems and their reconstitution under the common agency system. It is possible that the common system will bear a strong resemblance to the NHSN system and if this is the case then the disruption to the NHSN user community will be minimal.

Facilitate data sharing among the PSTF agencies. During Phase 1, this option does little to increase data sharing among the PSTF agencies. This is by design, as we anticipate a number of administrative, regulatory, and legal obstacles will have to be overcome in order to allow FDA and CDC data to commingle. However, this criterion is partially satisfied by construction of a prototype data warehouse in Phase 1, and the development of a common data repository in Phases 2 and 3.

Incorporate a recommendation on a standard event-reporting format(s). Although the common front-end will implicitly establish a standard error-reporting format, it is not part of Option 1 that a formal standard be developed and promulgated. In addition, during Phase 1 it is probably premature to attempt to establish a standard, as it has already been established that it is very difficult to combine error report information across systems. Hopefully the results of the data warehouse prototype analyses will help determine changes that can be made to the data collection process to facilitate combined reporting and analysis. If and when this happens the project will be in a better position to formulate a standard. We do not anticipate that this will occur until the second phase of the Option 1.

Develop a plan for building a secure data collection, storage, and reporting system. Security is an integral component of Option 1, as is the ability to utilize a variety of authentication schemes. Certain data are transmitted via cryptographically strong Internet connection (SSL) with or without a username/password, and other data are sent to the common agency web server via certificate-based encryption schemes. Although not explicit in the diagram, we anticipate standard security tools (e.g., firewalls) will be used to protect both the web server and the underlying databases.

Incorporate a mechanism for collecting and analyzing information associated with "root causes" of adverse events. While this criterion is not specifically address the collection of RCA data, it does not preclude collection of these data. In short, Option 1 can be implemented with or without RCA data, although such data would almost certainly be useful.

Develop requirements for a system that includes information on inpatient medication errors. Option 1, as currently defined, does not satisfy this criterion. It is conceivable that at some point during Phase 3 (or beyond), as more systems are incorporated, inpatient medication errors might be included, but there is no definite plan when this will occur. However, USP (USP, 2002) found that although medication errors are not uncommon, most (97%) do not result in harm to patients. Thus, focusing on inpatient medication errors may not be as high a priority as we originally believed.

Increase the value of the individual pieces of information by linking them with other types of information. The data warehousing prototype is a first step in this direction. The prototype should reveal what needs to happen on the data collection side to make this goal possible. The NHSN system makes some provision for attaining this goal in the sense that it will allow the uploading of aggregate benchmark data to facilitate reporting. Ultimately, this goal will be achieved in Phase 2 of Option 1 when integrated reporting and analysis is incorporated.

Include a mechanism through which data standards, classifications, technical standards, and best practices can be shared. Option 1 will partially fulfill this criterion. Through its early (although seemingly partial) adoption of the NEDSS standard, and the use of NEDSS XML messaging as the protocol for front-end to back-end communication, a core technical standard will be promulgated. It remains to be seen whether the data warehouse prototyping project will result in the choice of standard classification schemes, although clearly this is highly desirable. There is no currently defined component of Option 1 that would result in the dissemination of best practices.

That said, to the extent that standards are established and/or recommended by the IOM study on patient safety standards then such standards can be incorporated in the design of the system. It is important to note that such standards must satisfy the regulatory mandates of the affected agencies.

Make data from the PSTF agencies more accessible outside of the agencies. The NHSN system will hopefully lead the way in meeting this criterion. NHSN includes capabilities for the dissemination of aggregate de-identified data. This capability will be operational for the NHSN system during the course of the project. Some version of this capability will be incorporated into the design of the common data warehouse and common reporting capabilities of the Option during Phase 2.

Leverage State reporting systems as data source. Option 1, as currently defined, does not meet this criterion. If AHRQ wants to accommodate a common State reporting format and develops that through

demonstration programs with States, such a format could be added to the forms library. However, routing of information could be complicated, depending on State capabilities.

Provide optional (user-defined) fields for custom event types. Once again this criterion will be met incrementally by leveraging capabilities that are intended to be part of the NHSN system. The design specification for NHSN includes functionality that will allow administrators to define custom fields for their facilities and domains, and then incorporate those fields into custom reports. We anticipate similar functionality will be part of the common data warehouse and common reporting.

5.4.15 Advantages and Disadvantages of Option 1

There are a number of reasons to recommend this approach.

Option 1 demonstrates a positive, visible action to the outside user community by presenting a unified and coherent structure for hospital error reporting.

- It minimizes the re-implementation of existing systems and requires only a modest upfront resource investment from participating agencies.
- It reduces the inconvenience to end users through a simpler, more consistent user interface.
- It is a phased approach that allows an initial demonstration early on, but continues on to build the foundation for a truly integrated multi-system data warehouse.
- It allows the PSTF to take a leadership position while moving the participating agencies toward emerging messaging and data standards.

Although there are a variety of reasons to recommend this option, there are also a number of problems and drawbacks to the plan. Among the disadvantages and potential risk points to Option 1 are:

- At least initially, it may not be possible to follow through on the objective of an integrated, visually and functionally consistent web site for event reporting and related activities to a point of satisfactory closure.

5.4.15.1 Partitioning Functionality of the NHSN

To varying degrees, all four of the agency systems perform, or will perform when completed, considerably more than just the eliciting of information on adverse events. For example, based upon its requirements definition, the NHSN system will:

- Authenticate various classes of users
- Validate facilities providing information
- Enable facility administrators to select the set of fields that the facilities users see and populate
- Allow administrators to change the labels used to define various fields
- Allow administrative users to grant rights to other users
- Provide aggregate data to registered users that are not information providers
- Distinguish organizations actively using the system from inactive users
- Allow the system administrator to perform a wide range of actions that control use of the system by other classes of users
- Enable the management of organization-specific denominator data
- Enable an organization to create and manage patient-level identifying data
- Allow authorized users to export facility event and patient data
- Allow users to perform and manage batch importation of data
- Allow users to generate and customize a variety of pre-defined reports
- Allow users to create ad hoc reports via a QBE (Query by Example) facility

Looking at this list, it is evident that NHSN is much more than a system for collecting information on adverse events. Rather, it is more accurate to think of it as a portal into a collection of functions that support a community of users. This community is to a large degree self-administering, that is, members of the community can admit new members and can alter the view of the site in a variety of ways; they can place data into the shared repository, including data that is not strictly adverse event data (such as patient data and denominator data) and they can extract data in a variety of user-configurable ways.

5.5 Option 2 – Complete Integration of Two Systems

5.5.1 Overview

Option 2 emphasizes making maximum possible use of the existing data while providing a mechanism to learn as much as possible about the technical and organizational issues that affect integration efforts. This option would provide "end-to-end" integration of medical event reporting systems in terms of data collection, data storage, and data analysis with relatively little change in the data collected from each system. In order to accomplish this, initial development would be limited to a few systems. Whereas Option 1 is likely to encompass some aspects of three or four systems, Option 2 is designed to include all aspects of only two existing systems.

Two key points define this approach. One is that the administrative aspects of data collection could be reduced through the integration of data collection points for distinct systems. As with Option 1, this approach provides users with a single access point for submitting information about events, and enforces similarity across systems in terms of both content and conventions.

A second point is that the value of combined data is of greater value than the sum of the individual components. Although it is important to reduce the amount of effort required to submit data, it is also important to link potentially related events, even though the event may come from different data sources. For example, a faulty catheter or other device may lead to an infection or other adverse event. Such an "episode" consists of at least two distinct events – use of a catheter and diagnosis/treatment of an infection. While collecting both pieces of information separately is useful for certain purposes, linking the two events together can illuminate patterns that would otherwise be undetectable. Although the detection of one such episode may not be noteworthy, a collection of several such episodes that share a common thread (e.g., device type) would warrant a more detailed follow up.

We anticipate that development would proceed through three distinct phases, and each phase would culminate in a functional version of the integrated system. These phases are described below, along with a description of the common architectural components, as is an evaluation of the advantages and disadvantages of each approach.

5.5.2 Architecture

This option merges and updates two rather disparate systems into a common system that would be accessible by user communities associated with each of the original systems. Although the specific architectural characteristics vary as development progresses, the general features include a web-based data entry mechanism for anonymous and authenticated submission, development of a common data repository, and a set of web-based analysis tools. Several COTS options are available for each component (e.g., web servers, databases, programming languages), and such a system would be relatively straightforward to implement once specifications have been developed. However, we anticipate that developing the common data model and designing the data repository will require a significant level of effort and coordination with representatives of participating agencies.

5.5.2.1 Phase 1

Phase 1 would integrate two medical event reporting systems (as compared to administrative data systems like HCUP) from different agencies. Although it would be possible to integrate systems that are relatively similar, we expect it will be more valuable to integrate systems with different objectives and/or foci. For example, the integrated system developed in Phase 1 of this approach could involve integration of patient-centered data from the CDC with a device-based system from the FDA. Although there are many possible candidates from integration, the two most promising alternatives are the CDC's National Healthcare Safety Network (NHSN) and the FDA's Medical Device Surveillance Network (MedSun). Both systems allow for voluntary, hospital-based reporting of adverse events, and address important domains of patient safety. The NHSN will initially collect dialysis- and infection-related events, whereas MedSun collects device-related information. All of the data collected by NHSN is voluntarily submitted (i.e., not mandated), whereas MedSun includes voluntary and mandated information. As noted previously, the NHSN replaces the functions performed by the NNIS and Dialysis Surveillance systems, whereas MedSun is designed to augment the existing MAUDE system.

Integrating these two systems and developing a single system allows for a more complete picture of adverse events at a given facility. Such an integrated system would allow hospital-based users (e.g., infection control officers, QA staff) to enter all or most of their medical event information through a single location, using a common data format, and obtain reports and results in a common format. Given the common data model and analysis framework, this architecture would also allow analysts to build "episodes" of related events, such as patients with device failures and subsequent infections. The integrated front end offers the advantages of Option 1, albeit on a smaller scale, and adds capabilities to facilitate advanced analyses.

Figure 11: Overview of Current MedSun Architecture

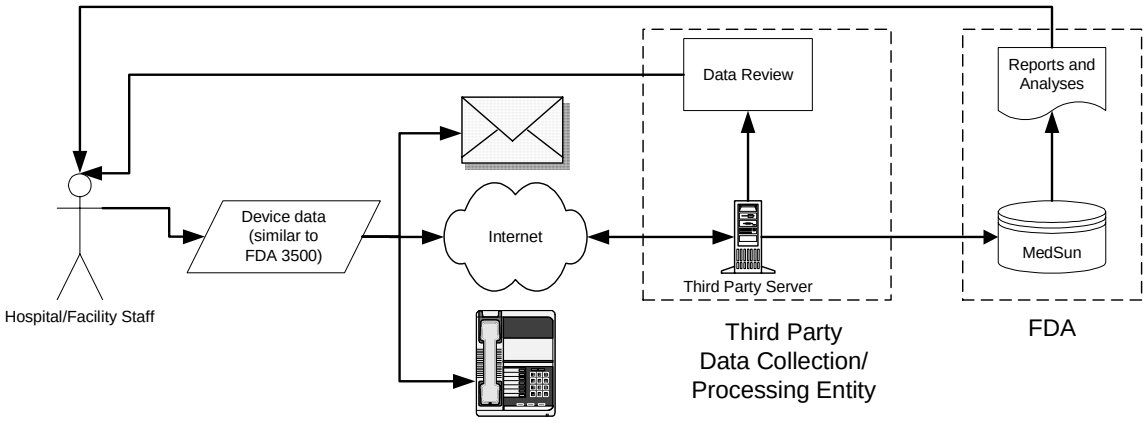
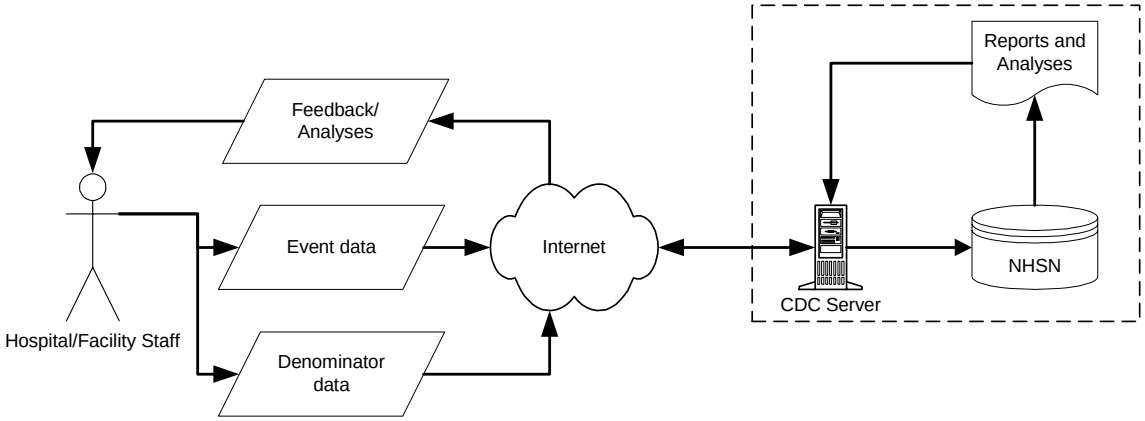


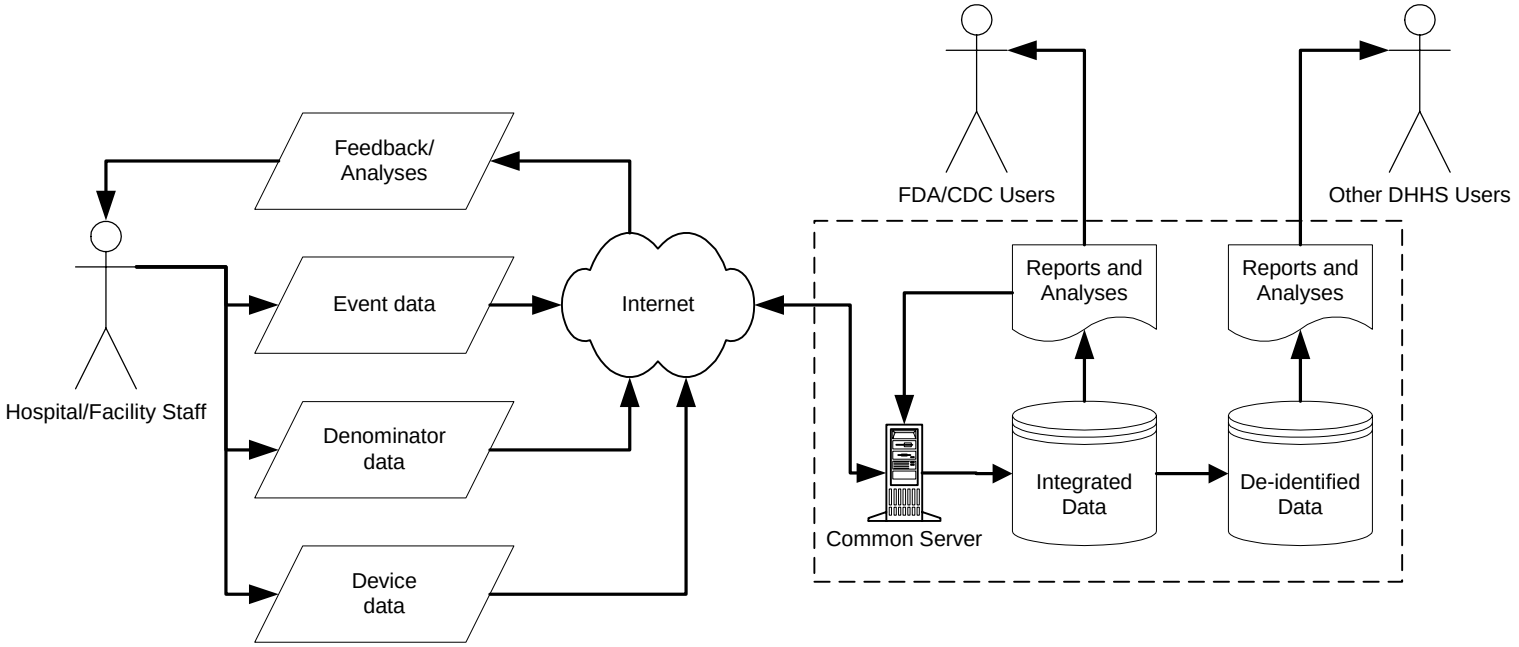
Figure 12: Overview of Current NHSN Architecture



The Phase 1 integration would include development of:

- A common web-based collection system that allows for both anonymous and authenticated data collection,
- A common data model which accommodates information from each agency,
- A centralized data warehouse accessible to appropriate agencies and allowing for user- and role-based data access,
- A separate de-identified data repository for data sharing among agencies and with other researchers,
- A web-based analysis tool, and the ability for certain users to create data extracts for off-line analysis.

Figure 13: Overview of Option 2



Development of common web-based input system

As with Option 1, development of a common front end is the most public aspect of the system, providing users with a common entry point for collecting information. The purpose of a common web front end is twofold: expedite data processing; reduce the reporting burden.

Common sense and extant research (Reason, 1990) suggest reducing the latency between when an event occurs and when such data are available for analysis is a critical step in the process of improving safety. Much as a patient suffering a stroke or heart attack benefits from prompt attention and treatment, timely submission of medical event information is key to prevention of future adverse events. Submitting data by mail could take several days, and data entry could take several more days. As the recent anthrax attacks illustrated, a difference of a few days can mean the difference between life and death.

If reducing the time between when an event occurs and when it is reported impacts the quality of the data system, reducing the burden associated with submitting event-related information should have an effect on the quantity of data submitted, whereby the volume of events increases as barriers decrease. The result should be a more complete and representative representation of the patient safety landscape. This can be used to inform the patient safety agenda and ultimately improve quality of care by addressing those domains with the greatest opportunities for improvement.

The proposed architecture eliminates two data entry channels present in MedSun: mail and telephone. This elimination is chiefly for efficiency, and reflects the ubiquitous nature of Internet access in today's healthcare landscape. It would be possible to retain these data entry mechanisms, although given the facility-based nature of the proposed system we do not anticipate a significant number of events would be reported through these channels. Dixon and colleagues found that replacing a paper-based system with a web-based event reporting system resulted in an 83 percent increase in the number of events submitted, which suggests that a web-based system can not only effectively replace a traditional reporting system, it may be superior to systems which depend on paper forms, fax transmissions, and telephone reports.

Both MedSun and the NHSN allow for web-based event reporting, although the form layout and content differs between the two systems. Since the two systems collect information regarding different types of events, it is unlikely (and perhaps undesirable) that a single web form could be developed which completely encompasses all information collected by both systems. However, a single web site (could be developed to collect this information, and "common" elements (e.g., date, patient ID) could be collected using a single form and event-specific information could be entered via set of forms with a similar look and feel. We believe that at least some functionality, and possibly source code, can be extracted from the existing systems. Source code for each system (i.e., MedSun and NHSN) should be available, and a code review/comparison of may expedite development.

From the users perspective, this change is likely to be somewhat trivial, and could be accomplished by a) redirecting users from existing sites to the new site, and b) communicating with existing user to explain the change.

Development of common data model

This is perhaps the most challenging aspect of the proposed design, as it entails developing a common database architecture/data model for both MedSun and NHSN information. In the interest of future development efforts, the data model should be sufficiently generalizable to accommodate other data types (e.g., AERS, BPD) that may subsequently be incorporated. Since neither the MedSun nor NHSN model is likely to be broad enough to encompass both event types, this activity would involve the development of a new data model and migrating information from the existing systems to the new system. This is obviously a disruptive activity, and would touch every aspect of the system from the nature and type of information entered and stored in the system, to the manner in which data are analyzed.

Although disruptive, there are a variety of tools available to facilitate this transition. The CDC have developed a comprehensive Public Health Data Model, which could be modified and extended to include any data elements that do not currently fit. Relatedly, the HL 7 organization has developed a Reference Information Model (RIM), which provided a basic framework for capturing and storing information from both MedSun and NHSN data sources. The International Conference on Harmonisation (ICH) maintains a set of standard for the transmission of adverse event information. Although chiefly used for transmission of data, it may be possible to develop a more abstract model that would be compatible with existing standards.

We expect the common data model would include not only a logical data model, but would also define possible values and/or formats for several important data elements. For example, uniform codes could be used for certain data elements (e.g., demographic data elements) and a set of possible vocabularies could be defined for other fields, much as current patient claim forms allow for ICD-9 and CPT-4 codes.

Finally, development of the common data model might require changes to the type of data collected by each system. Submitting a device-related event may require more patient-level information than is currently required by MedSun, and submitted information on a dialysis- or infection-related event may require submission of device information that will not be collected in the first version of the NHSN. Where privacy and confidentiality restrictions do not permit such information to be collected, encrypted versions of this information can be stored such that it each person-level record has a unique identifier that can be replicated by the data source but could not be reverse engineered by someone who has only the encrypted identifier.

Development of a centralized data warehouse

Once a model has been developed, it is relatively easy to develop a centralized repository to store the collected information. Any one of several widely used databases (e.g., Oracle, Sybase, DB2) could be employed to store data, and access to information could be granted to specific users or categories of users based on the data element and the user.

This step would consist of several distinct but related activities, including translating the common data model into a platform-specific physical model that corresponds to the, setup and implementation of the data warehouse, and general system administration tasks.

Initially, the design of the data warehouse would be closely linked to the logical design of the common data model. As time and resources allow, the data warehouse could be expanded to include additional data elements and analytic components. This could include data elements that are not collected but may prove useful for analysis (e.g., urban/rural indicators for zip codes).

The data warehouse could be hosted either by DHHS or by a third party. Given modern networking capabilities, hosting by a third party is likely to be transparent in terms of access time and connectivity, and use of a third party may facilitate data collection. The FDA's MedSun system and the FAA's ASRS system both use external entities to collect information.

Development of a de-identified data repository

In addition to the centralized data warehouse, we also propose the development of de-identified data repository for purposed of sharing information with other DHHS data users and even external researchers. This repository would consist of encrypted versions of: a) personally identifiable information, and b) facility identifiers, and limited detail on other potentially sensitive information. Making this information should facilitate research without compromising confidentiality.

From the centralized data warehouse, it should be relatively easy to de-identify these data and create a version of the warehouse that can be shared with extramural researchers. Several options exist with

respect to creation of the de-identified data warehouse, and two of the most prominent relate to the design and logistic aspects of the system.

In terms of design, algorithms exist which could de-identify individual data in either of two ways. One method allows encrypted identifiers to be back-translated to match the original data, which can be useful for epidemiological studies collaborative efforts between extramural researchers, DHHS staff, and even facilities. Alternatively, data can be de-identified in such a way that records in the resulting data set cannot be linked to the "source" records in the data warehouse. This can be accomplished by removing any non-essential information that could be used to identify patients (e.g., medical record number, SSN) and generating synthetic identifiers for patients, facilities, and other key data elements.

In either case, certain demographic and other data elements that may be used in analysis. This can be accomplished by converting potential identifiers into broader, categorical variables. For example, age would be converted into age group, 5-digit zip codes into 3-digit codes or State codes.

Another issue is how users should be allowed to access the de-identified data set. It is possible to implement the de-identified data base in much the same way as the data warehouse, granting online access and providing web-based analytic tools to a set of either anonymous or authenticated users. Alternatively, the data set could be made available in an analysis-ready format and distributed on a periodic basis. The latter approach is less resource intensive, in terms of both development and maintenance, but limits the types of research that can be performed with using these data.

Implementation of web-based analysis tools

The final component includes a suite of a web-based analyses similar to those used in the NNIS and those planned for the NHSN. A key factor in the success of any system is the perceived value to the user, and such tools allow users to generate summaries and comparisons to other facilities either immediately following data submission or on an ad hoc basis.

For this activity, we anticipate the development of "canned" reports and ad hoc reporting functions. Canned reports would include high-level reports that could be tailored to each facility or specific types of events, conditions, and populations. Ad hoc reports would enable users to create custom reports and analyses using web-based tools. Analyses would typically be performed using data stored in the centralized warehouse, although data snapshots could be downloaded for more extensive off-line analysis.

Although there are certainly a number of architectural options, many of these features and functions are included in the NHSN and the existing design and source code might be employed as part of the reporting system. This could result in cost and time savings during implementation.

5.5.2.2 Phase 2

The second phase would involve designing and incorporating a mechanism to include information from one administrative data system (e.g., CMS claims/encounters, HCUP discharge data, or NCHS surveys) that could enhance results from the integrated systems in Phase 1. A logical extension of the first step is to broaden the scope of available data, and incorporate other types of data to the extent possible.

This phase has several components:

- Identify what information from various DHHS-based administrative data systems could inform data collected in Phase 1,
- Identify other DHHS event reporting systems that could be added to the integrated system,
- Develop an analysis and software tool for one of the administrative systems (e.g., the one that can provide the most value-added information),
- Incorporate information from the administrative data system into the common data warehouse on an ongoing periodic basis (e.g., quarterly or semi-annually), and

- Integrate other event reporting systems as appropriate.

5.5.2.3 Identify DHHS administrative data systems

Adding information from appropriate administrative data sets (e.g., HCUP, Medicare claims) can provide context for the event- and device-based data associated with Phase I. These data could be linked to existing data where feasible, and used as denominators to create population-based rates. Where appropriate, data could be mined to extract information about adverse events that occur in facilities but are not reported through channels such as the NHSN. Finally, results based on administrative data could be compared to results based on event-reporting systems for certain conditions (e.g., nosocomial infections). Although one might expect some differences in reporting rate, the results of this analysis could inform the design of data collection efforts for both administrative and event-reporting data systems.

Since these and other data may be accessible to a fairly broad audience, it may be necessary to execute data use/data sharing agreements with some or all users who require access to the integrated system. This can be addressed either through a set of individual agreements, or through legislative and executive mechanisms. While the legislative approach is perhaps the most straightforward, it is also complicated and time consuming.

5.5.2.4 Identify other DHHS event reporting systems

While it is important to include information from administrative datasets, it is also important to take advantage of opportunities to incorporate other event reporting systems. Since the MedSun data are generally similar to that collected on FDA form 3500A, and since this form is the basis for AERS and MAUDE systems, it would seem that facility-based reporting for device- and medication-related events could be incorporated into the integrated system with relatively minor modifications.

We anticipate that integrating these data sources would have little impact on the design of the user interface or database structure, but may have a significant impact on the operational aspects of the integrated system. Since there will likely be fewer than 500 facilities involved in Phase I, opening up the system to all facilities is a difference of roughly an order of magnitude. Additional staff and resources may be required to ensure the system will be operational for large user base, and the implementation plan should take into account factors such as the effort associated with assigning username, passwords, and/or digital certificates to thousands of facilities. This is not to say that this cannot be accomplished, only that phased approach may prove more useful. One possible alternative is to allow the system to accept only mandatory (Form 3500A) report and later accept voluntary reports (i.e., those reported on the FDA form 3500).

Assuming both voluntary and mandatory reports are eventually submitted to the integrated system, it may be possible to phase out the existing systems that currently house these data (i.e., AERS, MAUDE) and reduce the overall cost of collecting information by centralizing data storage and analysis functions.

5.5.2.5 Expand analytic capabilities to include additional datasets

Assuming the data model adopted in Phase I can accommodate data added in Phase 2, importing the data should be relatively easy. However, this opens up a range of analyses (both simple and complex) that can be conducted. For example, adding additional datasets may make it possible to create population-based rates or comparisons to benchmarks. While such calculations may be easy to perform, adding this functionality to the web-based analysis tools will require some planning and resources. Although making these data available for ad hoc analysis should be straightforward, development and revision of canned reports may be more challenging as it opens up a wide range of possibilities. A useful activity would be to query users of the integrated system in order to determine what reports they would like to see developed

and even how such reports could be formatted. Engaging users in this way helps ensure that facilities are using the system, and that the analytic goals of the user community are being served.

5.5.2.6 Incorporate administrative data into the common data warehouse

Once potential administrative data sources have been identified, the next step is to transform these data and load it into the common data warehouse. If very large data sets (e.g., Medicare claims) are involved, it would be more practical to load summarized data sets that do not store information at the level of the individual claim or enrollee.

Although new data are being added to these systems on an on-going basis, we expect the most productive means of incorporating these would be to load extracts into the data warehouse on a periodic basis, either monthly or quarterly.

5.5.2.7 Integrate other event reporting systems as appropriate

As noted previously, Phase 2 may be an opportune time to integrate other event reporting systems, especially MAUDE and AERS, since these systems collect data which is generally similar to that collected by MedSun. The level of effort associated with activity will depend to a large extent on whether both anonymous (voluntary) and non-anonymous (authenticates) data are included. Collecting both would not require significant changes in database design or structure, but might require changes in the scale of the system and resources required to maintain it. However, even a volume of 200,000 submissions per year would translate to an average load of approximately 50 records per hour (during business hours averaged over a seven day week), which is easily obtainable with currently available technology and tools.

5.5.2.8 Phase 3

While it is difficult to predict what system needs will be several years into the future, we expect that Phase 3 would involve adding remaining event reporting systems such as the FDA's BPD system and other systems that contribute to the collective knowledge base developed in Phases 1 and 2.

Phase 3 would also include data from other systems such as the CDC's NCHS, CMS's MPSMS, and administrative data from CMS's OASIS and MDS programs.

5.5.3 Evaluation of Option 2

5.5.3.1 Advantages

The option effectively replaces and augments two systems with one, combining the best aspects of each system. This change should both reduce the administrative burden associated with submitting information about a medical event, and provide value to facility staff who either submit information about events or analyze existing event information.

This approach should also allow for reduced cycle times between input and analysis. In fact, some analyses are available immediately, and others can be conducted within a very short period of time relative to when the event was entered.

Option 2 provides a learning opportunity with lessons that could ostensibly be applied to other patient safety domains including State-based integration efforts and activities to further integrate DHHS data systems.

Finally this approach allows for sophisticated analyses that could not otherwise be conducted including the development of "episodes" and linking devices to specific patient-based outcomes.

5.5.3.2 Disadvantages

An obvious disadvantage of Option 2 is that it does little to encourage the public, or at least non-facility reporting of events. In fact, the initial implementation will likely be limited to no more than 300 hospitals. Although a common data model will be developed in Phase 1, it is possible that future revisions of the data model will be equally disruptive as other domains (e.g., medication errors, medical/surgical errors) are included.

Another disadvantage is that the technological and conceptual model implemented may not scale well as additional systems are ultimately incorporated. It may be the case that a system which works well for hundreds of facilities may not be sufficient when rolled out to the general public. While use by such a broad user community is likely several years away, it is worth considering during Phase 1 how such a system might be expanded.

Finally, there is a significant level of effort and some level of risk associated with development of the common data model. While we feel this can be accomplished within a reasonable time horizon, it is important that the resulting model and associated standards be agreed upon by the DHHS and other entities.

5.5.3.3 Variations

The core of this approach rests with the end-to-end integration of a small number of systems. We have selected NHSN and MedSun to illustrate the proposed approach, but the actual implementation could use any of several combinations of systems. It might be as efficacious to integrate NHSN with AERS, or to combine FDA systems (i.e., AERS, BPD, MAUDE/MedSun, and MedWatch). All of these possibilities use facility-based collection system which are an appropriate starting point for an integrated patient safety effort.

Moreover, regardless of which systems are selected, there is considerable flexibility in how this new integrated system might be implemented. There are several technical options for web servers and databases, each with relative strengths and weaknesses. In our experience, virtually all of the leading options for operating systems, web servers, databases, and the like *can* be securely and efficiently implemented. A key factor in the success of any development effort is the developers experience with the tools and ability to leverage this knowledge. Thus, while we could easily recommend an Oracle-based server with SAS/IntrNet running on a Microsoft Windows 2000 server, we feel that such decisions are best sorted out during the procurement process.

Various components can also be placed at any of several locations, including a given agency or a third party. While we recommend a third party, we also recognize that such a system could be hosted by an existing entity (including AHRQ) provided sufficient resources could be made available.It is also worth considering whether all or some of the NHSN facilities should be included in the integration effort. Since the NHSN is the CDC's primary event reporting system, we recommend developing a pilot phase that includes some (approximately 25-50) hospitals, and include the remaining facilities in Phase 2. This preserves the operational component of the existing system while advancing the integration effort.

As noted previously, we do not foresee the need to allow mail- and telephone-based data collection for medical device data but these methods could be incorporated with relatively minor changes in the design if required. Additional modules would need to be developed to allow staff to enter these data, and resources would be added to accommodate the data submitted via these routes.

6 Summary and Conclusions

6.1 Findings

This project comprehensively examined systems within the FDA, CDC, CMS and AHRQ with respect to both their current role in medical error reporting/analysis and their future integration. MEDSTAT project staff formed and consulted with an expert advisory panel, extensively reviewed system documentation, conducted interviews with key agency personnel and researched medical error reporting systems in other jurisdictions, both within and outside the U.S.

From this work, several key findings emerged:

- The systems demonstrated a wide range of diversity across a number of key dimensions including purpose, scale, anonymity, coding systems, IT structure, and depth of data collection.
- With respect to their contribution to medical error reduction, the systems generally fell into two categories:
    - those that directly receive adverse event report and support their analysis/investigation, and
    - those that do not contain adverse event reports but may contribute to research and analysis of patient safety issues
- Given the lack of common identifiers/data elements, linkage of data across systems, as currently structured, would be very difficult, if not impossible.
- Competing and overlapping medical error-related coding systems will hamper integration.
- The majority of product-related adverse events are reported to the FDA by manufacturers.
- Adverse event reporting by user facilities is relatively limited and is not well supported by existing structures and processes.
- Reporting of adverse medical events faces many barriers including liability and confidentiality concerns and fear of reprisal. The legislative privacy and security framework within which these systems exist is complex and must be addressed in order to support expanded medical error reporting.
- Medical error-related activity is burgeoning at the institutional and state-level as well as internationally and within professional/industry organizations. As this activity grows rapidly, so does the need for leadership, convergence, and integration.

Informed by these findings, the project team identified a set of required and optional Solution Criteria consistent with the project mandate and advisory committee input.

6.2 Recommendations

Various integration options were developed and evaluated against the Solution Criteria. Two leading options emerged and were fully developed. Both options lead to the same end result of integration of all of the relevant error-related databases but differ in the phasing of the work, especially phase 1:

- Front-End Integration and Prototype Data Warehouse (Option 1, Phase 1): Development of a common agency web server for the reporting of adverse events to three FDA systems (AERS, MAUDE and BPD) and the CDC NHSN system and development and testing of a prototype for consolidating reports, conducting analyses, and returning information learned to reporters to the system.
- End-to-End Integration for Two Systems (Option 2, Phase 1): Integration of two medical event reporting systems from different agencies with respect to adverse event reporting, data storage and data analysis. Leading candidates for integration were identified as MedSun and NHSN.

Both options preserve existing system functionality. Section 5 of this report describes each of these options in detail. Based upon our investigation of the current status of event reporting across the four agencies that comprise the PSTF, we recommend Option 1 for implementation.

6.3 Implementation Steps

Implementation of Option 1 is envisioned in three phases. In Phase 1, horizontal integration, a common agency web server will be developed to serve as a mechanism for eliciting event reports from users and forwarding the information to the appropriate agency systems. The permanent storage of complete report information will reside with the systems maintained by the agencies at this phase. In a parallel Phase-1 activity, a prototype for a centralized, de-identified database for analysis will be assembled from *existing* databases and tested, with approaches for summarizing data and returning it to the reporters of errors. Early developmental work on the feedback of information is not only essential for learning but also for providing value to reporters whose cooperation is paramount to the success of the system.

In Phase 2, vertical integration, work will foster a common data model for the integrated systems and inclusion of real-time reports in the common data warehouse. Key steps would be:

- Integrating the data store
- Integrating the analytical and reporting capabilities
- Integrating some administrative data from the CMS Medicare and Medicaid research databases and HCUP

In Phase 2, after having developed a common data model and platform in Phases 1 and 2, the system will continue to expand horizontally, adding additional DHHS and non-DHHS systems.

6.4 Advantages

The project team has identified the following advantages of Option 1:

- It demonstrates a positive, visible action to the outside user community. By presenting a unified and coherent structure for all hospital error reporting to the CDC and FDA, it strongly conveys the message that the DHHS agencies will maintain a singular focus on the detection, capture, analysis and reporting of all aspects of medical errors.
- By encouraging the reporting of adverse events by those who are closest to care, the system will capture the type of information that will support a deeper understanding of medical error, implementation of positive actions and, ultimately, facilitate a reduction in the risk of harm to patients.
- It provides a flexible infrastructure that will support the modular development of a broader facilities-based adverse even reporting system. Modules can be added to address emerging public health concerns, including the need for a coordinated sentinel reporting system for bioterrorism-related incidents. At the same time, modules can be added to address facility-specific or regional interests.
- It reduces the inconvenience to end users through a simpler, more consistent user interface. By standardizing the elements of the user interface, and utilizing a single consistent procedure for access to the system, it opens use to a broader group of users and eliminates the need for users to establish and maintain specialized, unique familiarity with a variety of “niche” systems.
- It is a phased approach that allows an early initial demonstration after two years with the completion of Phase 1. Phase 2 continues building the foundation of a truly integrated multi-system data warehouse and in Phase 3 capitalizes on this foundation by bringing in and utilizing multiple types of adverse event data from a variety of sources.
- While accomplishing the goals above, it minimizes the re-implementation of existing systems. Our investigation has confirmed that a significant level of effort has gone into developing the systems now used by the FDA and CDC and, for the most part, the systems employ advanced architecture and embrace the most recent medical and technological standards. The work simply has not been coordinated between the agencies. This option builds out from work already performed and requires only a modest upfront resource investment from participating agencies.

- It moves the participating agencies (and ultimately other partners in the project) toward the emerging HL7 standard for data structure and messaging.
- It allows the PSTF to take a leadership position. By demonstrating early on that various types of event reporting can be merged and standardized, it sets a precedent for other efforts.

6.5 Conclusion

In spite of these benefits, the approach is not without risks. Our efforts to research the existing systems has pointed out very clearly that the expertise with and the authority to shape these systems is spread across a great many agency staff and contracting firms. The inertia of existing systems and the momentum of developing systems should not be underestimated. Bringing all of these parties and forces into line to accomplish the objectives set out here will be a monumental task, and one that is perhaps not entirely under the control of the PSTF. During the course of this project we have worked with and listened to many of the leading stakeholders in the patient safety and medical errors world. They do not speak with one voice and the disparate issues they raise all appear valid to those trying to synthesize these views. Even more than the technological hurdles that must be overcome, we believe that these environmental issues represent the greatest risk to implementing Option 1 within the time frame and budget we have suggested.

References

AHA News Now. CDC pushes awareness in campaign on hospital-acquired infections. March 27, 2002. Available at: http://www.ahanews.com (last viewed April 15, 2002).

Atherton T. Description and outcomes of the DoctorQuality incident reporting system used at Baylor Medical Center at Grapevine. *Baylor University Medical Center Proceedings* 15(2):203-208, April 2002. Available at: http://www.BaylorHealth.com/Proceedings.

Australian Council for Safety and Quality in Health Care (ACSQHC). "Safety in Numbers: A Technical options Paper for a National Approach to the Use of Data for Safer Health Care" in Safety in Practice – *Making a Safer, Second Report to the Australian Health, Second Report to the Australian Health Ministers' Conference*. Canberra, August 2001.

Bagian JP, Gosbee JW, Lee CZ. Partners in Prevention: The VA-NASA patient safety reporting system. Federal Practitioner, 18(3):10-15, March 2001.

Bagian JP, Lee C, Gosbee J, DeRosier J, Stalhandske E, Eldridge N, Williams R, Burkhardt M. Developing and deploying a patient safety program in a large health care delivery system: you can't fix what you don't know about. *Joint Commission Journal of Quality Improvement*, 27(10):522-32, October 2001.

Battles JB, Kaplan HS, van der Schaaf TW, Shea CE. The attributes of medical event reporting systems: Experience with a prototype medical event reporting system for transfusion medicine. *Archives of Pathology and Laboratory Medicine*, 122:231-238, 1998.

Battles JB, Shea CE. A System of Analyzing Medical Errors to Improve GME Curricula and Programs. *Academic Medicine*, 76, 2001.

Battles JB. Disaster prevention: Lessons learned from the Titanic. *Baylor University Medical Center Proceedings* 14:150-153, 2001.

Battles, JB. Personal Communication. Expert Advisory Panel Meeting, May 16, 2002b.

Battles, JB. *The Need for Data Guidance for Patient Safety*. Presentation to the Institute of Medicine Panel on Patient Safety Data Standards. May 7, 2002a.

Benesch, B., Parr, R., and Stockdale, T. Medical device reporting for manufacturers. FDA Center for Devices and Radiologic Health website, 1997. Available at: http://www.fda.gov/cdrh/manual/mdrman.html (downloaded April 11, 2002).

Bhasale AL, Miller GC, Reid SE, Britt HC. Analysing Potential Harm in Australian General Practice: An Incident-Monitoring Study. *Medical Journal of Australia* 169:73-76, 1998.

Brennan TA, Leape LL, Larid NM, Herbert L, Localio AR, Lawthers AG, Newhouse JP, Weiler PC, Hiatt HH. Incidence of adverse events and negligence in hospitalized patients: Results of the Harvard Medical Practice Study I. *New England Journal of Medicine* 324(6):370-376, 1991.

Bruley, M., Vice President, Accident and Forensic Investigation, ECRI. Personal Communication, March 19, 2002a

Bruley, M., Vice President, Accident and Forensic Investigation, ECRI. Personal Communication, April 19, 2002b

Bureau of Data Management and Strategy (BDMS). "HCFA Data Release Policies and Procedures" in *Data Users Reference Guide*, pp. 1-3. Baltimore, MD: U.S. Department of Health and Human Services, Health Care Financing Administration, November 1993.

Burkhardt M. Developing and deploying a patient safety program in a large health care delivery system: you can't fix what you don't know about. *Joint Commission Journal of Quality Improvement,* 27(10):522-32, October 2001.

Campbell, S. Vaccine Safety: Government's Role. CDC website, September 2001. Available at: http://www.cdc.gov/nip/NIC/35th/Workshops/C3/Campbell-C3.pps (downloaded April 11, 2002).

Centers for Disease Control and Prevention. Description of the NEDSS Base System. CDC website, March 2001. Available at: http://www.cdc.gov/nedss/BaseSystem/NEDSSBaseSysDescription.pdf (downloaded April 17, 2002).

Centers for Disease Control and Prevention. *National Nosocomial Infection Surveillance System Manual*. US Dept of Health and Human Services, 1999.

Centers for Disease Control and Prevention. NEDSS Systems Architecture Version 2.0. CDC website, April 2001. Available at: http://www.cdc.gov/nedss/NedssArchitecture/NEDSSsysarch2.0.pdf (downloaded April 17, 2002).

Centers for Disease Control and Prevention. Overview of Vaccine Safety. CDC website, October 2001. Available at: http://www.cdc.gov/nip/vacsafe (downloaded April 11, 2002).

Chen RT, DeStefano F, Davis RL, Jackson LA, Thompson RS, Mullooly JP et al. The Vaccine Safety Datalink: immunization research in health maintenance organizations in the USA. *Bull World Health Organ*. 78(2):186-194, 2000.

Chen RT, Glasser JW, Rhodes PH, Davis RL, Barlow WE, Thompson RS et al. Vaccine Safety Datalink project: a new tool for improving vaccine safety monitoring in the United States. The Vaccine Safety Datalink Team. *Pediatrics*. 99(6):765-773, 1997.

Chen RT, Rastogi SC, Mullen JR, Hayes SW, Cochi SL, Donlon JA et al. The Vaccine Adverse Event Reporting System (VAERS). *Vaccine.* 12(6):542-550, 1994.

Chen, R. T. and Hibbs, B. Vaccine safety: Current and future challenges. CDC website, 2002. Available at: http://www.cdc.gov/nip/vacsafe/research/ped.htm (downloaded April 11, 2002).

Chen, R. T. Making headlines: Vaccine safety debates and their impact on parents, providers and public health. CDC website, September 2001. Available at: http://www.cdc.gov/nip/NIC/35th/Plenary/Plen-2/chen-presentation.pps (downloaded April 11, 2002).

Comden SC, Rosenthal J. *Statewide Patient Safety Coalitions: A Status Report*. Portland ME: National Academy for State Health Policy, May 2002.

Cousins D. Vice President, US Pharmacopeia. Personal and facsimile communication, March 22, 2002.

Crafton, M. Director of State Affairs, JCAHO. Email correspondence, March 25, 2002.

Davies, J. Implementing NEDSS: the Washington State Experience PowerPoint presentation. Minnesota Department of Health website, 2002. Available at: http://www.health.state.mn.us/divs/dpc/nedss/nedss.html (downloaded April 17, 2002).

Davis K, Schoenbaum SC, Collins KS, Tenney K, Hughes DL, Audet AJ. Room for Improvement: Patients report on the quality of their health care. The Commonwealth Fund, April 2002. Available at: http://www.cmwf.org/programs/quality/davis_improvement_534.pdf; last accessed May 22, 2002.

Department of Defense (DOD). *Military Health System Patient Safety Registry (MHSPSR). Armed* Forces Institute of Pathology (AFIP), undated. Available at: http://www.afip.org/PSC/index.html (last viewed March 1, 2002).

Department of Health and Human Services (DHHS). 45 CFR Parts 160 and 164 Office of the Secretary; Standards for Privacy of Individually Identifiable Health Information; Proposed Rule. Federal Register, 67(59), March 27, 2002.

Department of Health and Human Services (DHHS). DHHS Policy for the Protection of Human Research Subjects "The Common Rule".." *Title 45 Code of Federal Regulations* Part 46. 1991.

Department of Health and Human Services, Office of Civil Rights (DHHS/OCR). Standards for Privacy of Individually Identifiable Health Information. *Frequently Asked Questions (FAQ) Sheet*, last revised July 6, 2001. Available at: http://aspe.hhs.gov/admnsimp/final/pvcguide1.htm (last viewed April 18, 2002).

Department of Health, United Kingdom (DOH/UK). "Building a Safer NHS for Patients: Implementing 'An Organization with a Memory'".." Slide Presentation. National Health Service, 2001b. Available at: http//www.npsa.org.uk/publications/publications.asp (downloaded February 18, 2002).

Department of Health, United Kingdom (DOH/UK). Building a Safer NHS for Patients: Implementing *"An Organization with a Memory – Report of an Expert Group on Learning from Adverse Events in the NHS."* National Health Service, 2001a. Available at: http://www.npsa.org.uk/ (downloaded February 26, 2002).

Department of Veterans Affairs and National Aeronautics and Space Administration (VA and NASA). *VA Patient Safety Reporting System (PSRS)*, undated. Available at: http://www.psrs.arc.nasa.gov/ (last viewed March 14, 2002).

Department of Veterans Affairs and National Aeronautics and Space Administration (VA and NASA). *Patient Safety Reporting System (PSRS) Report Form*, June 2001. Available at: http://www.psrs.arc.nasa.gov/web_docs/PSRS_Form.pdf/ (last viewed March 14, 2002).

Dixon JF, Wielgosz C, Pires ML. Description and outcomes of a custom web-based patient occurrence reporting system developed for Baylor University Medical Center and other system entities. *Baylor University Medical Center Proceedings* 15(2):199-202, April 2002. Available at: http://www.BaylorHealth.com/Proceedings.

ECRI. *About Medical Device Safety Reports (MDSR).* [Online fact sheet] Plymouth Meeting, PA: 2002a. Available at: http://www.ecri.org/about_MDSR/content.asp (downloaded March 13, 2002).

ECRI. ECRI's Problem Reporting Form. [Online form] Plymouth Meeting, PA: 2002b. (Available at: http://www.ecri.org/documents/Prob_Reporting/problemreportform.asp (downloaded March 13, 2002).

ECRI. *Health Devices Alerts Database*. [Online fact sheet] Plymouth Meeting, PA: 2002c. Available at: http://www.ecri.org/documents/448596.htm (downloaded March 13, 2002).

ECRI. *Medical Device Problem Reporting.* [Online fact sheet] Plymouth Meeting, PA: 2002d. Available at: http://www.mdsr.ecri.org/PRP/content.asp (downloaded on March 13, 2002).

ECRI. *Welcome to Medical Device Safety Reports (MDSR)*. [Online fact sheet] Plymouth Meeting, PA: 2002e. Available at: http://www.mdsr.ecri.org/search/content.asp (downloaded March 13, 2002).

Fischer G, et al. Adverse events in primary care identified from a risk-management database. Journal of Family Practice 45:40-46, 1997.

Flack M. Medical product surveillance network (MedSun) ready to launch first segment of the phase II pilot. *User Facility Reporting*. 36: 2001. Available at http://www.fda.gov/cdrh/fusenews/ufb36.html (downloaded April 11, 2002).

Flowers L. *State Response to the Problem of Medical Errors: An analysis of recent state legislative proposals*. Robert Wood Johnson Foundation, February 2002.

Food and Drug Administration Task Force (FDA TF). "Managing the Risk From Medical Product Use: Creating a Risk Management Framework." Rockville MD: U.S. Department of Health and Human Services, May, 1999.

Food and Drug Administration. *Adverse Events Reporting System: Overview PowerPoint Presentation*. FDA Center for Drug Evaluation and Research, January 2002.

Food and Drug Administration. *Alternative Summary Reporting System V. 1 User Guide*. FDA Center for Devices and Radiologic Health, 2000.

Food and Drug Administration. *Biologics compliance information system (BCIS) V.3 User Guide*. FDA Center for Biologics Evaluation and Research, January 2001.

Food and Drug Administration. *Guidance for industry: Biological product deviation reporting for blood and plasma establishments*. FDA Center for Biologics Evaluation and Research, January 2002.

Gardner S and Flack M. *Designing a Medical Device Surveillance Network: Report to Congress*. U.S. Department of Health and Human Services, Food and Drug Administration, September 1999.

Gardner S and Flack, M. *Designing a medical device surveillance network: Report to Congress*, 1999. Available at http://www.fda.gov/cdrh/postsurv/medsun.html (downloaded April 11, 2002).

Gaynes RP. Surgical-site infections (SSI) and the NNIS Basic SSI Risk Index, part II: room for improvement. *Infection control and hospital epidemiology*. 22(5):266-267, 2001 (downloaded April 17, 2002).

General Accounting Office (GAO). Medical Records Privacy: Access Needed for Health Research, but Oversight of Privacy Protection Is Limited. *GAO/HEHS*-99-55, February 24, 1999.

Hammond WE. Personal Communication, June 4, 2002

Health Care Financing Administration (HCFA, now Centers for Medicare and Medicaid (CMS)). Nuts and Bolts: Electronic Claim Attachments. Prepared for HCFA HIPAA Medicaid Conference, April 24-26, 2001. Available at: http://www.hcfa.gov/medicaid/hipaa/adminsim/0401conf/3-6sanchez.rtf (downloaded April 5, 2002).

Health Care Financing and Organization (HCFO). HIPAA Privacy Regulations: Researchers Prepare for New Rules. News and Progress, Funded by the Robert Wood Johnson Foundation (RWJF) in collaboration with the Academy for Health Services Research and Health Policy. Washington DC: RWJF, March 2002

Health Level 7 (HL7). *Reference Information Model Version 1.15 (RIM Billboard)*. Prepared for Harmonization and currently under review. HL7: March 7, 2002.

Heinrich HW. Industrial accident prevention: A scientific approach. New York, McGraw-Hill, 1941.

Held PJ, Wolfe RA, Gaylin DS, Port FK, Levin NW, Turenne MN. Analysis of the association of dialyzer reuse practices and patient outcomes. *American Journal of Kidney Diseases* 23(5):692-708, May 1994.

HIPAA. *National Electronic Data Interchange Transaction Set Implementation Guide, Health Care Eligibility Benefit Inquiry and Response, 270/271*, May 2000a. Available at: http://www.wpc-edi.com/hipaa/HIPAA_40.asp (downloaded January 28, 2002).

HIPAA. *National Electronic Data Interchange Transaction Set Implementation Guide, Benefit Enrollment and Maintenance, 834*, May 2000b. Available at: http://www.wpc-edi.com/hipaa/HIPAA_40.asp (downloaded January 28, 2002).

Horan TC, Emori TG. Definitions of key terms used in the NNIS System. *American Journal of Infection Control*. 25(2):112-116, 1997.

Information Management Consultants. *Medical Event Reporting System for Transfusion Medicine (MERS-TM)/Electronic Biological Product Deviations Reporting System (BIODEV) interface feasibility study*. November 2001.

Institute for Safe Medication Practices (ISMP Canada). *Analyze-Err (Fact Sheet).* ISMP-Canada, 2002a. (Available at: http://encrypt7.name-serve.net/ismp-canada/analyze-err.htm (Downloaded on March 11, 2002a).

Institute for Safe Medication Practices (ISMP Canada). *Analyze-Err Medication Error Report Form*. ISMP-Canada, 2002b. Available at: http://encrypt7.name-serve.net/ismp-canada/smederr.htm (Downloaded on March 11, 2002b).

Institute of Medicine (IOM): Kohn LT, Corrigan JM, Donaldson MS (eds). *To Err is Human: Building a Safer Health System.* Washington DC: Institute of Medicine, National Academy Press, 1999.

Institute of Medicine. Guidance for Development of Patient Safety Data Standards, April 15, 2002. Available at: http://www.iom.edu/IOM/IOMHome.nsf/Pages/Patient+Safety+Data+Standards (last viewed April 16, 2002).

Iskander, J. K., Miller, E. R., Pless, R. P., and Chen, R. T. Vaccine safety post-marketing surveillance: The vaccine adverse event reporting system. CDC website, February 2002. Available at: http://www.cdc.gov/nip/vacsafe/VAERS/CME-post-mktg-surv.pdf (downloaded April 11, 2002).

Jaynes, A. and Lyle, J. NEDSS and NEDSS. CDC website, 2002. Available at: http://www.cdc.gov/nedss/BaseSystem/NEDSSBusinessDiscoveryStatement1_2.pdf (downloaded April 17, 2002).

Joint Commission on Accreditation of Healthcare Organizations (JCAHO). *Revisions to Joint Commission Standards in Support of Patient Safety and Medical/Health Care Error Reduction*, July 1, 2001. Available at: http://www.jcaho.org/standard/ptsafety_mpfrm.html (last viewed April 22, 2002).

Joint Commission on Accreditation of Healthcare Organizations (JCAHO). *Sentinel Event Policy and Procedures.* (Online Manual) JCAHO, 2002. Available at: http://www.jcaho.org/sentinel/se_pp.html) (Downloaded March 5, 2002).

Joint Commission on Accreditation of Healthcare Organizations (JCAHO). *Sentinel Event Policy and Procedures.* Online Manual, 2002a. Available at: http://www.jcaho.org/sentinel/se_pp.html) (Downloaded March 5, 2002).

Joint Commission on Accreditation of Healthcare Organizations (JCAHO). Joint Commission Commends Patient Safety And Quality Improvement Act. Press Release, June 7, 2002b.

Kaplan HS. *Medical Event Reporting System for Transfusion Medicine (MERS-TM) Reference Manual Version 3*. Prepared by Westat for Columbia University, under NHLBI grant RO1 HL53772. New York: Columbia University, 2001. Available at: http://www.mers-tm.net/support/MERS_TM_Ref_Manual.pdf (last viewed April 16, 2002).

Kaplan, H. S. *Medical Event Reporting System for Transfusion Medicine (MERS-TM) Reference Manual Version 3.0.* MERS-TM website, 2002. Available at: http://www.mers-tm.net/support/MERS_TM_Ref_Manual.pdf (downloaded April 11, 2002).

Khuri, SF (PI). "Reporting system to improve patient safety in surgery." AHRQ Grant HS11913-01. West Roxbury, MA: VA Boston Healthcare System, April 26, 2001

Kohn LT, Corrigan JM, Donaldson MS (eds). *To Err is Human: Building a Safer Health System.* Washington DC: Institute of Medicine, National Academy Press, 1999.

Leape LL, Bates DW, Cullen DJ. Systems analysis of adverse drug events. *Journal of the American Medical Association* 274:35-43, 1995.

Leape LL, Brennan TA, Laird N, Lawthers AG, Localio AR, Barnes BA, et al. The nature of adverse events in hospitalized patients: Results of the Harvard Medical Practice Study II. *New England Journal of Medicine* 324(6):377-384, 1991.

Leape LL. Error in medicine. *Journal of the American Medical Association* 272(23):1851-57, 1994.

Liang BA, Storti K. Creating Problems as Part of the "Solution": The JCAHO Sentinel Event Policy, Legal Issues, and Patient Safety. *Journal of Health Law* 33:263-285, 2000.

Liang BA. Error in Medicine: Legal Impediments to U.S. Reform. *Journal of Health Politics, Policy, and Law* 24:27-58, 1999.

Liang BA. Other People's Money: A Reply to the Joint Commission. *Journal of Health Law* 33:657-64, 2000a.

Liang BA. Personal communication, May 14, 2002.

Liang BA. Risks of Reporting Sentinel Events. *Health Affairs* 19(5):112-120, 2000b.

Liang BA. The Adverse Event of Unaddressed Medical Error: Filling the Holes in the Legal and Health-Care Systems. *Journal of Law and Medical Ethics* 29(3/4):346-368, 2001.

Lowe, M. A. and Scott, W. L. *Medical device reporting for user facilities*. FDA Center for Devices and Radiologic Health website, 1996. Available at: http://www.fda.gov/cdrh/devadvice/351.html (downloaded April 11, 2002).

Malpass A, Help SC, Sexton EJ, Maiale D, Runciman WB. A classification for adverse drug events. *Journal of Quality in Clinical Practice,* 19:23-26, 1999.

Marchione M. One of tainted-tissue recipients from Wisconsin. *Milwaukee Journal Sentinel, March 15, 2002.*

Marx, D and Kaplan, H. S. *Patient safety and the "Just Culture": A primer for health care executives*. MERS-TM website, 2002. Available at: http://www.mers-tm.net/support/Marx_Primer.pdf (downloaded April 11, 2002).

Medicomp Systems, Inc (Medicomp). MEDCIN: Nomenclature Properties. Available at: http://www.medicomp.com/nomen.htm (last viewed, June 10, 2002)

Merewitz SG. Confidentiality Certificate for AHCPR Grantee. USDHHS Memorandum to J.P. Fanning, January 30, 1995.

Minnesota Department of Health. *Minnesota's National Electronic Disease Surveillance System (NEDSS) Project*. Minnesota Department of Health website, 2002. Available at: http://www.health.state.mn.us/divs/dpc/nedss/nedss.html (downloaded April 17, 2002).

National Aeronautics and Space Administration and Federal Aviation Administration (NASA and FAA). *Aviation Safety Reporting System Program Overview*, 1999. Available at: http://asrs.arc.nasa.gov/overview_nf.htm (Downloaded April 3, 2002).

National Center for Patient Safety (NCPS). *Patient Safety Program*. Ann Arbor, MI: Veterans Affairs, undated(a). Available at: http://www.patientsafety.gov (downloaded, April 15, 2002).

National Center for Patient Safety (NCPS). *Safety Assessment Code (SAC) Matrix*. Ann Arbor, MI: Veteran's Affairs, undated(b). Available at: http://www.va.gov/ncps/matrix.html. (Downloaded, April 9, 2002).

National Committee on Vital and Health Statistics (NCVHS). Information for Health: A Strategy for Building the National Health Information Infrastructure. Washington DC: U.S. Department of Health and Human Services, November 15, 2001.

National Committee on Vital and Health Statistics (NCVHS). Uniform Data Standards for Patient Medical Record Information. Washington DC: U.S. Department of Health and Human Services, July 6, 2000.

National Coordinating Council for Medication Error Reporting and Prevention (NCCMERP). *NCC MERP Taxonomy of Medication Errors*, 1998. Available at: http://www.nccmerp.org (see "About medication errors" and "Taxonomy") (last viewed April 11, 2002).

National Library of Medicine. *Unified Medical Language System (UMLS) Knowledge Sources, 13 edition*. U.S. Department of Health and Human Services, National Institutes of Health, January 2002.

National Nosocomial Infections Surveillance (NNIS) report, data summary from October 1986-April 1996, issued May 1996. A report from the National Nosocomial Infections Surveillance (NNIS) System. *American Journal of Infection Control*. 24(5):380-388, 1996.

National Nosocomial Infections Surveillance (NNIS). *Semiannual report, Data summary from October 1986-April 1998*. Department of Health and Human Services. 1-25. 1998.

National Quality Forum. Serious Reportable Events in Healthcare: A Consensus Report. Washington DC: National Forum for Healthcare Quality Measurement and Reporting, 2002. Available for order at: <http://www.qualityforum.org/neverteaser.pdf> (accessed May 23, 2002).

Newcomb, Carol. *Project Manager for Patient Safety, University HealthSystem Consortium.* Email correspondence (April 9, 2002).

Newcomer LN. Medicare pharmacy coverage: Ensuring safety before funding. *Health Affairs* 19(2):59-62, March/April 2000.

O'Callaghan, S. Biological Product Deviation Reports: What have we learned? PowerPoint Presentation. FDA Center for Biologics Evaluation and Research, January 2002.

Oregon Department of Human Services. *Oregon Public Health Service National Electronic Disease Surveillance System: About the Project*. Oregon Department of Health website, 2002. Available at: http://www.ohd.hr.state.or.us/nedss.about.htm (downloaded April 17, 2002).

Osborn S. Chief, National Patient Safety Agency. Personal Communication, February 7, 2002.

Pezzino, G. *A guide to the implementation of the National Electronic Disease Surveillance System (NEDSS) in State public health agencies.* Oregon Department of Health website. April 2001. Available at: http://www.ohd.hr.state.or.us/nedss/docs/cste-nedss-guide.pdf (downloaded April 17, 2002).

Pickett, D. Personal communication. ICD coding modifications, April 8, 2002.

Popovich, M. Communicable disease surveillance systems - Approach for developing a State-level national electronic disease surveillance system (NEDSS) strategic technology plan. CDC website, 2000. Available at: http://www.stchome.com (downloaded April 17, 2002).

Pritts J, Goldman J, Hudson Z, Berenson A, and Hadley E. The State of Health Privacy: An Uneven Terrain, *A Comprehensive Survey of State Health Privacy Statutes.* Washington DC: Georgetown University, Institute for Health Care Research and Policy, August 1999.

Quality Interagency Task Force (QuIC). Doing What Counts for Patient's Safety: Federal Actions to Reduce Medical Errors. Washington DC: U.S. Department of Health and Human Services, 2000.

Reason JT. *Human Error*. Cambridge MA: Cambridge University Press, 1990.

Reichard J. How the Senate and House Error Reduction Bills Differ. Online: Washington HealthBeat, June 7, 2002. (For information inquire at: HealthBeat.@Starpower.net).

Reichard J. Johnson Introduces Medical Error Bill. Online: Washington HealthBeat, June 7, 2002. (For information inquire at: HealthBeat.@Starpower.net).

Reichard J. New Hope for Legislation to Reduce Medical Errors. Online: Washington HealthBeat, June 5, 2002. (For information inquire at: HealthBeat.@Starpower.net).

Revelle PW. Personal communication. MedDRA MSSO, March 21, 2002. Some information is available at http://www.meddramsso.com.

Richards C, Emori TG, Edwards J, Fridkin S, Tolson J, Gaynes R. Characteristics of hospitals and infection control professionals participating in the National Nosocomial Infections Surveillance System 1999. *American Journal of Infection Control*. 29(6):400-403, 2001.

Rosenthal J, Booth M, Flowers L, Riley T. Current State Programs Addressing Medical Errors: An Analysis of Mandatory Reporting and Other Initiatives. Portland, ME: National Academy for State Health Policy, January 2001.

Schoeffler K. Duke University Medical Informatics, Sixth-Year Student. Personal Communication, April 12, 2002.

Sexton JB, Thomas EJ, Helmreich RL. Error, stress, and teamwork in medicine and aviation: Cross sectional surveys. *British Medical Journal* 320:745-749, 2000.

Singleton JA, Lloyd JC, Mootrey GT, Salive ME, Chen RT. An overview of the vaccine adverse event reporting system (VAERS) as a surveillance system. VAERS Working Group. *Vaccine.* 17(22):2908-2917, 1999.

SNOMED International. *SNOMED® Clinical Terms™ Technical Specification, Version 23 (2001-12-12).* Available at: http://www.snomed.org (downloaded March 27, 2002a).

SNOMED International. *SNOMED® Clinical Terms™ Consultation Document, Draft Version 23 (2001-10-12).* Available at: http://www.snomed.org (downloaded March 27, 2002b).

Stationery Office (SO). An Organization with a Memory: A Report of an Expert Group on Learning from Adverse Events in the NHS. London: The Stationery Office, 2000.

Thomas EJ, Studdert DM, Burstin HR, et al. Incidence and Types of Adverse Events and Negligent Care in Utah and Colorado. *Medical Care,* Spring 2000.

Thomas EJ, Studdert DM, Newhouse JP, et al. Cost of medical injuries in Utah and Colorado. *Inquiry,* 36:255-264, 1999.

TRW, Inc. "*Medical Dictionary for Regulatory Activities: MedDRA™ Introductory Guide," Version 4.0,* June 2001.

United States Pharmacopeia (USP). *Medication Errors Reporting (MER) Program. Undated(b).* Available at: http://www.usp.org (last viewed April 14, 2002).

United States Pharmacopeia (USP). *MedMARx: A National Database to Reduce Hospital Medication Errors.* Undated(a). Available at: http://www.usp.org (last viewed April 14, 2002).

United States Pharmacopeia (USP). Summary of 1999 Information Submitted to MedMARx^{SM}*: The National Database to Reduce Hospital Medication Errors. Rockville, MD: USP, 2000.* Available at: http://www.usp.org (last viewed April 14, 2002).

University HealthSystem Consortium (UHC). *The UHC Patient Safety Net. Presentation*. Oak Brook, IL: UHC, October 4, 2000.

University HealthSystem Consortium (UHC). *UHC Patient Safety Network.* Online demonstration courtesy of UHC. April 1, 2002.

Varricchio F. The vaccine adverse event reporting system. *Journal of toxicology. Clinical toxicology.* 36(7):765-768, 1998.

Wasserstrom D. Vice President, Healthcare IT Sales, Language and Computing Consultants, Inc. Personal and email communication, April 11, 2002.

Weber DO. One giant leapfrog for health care. *Physician Executive*, 27(6):6-12, November-December, 2000.

Wilson RM, Runciman WB, Gibberd RW, Harrison BT, Newby L, Hamilton JD. The Quality in Australian Health Care Study. *The Medical Journal of Australia*. 163(9):458-71, 1995.