# COMMUNITY IMMUNIZATION REGISTRIES MANUAL

## CHAPTER III: TECHNOLOGY*

**Prepared by**

**All Kids Count Program of The Task Force for Child Survival and Development**

**The National Immunization Program of the Centers for Disease Control and Prevention**

June 19, 1997

**CONTENTS**

---

* Principal contributors: Joseph Henderson, Immunization Program, New York Department of Health; Ernie Hernendez, CNE, Nevada Department of Health; and Chris Mickens, Indiana State Department of Health.

# INTRODUCTION TO CHAPTER III

Understanding the technological issues early in the registry planning process may help set goals and objectives that are both realistic and achievable. This chapter should be reviewed before firm decisions are made about the vision and objectives of the registry. Designing technological approaches for the registry will require many choices to be made. Some of the issues bearing upon your decisions are listed here:

- The cost of equipment and its support
- The availability of appropriate software from commercial vendors/developers
- Applicability, versatility, sophistication, and elegance of application software
- Software development time and expense
- Efforts required to establish and maintain telecommunications interfaces with users
- Ensuring adequate security systems and procedures

No single solution will be appropriate for all communities. Registries will need to be "tailored" to fit the environment in which they operate. Different recent approaches, experiences, and lessons learned by others should be carefully examined and built upon. The purpose of this chapter is to make those planning a registry aware of the technological issues, policies, and decisions which must be made prior to a registry's startup. Where compatibility between different registries is essential, specific recommendations have been made concerning data sets and record exchange procedures.

Information is presented about six topics, each of which must be addressed. The order in which they are undertaken may vary depending upon individual circumstances. The process should be considered a dynamic and fluid one. All the topics are closely related and decisions made in one area probably will impact others. Earlier steps may need reevaluation based upon newly gained information from a later step. The scope of the project itself may need to be reviewed as more understanding is obtained about various technological implications.

A significant problem to be addressed is ensuring reliable electronic interfaces for private providers and other participants enabling them to input data into the registry data base and access data from it. The importance of this issue is demonstrated by the fact that many providers may be unwilling to "double enter" immunization data into their own office systems as well as a registry. They will tend to expect the connection with the registry to be

automatic and sufficient, requiring no further action on their part.

Meeting these goals will be a formidable challenge. A solid, cooperative working relationship between the registry developer and vendors of patient management and billing systems is essential. For the long-range effectiveness of the registry, such a relationship needs to be energetically pursued by the registry developer. Recent developments in standardization of data sets and specifications for record exchanges (Health Level 7) are expected to facilitate this cooperation. To further foster a cooperative spirit, registry planners should explain to vendors that their efforts to meet the needs of one state or community will be relevant to the needs in other locations, potentially expanding their revenues.

The intent of this chapter is to facilitate a future when: 1) providers who give immunizations can expect the software they install in their offices to interface directly with community immunization registries; and 2) registries will incorporate standardized record exchange features. Until that time, individual solutions are necessary within each state or community to accommodate existing systems in the best possible ways. This is often a complex and difficult task. It becomes essential that there be continuing discussions between those who will be involved in using the software and those who are establishing and supporting the data communications linkages. The following general principles may be helpful:

- Identify early the essential functions to be performed, find solutions, and prove them prior to registry start-up.

- Evaluate nonessential functions and consider whether they are worth their short- and long-term costs, both direct and indirect.

- Pay close attention to the kinds of access the users state they need and/or desire.

- Establish and carefully review security and confidentiality policies when considering each design question.

- Design systems to be flexible for several years in a rapidly changing technological environment and to be responsive to the dynamic needs of immunization programs.

# 1: DEFINING THE APPLICATION FUNCTIONS

Before technical approaches are developed for operating a registry, a team consisting of a systems analyst and key immunization program staff should be assembled. Their goal is to define the specific tasks the registry will perform for its users. These tasks should enable the operational registry to meet the objectives defined by the governing body. Additionally, a mutual understanding of the program requirements and the technical capabilities will preclude numerous later problems. As the defining task proceeds, representatives of user groups should be included in the discussions as early as possible. Their input will be necessary to identify or clarify issues needing resolution prior to becoming operational. This approach will reduce misunderstandings leading to costly software or hardware changes made after considerable technical development is invested.

Table III-1, on the following page, lists functions that either will be **required** or are **recommended** to ensure that the registry can perform essential tasks. Data sets needed to perform these applications are discussed in the next section. An example of a recommended function is **vaccine inventory management**. Many providers would benefit from having a vaccine inventory management and automatic re-ordering system built into a registry they use. This capability enhances the attractiveness of the registry and represents another incentive for the provider to become involved. However, the complexity of the required programming for this service may mean that many registries will choose not to provide this service.

Registries opting for vaccine inventory management capability will find the following features desirable:

- **o** A dynamic table-driven ability to add new types of vaccines to the system.

- **o** The ability to control the following inventory actions through user-set parameters:

  - Reorder levels, specific to provider facility and vaccine.

  - Short-dated notices, specific to provider facility and vaccine.

  - Reallocation notices, specific to provider facility and vaccine. These will be cued by stock rising over a set level or passing its expiration date within a set period of time.

- **o** Tabulation of doses administered by patient classification groupings, defined by the Vaccines for Children Program, specific to provider facility and vaccine.

- The ability to generate recall lists of individuals who have received vaccinations of a specified type or lot, in the event of a vaccine recall. While not specifically an inventory function, it may be accomplished by scanning the patient immunization database.

**Table III-1: Application functions for registries, according to type**

| **Client Record Management Functions** | |
|---|---|
| **REQUIRED** | **RECOMMENDED** |
| **o** Identify client and client record.<br>**o** Create, delete, modify or update client records. | **o** Associate client record with family records.<br>**o** Prompt physician/nurse about client needs.<br>**o** Record client health care plan/payer.<br>**o** Record program eligibility for vaccine.<br>**o** Designate/update medical home of client.<br>**o** Request and receive birth notice or client record.<br>**o** Vaccine inventory management. |
| **Client Immunization Management Functions** | |
| **REQUIRED** | **RECOMMENDED** |
| **o** Create, delete, modify or update immunization history records.<br>**o** Retrieve immunization history records.<br>**o** Maintain an immunization schedule.<br>**o** Evaluate client immunization status. | **o** Record adverse reaction, contraindications, and exemptions.<br><br>***Note:*** *Storing adverse reaction and/or contraindication information on a child could involve storing disease history information on the child. This would affect the security/confidentiality requirements for the system.* |

**TABLE III-1 (continued)**

| **Client Scheduling, Follow-up and Outreach Functions** | |
|---|---|
| **REQUIRED** | **RECOMMENDED** |
| **o** Issue reminders/recalls to clients.<br>**o** Import and export immunization records to other data systems. | **o** Schedule client visits.<br>**o** Refer to other "special" immunization services.<br>**o** Refer to public services such as the Special Supplemental Feeding Program for Women, Infants, and Children (WIC). |

| **Assessment and Evaluation Functions** | |
|---|---|
| **REQUIRED** | **RECOMMENDED** |
| **o** Assess immunization levels. Some of the assessment information should be the same as that produced by the Clinic Assessment Software Application (CASA) developed and distributed by CDC. | **o** Update on-line immunization reference information.<br>**o** Produce legally recognized immunization records for those entities required by law to check individual histories such as schools and day-care centers. |

| **Standard Data System Functions** | |
|---|---|
| **REQUIRED** | **RECOMMENDED** |
| **o** Backup software and data to some media other than disk.<br>**o** Archive data that is no longer needed routinely to some other file and/or media.<br>**o** Create, delete, modify or update security information on users of the system. | |

# 2: DATA DESIGN

When agreement has been reached on the application functions that are required for the registry, the data elements which need to be collected should be identified. Some general guidelines about data collection include:

**Request only data that are needed.** Requesting data that are not essential decreases confidentiality, slows data entry, overburdens the system, and makes it difficult to manage. All data in the registry should be kept accurate and current. Asking users to enter data "because they might be useful" will add to their workload and decrease time available to ensure the quality of essential data.

**Insist on systems requiring only essential data to operate.** Programs that constantly force users to complete fields with unnecessary data in order to continue the application may tempt users to enter inaccurate information. It is preferable for the program to allow a blank or code meaning “unknown” than to increase the risk of entering incorrect information. However, some data may be useful in performing nonessential registry functions.

**Opt for systems which validate data during data entry to reduce mistakes.** Data fields should include edit checks to reduce the entry of false information. For example, dates for immunizations can be cross-checked by the computer to ensure they are equal to, or later than the child’s birth date, and not later than the current date. Data combinations can be validated, such as ensuring that a zip code is valid for a particular state.

**Use table-driven instead of hard-coded values**. Database software using tables to store codes for commonly needed data elements (e.g. for counties) and for immunization schedules will require the fewest programming changes. Permanent computer codes (hard-coding) demand many more updates for the same information. Thus, table-driven database software is less expensive to maintain and operate. However, initially they are more expensive to produce and require more training for the system administration staff to update. For example, if immunization schedules are stored as tables and new vaccines are made available, the system administration staff must know what information to put in the tables, and how and when to do it. Table changes would then take effect immediately. If the schedule is hard coded, schedule information would be passed along to a programming staff to update the system. This change could take a significant amount of time and money to implement. It is projected that the kinds and availability of vaccines will change several times in the next few years. These changes will impose recurring costs and delays for systems not

using tables to define at least those data elements.

**Balance security with ease of access**. Protecting the security of a system against unauthorized access and tampering requires restrictions and controls on data access. However, these same safeguards complicate use by authorized users. Specifying which data elements are restricted and not displayed to all users permits nonrestricted data to be viewed without encountering annoying security features. For example, displaying children's names and birth dates without indicating where vaccines were given, where the child lives, or any prior name will protect the privacy of the parent wishing to avoid an abusive spouse. The user still retains the ability to evaluate any immunization needs. The basic concept is one of restricting access to anyone who does not have a **right** and a **need** to know. In designing data sets, security considerations should be included from the outset. Strive for a realistic working balance between permitting use by authorized personnel and preventing access by those not authorized.

**Balance input/output options with cost**. Adding optional applications will require the collection of more data and higher development costs. Immunization histories may be supplied in a variety of ways, such as electronic data files, printed reports in the provider's office, FAX, mailed reports, and on-line computer screens. Development costs increase with each additional method implemented. Some of the options may cost more to develop, such as FAX, but may be less expensive per individual history delivered than print, if the print history has to be mailed.

Regardless of the technical design, consistent core data elements need to be gathered to ensure information is shared as clients move between providers or registries. A recommended core data set that has been approved by the National Vaccine Advisory Committee (NVAC), and issued by CDC, is attached to this document as Appendix III-3. This has been widely distributed. The highlighted elements represent a minimum core of data to be collected by registries. Additional data elements may be desirable to permit the registry to perform its functions. Examples of some additional data elements are described in the following tables.

## DATA TABLES

Tables III-2 and III-3 were compiled by the staffs of several experienced, functioning community registries and list data elements they considered to be useful. These data not only capture and store information, but allow providers to share immunization records of their clients. The data are grouped into two tables which define the client and the client's immunizations. Each data element is identified, described, and given a Security Code of

**High** sensitivity, **Moderate** sensitivity, or **Low** sensitivity. Additionally, a Use Code is provided, describing whether those who compiled the tables considered the particular data as **(M)inimal** data, **(R)ecommended** data, or **(O)ptional** . The greater the sensitivity of the data the more restricted access will be. In most cases highly sensitive data would not be shared with registry users, but would be reserved for access only by senior registry staff. Minimal data are those which were considered necessary for the most basic immunization information system. Systems that capture recommended and optional data will afford greater versatility for users. But they will require more data entry time and will be more difficult and costly to establish and maintain. Additional comments about data elements are included in the HL7 specifications for immunization record exchange.

## Table III-2: Data elements which define the client

| Field Name | Description | Security Code | Use Code |
|---|---|---|---|
| Patient ID | Unique identifier determined by user. | Low | M |
| Pt. First Name | Child's First Name | High | M |
| Pt. Mid. Name | Child's Middle Name | Low | M |
| Pt. Last Name | Child's Last Name | High | M |
| A.K.A. First Name | Also Known As - First Name | High | R |
| AKA Last Name | Also Known As - Last Name | High | R |
| Date of Birth | Date of Birth | Mod | M |
| Birth File Number | State Birth Certificate Number | High | R |
| Birth Order | Birth Order | Low | O |
| Birth Facility | Birth Facility | Mod | R |
| Birth County | County Table | Mod | R |
| Birth State | State Table | Mod | R |
| Birth Country | Country Table | Mod | R |
| Social Security Number | Child's Social Security Number | High | R |
| Medicaid Number | Child's Medicaid Number | High | R |
| Gender/Sex | Child's - Male/Female Indicator | Low | R |

| Field Name | Description | Security Code | Use Code |
|---|---|---|---|
| Race | Child's Race | Low | R |
| Ethnicity | Child's Ethnicity | Low | R |
| Primary Language | Child's Primary Language | Low | R |
| Secondary Language | Child's Secondary Language | Low | R |
| Deceased Indicator | Child Deceased Indicator (Y/N) | Low | R |
| Deceased Date | Date Child Deceased | Low | R |
| Residence Street Address Primary | Child's Primary Street Address | High | M |
| Residence Street Address Secondary | Child's Secondary Street Address | High | M |
| Residence City | Child's City of Residence | High | M |
| Residence State | Child's State of Residence | High | M |
| Residence Zip | Child's Residence Zip code | High | M |
| Census Tract | U.S. Census Tract Delineation | High | R |
| Phone Number Primary | Child's Primary Phone Number | High | R |
| Phone Number Secondary | Child's Secondary Phone Number | High | R |
| Mother's First Name | Mother's First Name | High | M |
| Mother's Middle Name | Mother's Middle Name | High | R |
| Mother's Last Name | Mother's Last Name | High | M |
| Mother's Maiden Name | Mother's Maiden Name | High | M |
| Mother's DOB | Mother's Date of Birth | High | M |
| Mother's SSN | Mother's Social Security Number | High | R |
| Father's First Name | Father's First Name | High | R |

| Field Name | Description | Security Code | Use Code |
|---|---|---|---|
| Father's Middle Name | Father's Middle Name | High | O |
| Father's Last Name | Father's Last Name | High | R |
| Father's DOB | Father's Date of Birth | High | O |
| Father's SSN | Father's Social Security Number | High | O |
| Guardian First Name | Guardian First Name | High | R |
| Guardian Last Name | Guardian Last Name | High | R |
| Consent Flag | To be used to indicate consent for accination has been provided | Low | O |
| Health Plan ID | Health Plan ID Look-up Table | Mod | M |
| Primary Provider ID | Unique Provider ID determined by User | Mod | M |
| Last Vaccination Date | Date child last vaccinated | Low | R |
| VAERS Report Flag | Flag indicating that a vaccine adverse event has been reported to the Vaccine Adverse Event Reporting System (VAERS) | Mod | O |
| Record Active/Inactive Flag | Flag indicating whether the record is active or inactive | Low | M |

## Table III-3: Data elements that define the client's immunization

| Field Name | Description | Security Code | Use Code |
|---|---|---|---|
| Vaccine Type | Code from Vaccine Look Up Table | Low | M |
| Vaccine Dose Number | Dose number for multiple dose series | Low | R |
| Vaccination Date | Date vaccine was administered | Low | M |
| Vaccine Manufac. | Name of vaccine manufacturer | Low | R |
| Vaccine Lot Number | Vaccine Lot Number | Low | R |
| Vaccinator ID | User proscribed identifier (could be State License Number) | Low | M |
| VIS Date | Date from Vaccine Information Materials (indicates materials provided to parent/guardian) | Low | O |
| Source of Data | User determined. Indicates how the information was obtained (e.g., from primary care provider, other provider, child's immunization history/record) | Low | M |
| Vaccine Contra. Indicator | Indicates a child has a valid contraindication to a vaccine | High | R |
| Vaccine Contra. Indicator Descrip. | Describes the valid contraindication to a vaccine | High | R |
| Inject. Site | Look up table that indicates route of vaccination | Low | R |
| Vaccinator Facility ID** | Determined by user to identify facilities where a child receives an immunization | Low | R |
| Vaccinator Facility Name | Name of Facility | Low | R |

** Information about the facilities might be provided in a look-up table.

| Field Name | Description | Security Code | Use Code |
|---|---|---|---|
| Vaccinator Facility Address Line 1 | Facility Address Line 1 | Low | R |
| Vaccinator Facility Address Line 2 | Facility Address Line 2 | Low | R |
| Facility City | Facility City | Low | R |
| Facility State | State Look Up Table | Low | R |
| Facility Zip Code | Facility Zip Code | Low | R |
| Facility Zip Code Extension | Facility Zip Code Extension | Low | R |
| Facility Phone Number | Facility Phone Number | Low | R |
| Facility Fax Number | Facility Fax Number | Low | R |
| Vaccinator Provider ID*** | Determined by user to identify providers where a child receives an immunization | Low | R |
| Vaccinator Provider Name | Name of Provider | Low | R |
| Vaccinator Provider Address Line 1 | Provider Address Line 1 | Low | R |
| Vaccinator Provider Address Line 2 | Provider Address Line 2 | Low | R |
| Provider City | Provider City | Low | R |
| Provider State | State Look Up Table | Low | R |
| Provider Zip Code | Provider Zip Code | Low | R |

***

Information about providers might be provided in a table, either together with information on the facilities, or separately if appropriate (when the same provider works in different facilities). One solution to this type of situation might be using a composite provider ID number which combines the facility ID and the "personal" ID of the provider.

| Field Name | Description | Security Code | Use Code |
|---|---|---|---|
| Provider Zip Code Extension | Provider Zip Code Extension | Low | R |
| Provider Phone Number | Provider Phone Number | Low | R |
| Provider Fax Number | Provider Fax Number | Low | R |
| Vaccines For Children Eligibility | Child's VFC Eligibility Status from Look Up Table | Low | R |
| Vaccine Exemption | Indicates that a child has a valid medical or claims a religious exemption | Low | R |

A number of fields also will be required to monitor access and logging. Each access to records should be logged to ensure that transactions take place and that data is effectively maintained and safeguarded. Use of the above elements will promote similar data structures between registries and facilitate communication with each other.

## LOOK-UP TABLES

These tables, previously identified in some of the fields listed, permit selection from a menu of frequently entered information. They consist of a code and a description.

**TABLE III-4: Suggested Look-up Tables for Immunization Registry Databases**

| Table | Description | Comments |
|---|---|---|
| Injection Site | Place on the body where immunization would be administered | Example: R. Arm |
| Country | Country in the World | Example: USA |
| County | County in a State | Example: Fulton |
| Ethnicity | Ethnic Background | As defined by NCHS |
| Facilities | Identifies locations where immunizations are given, with address, phone number, Fax number etc. | May incorporate information on providers at the facility |
| Gender | Self-explanatory | Example: Female |
| Health Plan | Managed Care or other Health Plan | Example: US Health Care |
| Language | Identifies primary/secondary language the patient/family speaks | Example: English |
| Provider | Identifies providers by name, address etc. | May be combined with Table of facilities |
| Vaccine Type | Antigens used to immunize | Example: DTP (should use HL7 codes) |
| Vaccine Manufacturer | List vaccine manufacturers | Example: Lederle (should use HL7 codes) |
| Race | Self-explanatory | As defined by NCHS |
| Vaccines For Children Status | Code used to assist in assuring VFC eligibility is captured | Example: Code 1 = Medicaid Eligible |

# 3: SELECTING THE IMMUNIZATION REGISTRY

# SYSTEM ARCHITECTURE

The architecture of an immunization registry system may be defined as the physical structure of the information system. System architecture pertains to computers, telecommunications equipment (e.g., modems), database structure, and security devices. The system architecture chosen needs to be tailored to the specific goals of the registry as impacted by funding and existing technologies. Several standard software packages are available on the market or in the public domain. These programs are capable of providing the fundamental database and applications required by any immunization registry. The questions of how to collect data and provide users electronic access are often the most difficult to overcome and occur uniformly in designing registry systems. It is important that the trade-offs required be understood and accepted by program officials, partners, and users before actual development and implementation begins.

## USING EXISTING DATA SYSTEMS

It is likely that much of the information required by a registry is already being collected by existing provider or governmental information systems. If the legal restrictions based on privacy and confidentiality can be overcome, and technical problems resolved, state governments may be viable sources of data. It may be possible to electronically batch transfer data directly from computer-based birth certificate records, Medicaid billing records, and WIC patient records. Obtaining this data will help populate the registry data base with the identities of newborn infants, and identify those enrolled in Medicaid or WIC, who are among those most at risk of being under-immunized. The best data on immunizations will come from the records of private providers and public health clinics. Existing computer data bases with this information include patient management systems and electronic billing systems. Such systems may be operated by hospitals, managed care organizations, or individual practices.

The ultimate architectural objective is to have an electronic interface between the registry and patient management or billing systems used by providers. Achieving this degree of systems integration is a long-term task. It will be facilitated by extensive incorporation of one or two standard systems for exchanging immunization records. In the interim, it may be sufficient to request periodic batch transfers of data from existing systems to the registry. As with the large data bases discussed above, specific programming will be required to accomplish this. This programming should include applications for 1) collecting data from medical records, 2) putting it in the format necessary for transmission, 3) transmitting it, and 4) the communications application itself. In contrast to most government data bases, many small provider data bases do not have the technical support necessary to make such modifications. In these cases the provider may be called upon to bear the cost, or the goodwill assistance of software vendors may be sought. The question of whether the registry can pick up these

costs if the provider is unwilling or unable to do so must be settled early.

## NETWORKS

Telecommunications networks already exist in many areas. For example, there are private networks, university networks, and government networks, to name a few. Any of these may be part of the Internet, and any of these may function as part of a Community Health Education Network (CHIN). These networks can provide the infrastructure to support a registry. However, such networks may not be suitable if they are not active and robust, lack security, or if the network protocols are incompatible with protocols to be used by the registry. Issues of cost-sharing and "ownership" also may arise when operating with other networks. In some cases these disputes have delayed registry development. State governments may prohibit private providers from having access to their wide area networks for security reasons. Use of the Internet may be acceptable provided that issues related to confidentiality and security are resolved (see the section on Security).

These issues may prompt some registries to use a combination of methods. Alternatives include:

1. Computer connections via local area networks interconnected into a metropolitan area or wide area network. This may be desirable when leveraging local investments is desired along with connectivity to a central location (or interconnection between sites) at reasonable speeds;

2. Computer (modem) connections via analog (POTS) or digital (ISDN or DSL) telephone lines where use may be more occasional and/or costs need to be kept especially low;

3. Other technologies, like FAX and interactive voice response, connected via analog telephone lines where alternatives to desktop computer use is desired.

## DISTRIBUTED VERSUS CENTRALIZED SYSTEMS

A variety of systems architectures are possible when deploying a registry. Choosing the right architecture is important, since it will drive the way data flows between components, the currency and availability of data at different points in the system, and ultimately determine how satisfied the users of the system will be.

Centralized systems keep all the registry's data in a central location. Many technologies can be used to implement a centralized system. One may select a terminal-to-host system that uses a central timesharing computer to store all the data. Or, one may opt for a client-server system that uses desktop client software accessing a central data repository on a LAN, Unix, or mainframe server. The advantages of centralized systems are that all data reside in a

single authoritative location where they can be secured, managed, and protected more conveniently. The disadvantages include the additional computing power typically required to maintain the central server, and the reliance on networks to connect all the participants to their data.

Distributed systems place the registry data in a variety of locations, typically closer to the users. Standalone PC strategies are typical of this architecture, as are LAN-based systems that support some form of periodic consolidation of data in a central location. The advantages to this architecture include easier end-user access to frequently-used data about local patients, less reliance on multi-site networks to connect users to a central system, and more autonomy for local systems. The disadvantages include more data fragmentation, more problems determining which data are authoritative for a patient, added technical complexity when trying to consolidate data, and possible data quality problems unless standards are rigidly enforced.

To accommodate the wishes and needs of providers and others users of registries, hybrid system architecture combining features of both centralized and distributed systems should be considered.

## VOLUME OF TRANSACTIONS

Determining the potential magnitude and scope of the registry is an important part of choosing a system architecture. The system's designers will need to know the size of each record, the number of records likely to be entered in the system, and the length of time they will be stored. A determination should be made about the amount of time to be allowed for the system to respond when queried for information. This decision should be based upon peak usage times such as before school opening in the fall. Another helpful tool in planning registry architecture is an accurate prediction of the number and types of transactions that will be made on the system. Knowing this in advance will permit choices about the storage capacity required, types of network and telecommunications equipment needed, and protocols to be used. Keep in mind the need to build in the capability for expansion in the system as technology advances and user requirements increase.

## PLANNING FOR SECURITY

The degree of security required for a registry will influence its architecture at all levels. Security concerns will affect the types of data collected and where it is stored. Distributed systems (data retained in local computers) may be viewed as either an advantage or a disadvantage in terms of security. Centralized systems may better lend themselves to the design and implementation of security features. However, when unauthorized access is obtained to such a system, greater amounts of information are at risk. Use of existing or non-

dedicated networks, including the Internet, may have to be discouraged in the interest of controlling access to the information in a registry. Alternatively, sophisticated and expensive barriers, encryption technologies, and monitoring software can be used to protect registry data. Good security includes reliable means to back-up data regularly and a method to deal with equipment failure or destruction. At a minimum, data must be saved and protected during periods of equipment outage. At best, redundant components may allow a system to continue to function during such episodes. All of these factors should be taken into account when weighing the options for registry architecture.

## RESOURCES

Funding and staffing levels must be adequate in order for the system to perform as designed, be maintained, and meet the expectations of users. Staff training and user support must be planned for and funded in advance. Start-up expenses may necessitate limiting the initial scope of the registry to serving only selected providers. Such providers might include large-volume providers, automated providers, or providers serving populations most at risk of being under-immunized.

In the beginning, some trade-offs and compromises in desired architecture may be necessary due to funding and logistical constraints. More affordable, but less desirable, options may have to be accepted on an interim basis. These alternatives might include modifying and building on existing technologies or systems, or developing a system where the data and application software is centralized on a "host" computer. Partners will likely have opinions on the relative benefits and disadvantages of different trade-offs. A consensus is desirable about such cost related issues as whether to: 1) include a vaccine inventory system along with basic immunization information, or 2) incorporate registry functions into the providers' existing software on their computers with a graphical interface (e.g. Microsoft's Windows operating system[****]).

## TARGET POPULATIONS

The size of a registry will be determined by the scope of the population targeted. Factors to be considered include the geographic area served and the ages of persons to be included. As discussed previously, registries intending to capture immunization data for each person in their catchment areas may need to support a very extensive telecommunications infrastructure.

---

[****] Mention of the product of a specific company is for identification purposes only and does not constitute or imply endorsement by the U.S. Department of Health and Human Services or the All Kids Count Project.

System designers can anticipate costs based on staffing needs, the number of providers to be connected and age groups to be included. They may also help the project manager determine during the design process, whether an acceptable procedure would be for paper or faxed records to be sent by providers and encoded by registry (rather than provider) staff.

There is a growing recognition of the substantial extent of resources needed to design and implement an immunization registry. As discussed, these requirements go far beyond designing the data base and application software. The National Immunization Program has indicated that, in many cases, it may be appropriate to target limited resources in order to develop registries first for communities with large numbers of under-immunized persons.

# 4: IMPLEMENTING RECORD EXCHANGES

Immunization records need to be exchanged at several levels within a registry. Among these are recurring requirements to transfer large numbers of records in a batch file (e.g. data from electronic birth certificates, data transferred to or from Medicaid or the WIC program, and data transmitted to or from large health maintenance organizations). The effort to establish correct formats for batch file transfers may be considerable but justifiable in the above examples. In the cases of smaller data bases, the time and effort required to create batch files may be unreasonable in relation to the amount of information received. If the concept of state-based immunization registries is to be realized, it is imperative that mechanisms be in place for the exchange of records between providers and their community registry, between community registries within the same state, and between registries across state lines.

For record exchange to work, a core data set with one standard format must be defined. Every registry **must** structure its record exchange process to include these key data elements. With a standard format, data will not be lost when transferred between computer data bases. It is not mandatory for all data elements to be present before record exchange can be initiated, although this facilitates positive identification of individuals.

An authoritative record exchange protocol for immunization data was developed as a Health Level 7 (HL7, Version 2.3) standard accredited by the American National Standards Institute. All registry developers are strongly encouraged to be familiar with the HL7 standards, and to ensure that their registries are in compliance with these standards. Until implementation of the standard is more common, it is recognized that other communications methods will be utilized for record exchange. For the most up-to-date information on the standard, contact the National Immunization Program, Data Management Division, CDC, or:

HL7 Executive Director
Health Level Seven
Phone (313) 677-7777
E-mail: hq@hl7.win.net

## KEY ELEMENTS OF IMMUNIZATION RECORD EXCHANGE STANDARD

The following functional capabilities are required for two computer systems to exchange records on line.

1. QUERY: The ability for one computer system to electronically initiate a query to another to seek immunization data on (a) specific patient(s). The provider/system seeking these data must have authorization to do so.

2. RESPONSE: The ability for the system being queried to respond to the initiator whether a specific patient match is found or not. Multiple responses could be returned to the initiator if multiple matches to the query identifiers are found. For instance, if the initiator used only one or two fields of data to identify a record so that multiple records matched these fields, then the query would not uniquely identify the record being sought. In that case, the responder would request additional data until a unique match is found.

3. RECORD EXCHANGE: Once a unique match of a record is made, the responding system formats the immunization data on that child and transmits it to the requesting provider/system.

The HL7 standards specify the data and format of immunization record exchange messages. Any systems conforming to the standard, regardless of the platforms, environments, or application software used, can communicate efficiently. The data required by the HL7 standard messages is consistent with the recommended core data set developed by the CDC and approved by the National Vaccine Advisory Committee (see Appendix III-3). The HL7 standard query is not dependant on identification numbers for individuals. Rather, it allows basic elements of personal information to be provided which can be matched between systems. A minimum of one of the basic client identification elements must be used (e.g. name), but if more are provided (e.g. birth date, or mother's name), the likelihood for a unique match increases.

## CONSIDERATIONS

Data transmissions of immunization records must be secure, and systems should permit access only to the specific providers/systems authorized to receive them. A log of individuals making queries, times of queries, and dates of queries should be maintained. Log reports should be available to immunization registry monitoring agencies on demand.

# 5: DESIGNING ASSESSMENT ALGORITHMS

Providers using immunization registries need automation of at least two types of assessment activities. One is the assessment of vaccines needed for each client. This assessment can be used pro-actively to set appointments and send reminders, or retroactively to recall clients who have missed needed vaccines. A second assessment function is to report to providers on the immunization status of their client population as a whole. These assessments can help providers know how to improve the organization of their immunization services. A third assessment function, only possible when virtually the entire eligible population of a given area is enrolled, is the assessment of immunization coverage of children in the registry's geographic area and also in defined subsets of them. The degree of completeness required for this type of assessment has not yet been achieved for most registries and is not discussed further.

## DETERMINING VACCINATIONS NEEDED FOR INDIVIDUALS

An automated process for assessing the completeness of immunization histories is often the most complex and difficult part of the system to develop. Further complicating the matter, rules for assessing immunization histories change frequently, necessitating modifications to the automated process. "Hard-coded algorithms" (i.e., translating each aspect of the immunization schedule into computer code, without reference to any external, easy-to-update data structures or tables) make little sense in this situation. New and innovative approaches such as "rule-based" algorithms operating on the Internet are currently being explored.

### Table-driven assessment algorithms

Presently the most appropriate approach appears to be for registries to employ algorithms that use tables to define the following items:

- Types of vaccines recommended
- Age (often a range) at which each immunization is due
- Number of doses of each type of vaccine needed to complete a series
- Acceptable interval between doses in order for an immunization to be valid
- Vaccine combinations which may be used

There are also some specific technical issues for which policies must be set:

- **o** Should age be calculated in months, days, or other units?

- **o** How much flexibility should algorithms have to let providers set their own modifications of the schedule?

One difficulty faced by the registry developer and computer programmer is how software can be designed to accommodate all of the different ways health care providers actually function. Desired or ideal provider practices may be represented in a computer program but may not reflect reality. However, the system should not hamper or restrict the provider's mode of operating. For example, a nurse or physician may decide that 28 days is enough time to qualify as "a month" when deciding whether to give the next dose of DTP vaccine to a child. A computer rigidly defined algorithm which counts a month as 30 or 31 days may reject the immunization as not being given at a valid interval. Immunization program staff or providers may question "missing the opportunity" to vaccinate a child who is in the clinic 29 days after the last dose when the registry computer requires 30 days to have elapsed. Clearly these are issues that programmer, provider, and public health staffs must work together to resolve. Users' needs should be met without compromising the adequacy of the immunization services provided or risking not immunizing hard-to-reach children based on arbitrary computer-generated assessments.

New issues will continually arise as vaccine recommendations change (as with the new sequential use of inactivated and live polio vaccines) or as states make their own specific vaccination recommendations (such as giving a second dose of measles vaccine at school entry). High risk populations may have special recommendations (e.g., administering Hepatitis A vaccine) associated with them. Other variables may spring up with specific requirements such as future epidemic control measures. These will provide challenges that should be anticipated, to the extent possible, in the design of assessment algorithms. Programming staff need to be apprised as early as possible about new issues if they are to develop acceptable solutions.

**Validation of assessment algorithms**

Different algorithms created independently for different registries may be expected to produce different results for the same situations. Allowing the algorithm to process "test cases" in order to validate the outcome is desirable. The process involves generation of multiple fictitious immunization histories and their presentation to the immunization needs algorithm to see whether it gives the "correct" responses. The particular test cases generated reflect an implicit philosophy regarding which aspects of an immunization needs assessment algorithm are most important and how closely the algorithm must come to yielding standard responses.

## ASSESSING IMMUNIZATION STATUS OF A CLINIC POPULATION

Assessment enables providers to determine how well and how appropriately immunizations were administered during a particular period of time at their facilities. To date, this function has been made available primarily through a PC software application produced at CDC called Clinic Assessment Software Application (CASA). This software has wide applicability. Its main drawback is the effort required to capture data in a form suitable for analysis by the program. Until recently this effort required manual selection of medical records, their review, and then entry of data. CASA does not integrate the data on an individual child who may have received immunizations from different clinics. A recent version of CASA includes the ability to import data from external databases. Accordingly, linkage to registries is now possible. Alternatively, CASA may be built directly into registries. The CASA software can also produce a detailed report identifying possible barriers to immunizations within a practice, such as missed opportunities for simultaneous immunizations.

# 6: BUILDING IN SECURITY FEATURES

One step that must be taken by immunization registry developers is establishing and implementing a security policy. Information security is defined as: **a set of technical and administrative procedures designed to protect data systems against unwarranted disclosure, modification, or destruction and to safeguard the system itself.** The security policy should clearly delineate the respective roles and responsibilities of the registry staff and users with respect to:

- **o** protection of confidentiality of clients,

- **o** integrity of data, and

- **o** functionality of the hardware, software, and communications systems.

Most emphasis is placed on the technical approaches to security, revolving around controlling access to the database. But security also involves the physical facilities and the staff's adherence to confidentiality policies.

**Physical Security:** Computers holding the database should be kept in a locked facility. Unauthorized personnel should be automatically "locked out" whenever the computers are left unattended. Uninterrupted power supplies should be provided for the computers. Data backups, including off-site storage of backup data, should be in place and functioning. Restoration from backups should be periodically tested. Contingency plans for disaster recovery should include arrangements to utilize a separate computer in a different physical facility that could function identically to the primary system if that became necessary.

**Staff training:** It is essential that personnel responsible for the technical operation of a registry stay up to date with new developments affecting the software or hardware being used, including management of security. At times, the assistance of consultants may be needed.

## TECHNICAL MEASURES TO ENHANCE SECURITY OF DATA

**Create Security Levels for Applications:** The authority to access and modify data should correspond to a particular users needs. For example, three security levels should be created for users given access to a registry:

Reader: Can view data but cannot add or modify data; limited access to standard reports; no access to outreach processes.

User: Can view and modify data *except* for "critical fields"; cannot add new records; limited access to standard reports and outreach processes.

Manager: Can view and modify all data, including "critical fields"; can add children; full access to all standard reports and outreach processes.

The levels of access granted to the users of any given registry will depend upon the specific logistical requirements, applicable laws, and agreements with providers governing that registry.

In the example of the Manager, cited above, "Critical Fields" may be defined as those fields required to establish the uniqueness of a record in the registry. An application with a restricted screen or panel may be programmed for addition/update of these fields, as shown in Figure III- 1:

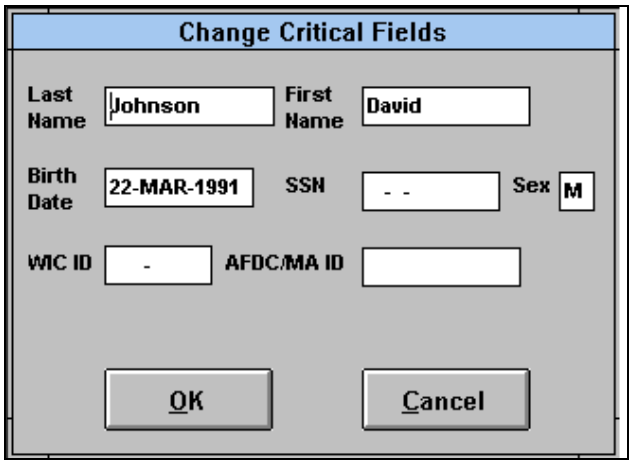
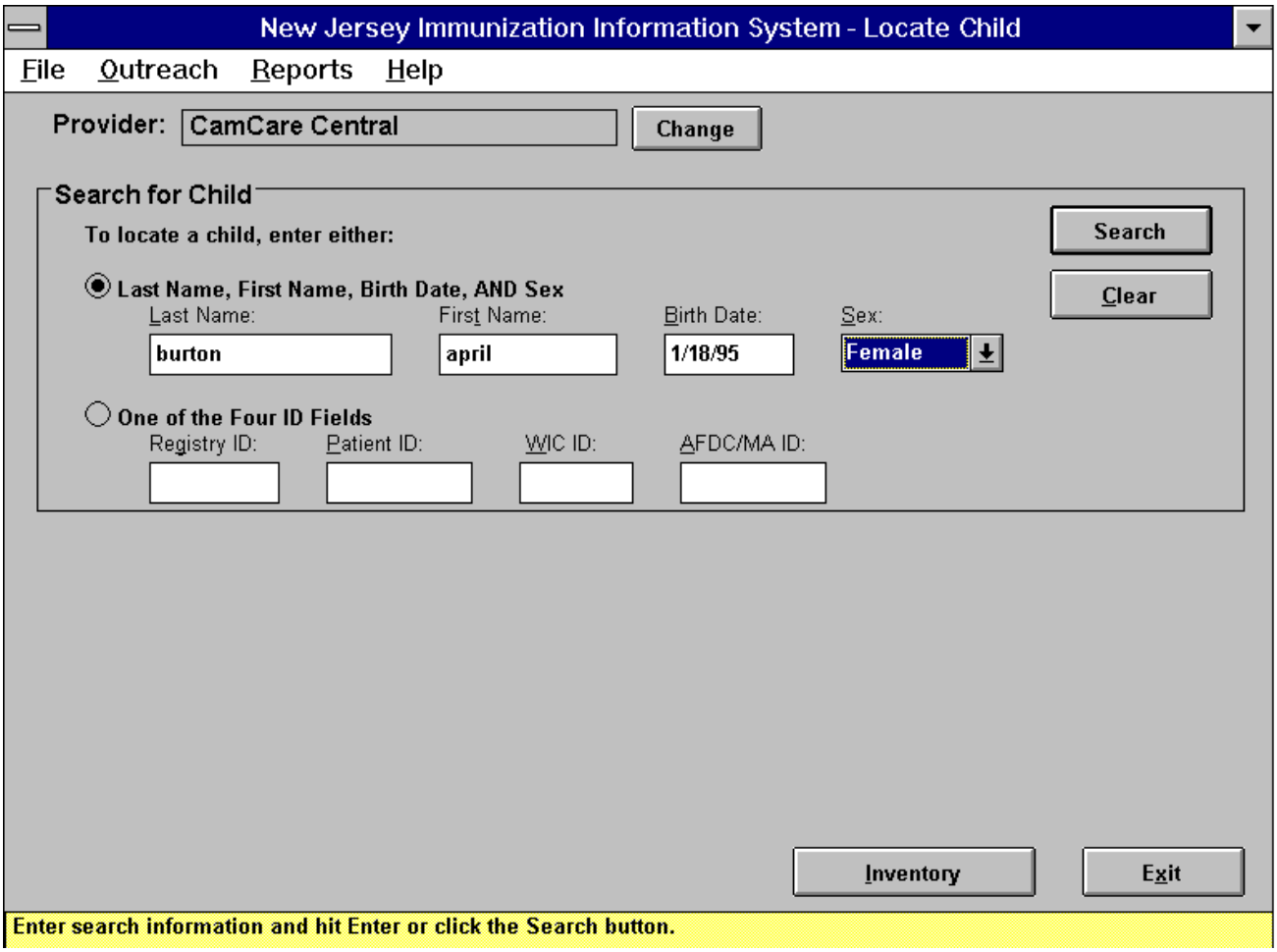



**FIGURE III-1: Example of layout that might be accessible only to managers with special access authorization, to modify critical data needed for uniquely identifying a record.**

Similarly, a look-up screen for a record might restrict simple, free browsing to ensure confidentiality of records, as in Figure III-2:

**FIGURE III-2: Example of a layout requiring the user to know specific patient information before opening the record. The screen display may be restricted to show no more personal information than that entered by the user. Data elements which might be protected in this way include those defined as sensitive in the data tables (see Tables III-2 and III-3).**



Information security and ease of access must be balanced. Ease of access can compromise information security if not carefully planned. Too much security can make an application difficult or impossible to use, even by valid users.

## THREAT ANALYSIS[+]

To understand and address specific security needs, a complete risk analysis is desirable. Consultants may be employed for this, or the following steps may be taken if there is adequate technical expertise available "in-house."

1. Identify information assets that need protecting.
2. Describe the architecture of information systems to be used.
3. Identify threats to those information assets based on architecture.
4. Rank threats on a high/medium/low scale; identify the most serious threats.
5. Develop solutions to mitigate threats as much as possible.
6. Make specific recommendations for solutions.

### Information Assets

Sensitive data may be identified for any major grouping of information. Typically they are:

- **o** personal information about clients, including addresses.
- **o** information about providers.
- **o** technical information such as user profiles, authorizations, system access logs.

### System Architecture

The major components to describe are:

| | |
|---|---|
| **Database** | The principal data repository and management system plus the computer, work-station, or server upon which it runs. |
| **Desktop Computer** | Client computers (e.g. terminals, industry-standard personal computers) including hardware, configuration, and desktop operating systems (if applicable). |

[+] Much of the information presented on information security, threat analysis, examples of threats and solutions was provided by Noam H. Arzt, Ph.D., Executive Director, Administration and Information Technology Architecture; Acting Director, Network Services; Research Associate/Senior Fellow, University of Pennsylvania, Suite 221A, 3401 Walnut Street, Philadelphia, PA 19104.

| | |
|---|---|
| **Network Protocol** | System for connecting users via local or wide area network, e.g. TCP/IP, SNA. |
| **Wide-area Network** | Examples include proprietary networks covering a large area (i.e., more than a single building or campus), including some existing state government operated networks, and the Internet. |
| **Applications** | Computer programs and tools used by clients, including the tools used to create them and their connections to the database. These may be host-based or client/server. |
| **Query Tools** | Commercial or custom-developed applications used to question a central database, including the network connection to the registry. |
| **Data Collection** | Methods by which data enter registries either via electronic interface with large data systems, from providers' systems, or by other means. |
| **Data Access** | Access to information via applications permitting clinical providers to see data in the registry and to transfer data to their systems. This also includes applications program interfaces (APIs) programs developed by vendors to facilitate access. |
| **User Access** | Methods by which on-line users receive direct or indirect access to the registry. |

A list of potential threats is provided in Appendix III-2 as a guide in analyzing security needs based on types of data included in the registry and system architecture. Threats are divided into three categories: 1) Those related to **desktop terminals** ("dumb" terminal or personal computer), 2) those related to **system computers** (mainframe, work-station, or server), and 3) those related to **Networks** (regardless of networking methods used).

For each threat considered, a ranking can be made of potential for the threat (**Risk**) and the severity of damage accruing if the threat does occur (**Harm**). Risk and Harm should be assessed as **High**, **Medium** or **Low**.

## EXAMPLES OF THREATS AND SOLUTIONS

Once the most serious threats are identified, some possible solutions should be developed

to mitigate these threats wherever possible. Solutions should focus first on threats where potential risk and harm are rated high. A list of typical serious threats and possible solutions developed for one state registry deployed in a client/server architecture follows:

***Threat:*** Unauthorized access to records; inappropriate disclosure of data via user's desktop computer.

***Solutions:*** Include sanctions for inappropriate behavior in a security policy.

Issue security clearances permitting user access on a need to know basis only.

Educate staff concerning the need not to leave terminals unattended with applications still running.

***Threat*:** Deletion of an important local file from a computer in a provider's office.

***Solutions:*** Develop an information security policy that incorporates regular data backups.

Require compliance for registry participation.

Purchase and install software or hardware to secure registry files on provider desktops.

Encourage sites to install registry software on local file servers that are routinely maintained and backed up.

***Threat:*** Physical damage occurring to server or network.

***Solutions:*** Locate server in a secure room.

Provide upgraded environmental conditions wherever the server is located. These may include uninterrupted power supply, redundant network connections, redundant systems in different locations, and special environmental controls (e.g., air conditioning).

Implement a sound backup procedure to facilitate recovery from a catastrophic event, including off-site storage of backup media.

# 7: SUMMARY OF 25 KEY ACTION STEPS: TECHNOLOGY

**System functionality**

1. Involve technical experts early in the planning process. Ensure that they are fully informed of the objectives and resource issues that will apply to their work. Include their expertise in discussions about these issues and implement their recommendations, where appropriate.

2. Identify which functions of the registry will be essential and which will be optional, taking into account the availability of resources and the anticipated scope of the registry.

3. Determine whether the registry will give high priority to serving certain groups within the community and if so, identify specific issues relating to that group. An example would be ensuring a satisfactory linkage with WIC clinics or key managed care organizations.

**Data design**

4. Establish minimum data sets that include the core elements recommended by the National Vaccine Advisory Committee and the Centers for Disease Control and Prevention. Other data elements may be added to these to increase registry functionality.

5. Build in data validation processes (error checks) to reduce the entry of erroneous information.

6. To avert concerns about misuse of data, develop identification procedures where client names are used in conjunction with confirmatory data such as birth date or mother's name. Use these data items in preference to more sensitive data, such as addresses.

**Technical architecture**

7. Design system architecture that can be implemented with the existing community computer and telecommunications infrastructure. However, ensure capacity for greater future usage as large banks of data become available.

8. Ensure that the registry design will handle periods of heavy demand, such as the beginning of the school year.

9. Accommodate users who will establish connectivity through a variety of methods.

Wherever possible, avoid attempting to force a single solution on multiple providers.

10. Seek support and cooperation from vendors of software used in provider's offices. Their support will tend to promote compatibility between provider systems and the registry, reducing the complexity of data entry and record exchange.

**Record exchange**

11. Ensure the design will be able to exchange records between providers and with other registries. Use procedures that are compatible with those recommended by appropriate standard setting bodies, such as Health Level 7 (HL-7), accredited by the American National Standards Institute (ANSI).

12. Build a working relationship with state and local WIC program staff to facilitate data sharing and access.

13. Identify and resolve issues, such as confidentiality concerns, that may inhibit participation and exchange of immunization data between different agencies. Organizations in question may include Medicaid, AFDC, WIC, community health centers and managed care organizations.

**Assessment algorithms**

14. Ensure that individual immunization software will accommodate expected frequent changes in vaccination recommendations. Table-driven applications may be easier to update and therefore the best long-term solution.

15. Establish a clear, consistent, and practical policy on acceptable minimum intervals between doses of vaccines in a series. Include guidelines for vaccines to be considered valid by an assessment algorithm, such as using calendar months and years rather than days.

16. Reach a consensus with providers in the community regarding which immunization schedules will be acceptable and usable by the assessment algorithm. Identify points that have to be customized.

17. Establish a clear policy regarding the validity of vaccinations recorded without an exact date of immunization, or whether algorithms will accept the provider's notation that the immunization is a specific dose in a series (1st, 2nd, 3rd, etc.).

18. Incorporate software applications that will assist providers in reviewing how well their clients are immunized and identify "missed opportunities" for vaccination. If possible

use table-driven software to facilitate changes in recommendations; the CDC Clinic Assessment Software Application (CASA) is available to integrate into registry systems or as a model for this function. However, it is presently "hard-coded."

19. In cooperation with immunization experts, develop or obtain test case sets to validate software algorithms to be used in performing assessment functions.

**Security**

20. Develop a security policy and procedures that provide an appropriate balance between protection from unauthorized access or data alteration and practicality of use for providers.

21. In selecting which hardware, software, and communications systems to use, consider the capabilities of the various alternatives with respect to confidentiality of the database.

22. Specify the sensitivity of each data element and define the policies and procedures applicable for restricting access to the most sensitive information.

23. Ensure that adequate physical security exists to protect the system against hazards such as fire. Develop and test a disaster recovery plan to include transfer of operations to an alternative, off-site computer.

24. Organize off-site storage for registry data backups. Assist users using more than "dumb terminals" with access to the registry. Establish satisfactory back-up procedures for their locally used software and client immunization records.

25. If using the Internet with the registry, ensure that adequate security procedures are in place to protect the entire database against unauthorized access. Use encryption to protect individual records while being transmitted.

# APPENDIX III-1

## THE INTERNET

In the last few years the Internet has evolved from a tool used almost exclusively by the scientific research community to a communications system employed by millions of individuals and businesses. Several dynamic circumstances suggest the Internet may play an important role in the future development of immunization registries. Among these are the increasing availability of personal computers, the merging of TV with Internet functions, and the spread of Internet access and simplification of its use. It is clear that the Internet has the potential to link providers to a registry and to link registries to each other. Beyond this, it may become a means to send and receive information about immunizations to and from individuals in their homes and work sites. Consumers may come to depend on the Internet to facilitate access to their personal health information. Registry planners should consider ways this development might be accommodated and plan for specific Internet utilization to be incorporated at the appropriate time.

Practical issues that may constrain Internet use between the registry and its users include:

- recurring costs (either charges by the hour, or for unlimited monthly use) for Internet connection.

- the possibility of lengthy waits, or of a cumbersome process to establish the first daily connection.

- the possibility of slow response time when interacting with the registry through the Internet.

- the possibility of repeated interruption of connection.

As a public network, the Internet poses greater risks of unauthorized access to the registry and the data it contains than for other types of telecommunication systems. These threats include sabotage of the database or operating software. Precautions that should be considered to ensure security of the system and data include:

- restricting database access from the Internet by placing barriers (“firewalls”) in the program between the server and users

- encrypting data

- keeping the operating system version current with all necessary security patches

- installing a reliable version of the operating system on the database server
- removing any unnecessary services
- allowing access for system administration only through "smart cards"
- installing a one-time password generator, and affecting frequent password changes
- auditing the system frequently for security risk exposure

# APPENDIX III-2

## POTENTIAL THREATS TO IMMUNIZATION REGISTRY SYSTEMS

### 1: THREATS TO DESKTOP COMPUTERS

- Unauthorized access via a user's desktop computer can result in the disclosure and compromise of sensitive data. Such access may take the form of viewing an unattended terminal, bribing or threatening a user to obtain information, or unauthorized electronic access or computer "hacking."

- Sensitive data stored on a workstation may be accidentally or deliberately altered or destroyed.

- The application code on a desktop may be altered making it possible to use the modified code to perform previously blocked functions, such as accessing or changing data on the database.

- Desktop computers are vulnerable to accidental or intentional infection by a virus.

- Physical damage may occur to a desktop computer by means such as fire, broken water pipes, or excess heat.

### 2: THREATS TO THE SYSTEM COMPUTER

- Unauthorized accesses to the server resulting in the compromise or circumvention of IDs and passwords and the further compromise or alteration of sensitive data.

- Special accounts that have the authority to damage the system if not used properly, such as the root or system account, are compromised by an intruder and the intruder alters the system, sometimes with the intent of making subsequent access easier.

- Misappropriation of a user ID with the intent to read, alter, or delete files or gain future access to information in the system.

- An authorized user engaging in deliberate sabotage of the system and/or data.

- A user or system administrator accidentally deleting or corrupting data or software in the course of performing his or her job responsibilities.

- The accidental introduction of a virus by someone performing his or her job responsibilities.

- The server being destroyed or incapacitated by natural or man-made catastrophe.

**3: THREATS TO THE NETWORK**

- The electronic theft of network addresses that are then used to gain access to systems on the network. Such theft is often accomplished by "spoofing, " or using one computer to impersonate a trusted computer on the network. Thereby unauthorized access is gained to read, alter, and delete data, or set up future access.

- Unauthorized access to restricted data by use of a "packet sniffing" tool (a software program that allows a computer on the network to view data intended for another computer). Such access permits the unauthorized operator to read restricted data or passwords being transmitted over the network.

- The intentional blocking of network service by flooding the network with messages.

- The compromise of a system ID or password caused by the user sharing it with an unauthorized user. Another means of compromise is writing down IDs or passwords and allowing it to be disclosed. Compromise may also take place by careless use of IDs and passwords on dial-up modem pools.

- Unauthorized data access can also be affected through an unsecured modem pool if network access can be obtained without requiring a password.

- Physical damage may occur to a network by means such as fire, broken water pipes, or excess heat.

# APPENDIX III-3

## RECOMMENDED CORE DATA SET FOR STATE IMMUNIZATION INFORMATION SYSTEMS

Extracted from Guidelines for State Immunization Systems, Version 2.8, with Vaccine and Manufacturer Tables updated November 1996

### 1: Listing of Core Data Set (Core data items are listed in **bold** print.)

The primary change in Version 2.6 of the Guidelines from the previous version is the refinement of core data items. This data set was prepared by the National Immunization Program in consultation with the Immunization Grantee Working Group, and further expanded by suggestions from public health representatives and private providers. It was reviewed by the National Vaccine Advisory Committee, and recommendations of the Committee were incorporated. In Version 2.7, patient birth order was added as an optional item to aid in patient identification in the event of multiple births. Additionally, vaccine and manufacturer tables were updated. Version 2.8 again updated the vaccine table. These tables will continue to be updated as changes in available vaccines occur. It is anticipated that record exchanges will occur within the framework of nationally recognized standards. To that end, a standard message for immunization data exchange has been developed using Health Level 7 (HL7) Standard Version 2.3.

### 2: Patient/System/State Identifiers (Until a unique personal identifier can be established on a national basis, multiple means of identification must be used).

**Patient name: first, middle, last**

Patient alias name: first, middle, last
(former names for management of adoptions and name changes)

Patient address, phone number, birthing facility:
(these variables should be locally defined)

Patient Social Security number (SSN)

**Patient birth date**

**Patient sex**

Patient race

Patient primary language

Patient birth order

Patient birth registration number

**Patient birth state/country**

Patient Medicaid number

**Mother's name: first, middle, last, maiden**

Mother's SSN

Father's name: first, middle, last

Father's SSN

## 3: Immunization Event Identifiers

**Vaccine type** (See attached table)

**Vaccine Manufacturer** (See attached table)

Vaccine dose number:

> NOTE: With a fully operating system, this variable is not needed. However, in the real world, and particularly during the initial startup phase, many systems will be gathering partial histories. To evaluate histories properly, dose number becomes very important. The ultimate goal is to remove this variable from the core data set within the first 2 to 3 years of system operation.

Vaccine expiration date

Vaccine injection site

**Vaccination date**

**Vaccine lot number**

Vaccine provider

Vaccine adverse events monitoring

[Such events must be linkable to the existing national adverse events surveillance system, with immunization information systems having ability to electronically report, without redundant keying of information to the Vaccine Adverse Events Reporting System (VAERS).]

Vaccine preventable disease reporting

[Such disease events must be linkable to existing local, state, and national disease reporting systems, with the immunization information systems having ability to electronically report, without redundant keying of information to the appropriate disease reporting systems.]

# Table of Vaccine Types

| Value | Description | Vaccine Name |
|---|---|---|
| 24 | Anthrax | Anthrax |
| 19 | BCG | Bacillus of Calmette & Guerin |
| 27 | Botulinum antitoxin | Botulinum antitoxin |
| 26 | Cholera | Cholera |
| 29 | CMVIG | Cytomegalovirus immune globulin, intravenous |
| 12 | Diphtheria antitoxin | Diphtheria antitoxin |
| 28 | DT (pediatric) | Diphtheria & tetanus toxoids |
| 20 | DtaP | Diphtheria-tetanus-acellular pertussis |
| 50 | DTaP-Hib | DTaP-Haemophilus influenzae type b conjugate |
| 01 | DTP | Diphtheria-tetanus-pertussis |
| 22 | DTP-Hib | DTP-Haemophilus influenzae type b conjugate |
| 30 | HBIG | Hepatitis B immune globulin |
| 31 | Hep A--(Pediatric) | Hepatitis A |
| 52 | Hep A--(Adult) | Hepatitis A |
| 08 | Hep B--adolescent or pediatric | Hepatitis B--adolescent or pediatric |
| 42 | Hep B--adolescent/high risk infant | Hepatitis B--adolescent/high risk infant |
| 43 | Hep B--adult | Hepatitis B--adult |
| 44 | Hep B--dialysis | Hepatitis B--dialysis |
| 45 | Hep B--other or unspecified | Hepatitis B--other or unspecified |
| 17 | Hib--unspecified | Haemophilus influenzae type b conjugate-unspecified |
| 46 | Hib--PRP-D | Haemophilus influenzae type b conjugate--PRP-D |
| 47 | Hib--HbOC | Haemophilus influenzae type b conjugate--HbOC |
| 48 | Hib--PRP-T | Haemophilus influenzae type b conjugate--PRP-T |
| 49 | Hib--PRP-OMP | Haemophilus influenzae type b conjugate--PRP-OMP |
| 51 | Hib-Hep B | Haemophilus influenzae type b conjugate-Hep B |
| 14 | IG | Immune globulin |
| 15 | Influenza--split (incl. purified surface antigen) | Influenza--split (incl. purified surface antigen) |
| 16 | Influenza--whole | Influenza--whole |
| 10 | IPV | Poliovirus vaccine, inactivated |
| 39 | Japanese encephalitis | Japanese encephalitis |
| 03 | MMR | Measles-mumps-rubella |
| 04 | M/R | Measles & rubella |
| 05 | Measles | Measles |
| 32 | Meningococcal | Meningococcal |
| 07 | Mumps | Mumps |
| 11 | Pertussis | Pertussis |
| 23 | Plague | Plague |
| 33 | Pneumococcal | Pneumococcal |
| 02 | OPV | Poliovirus vaccine, oral |
| 18 | Rabies--intramuscular injection | Rabies--intramuscular injection |
| 40 | Rabies--intradermal injection | Rabies--intradermal injection |
| 34 | RIG | Rabies immune globulin |
| 06 | Rubella | Rubella |
| 38 | Rubella/Mumps | Rubella & Mumps |
| 09 | Td (Adult) | Tetanus-diphtheria |
| 35 | Tetanus toxoid | Tetanus toxoid |
| 13 | TIG | Tetanus immune globulin |
| 25 | Typhoid--oral | Typhoid--oral |
| 41 | Typhoid--parenteral | Typhoid--parenteral |
| 21 | Varicella | Varicella |
| 36 | VZIG | Varicella zoster immune globulin |
| 37 | Yellow fever | Yellow fever |

Revised November 1996

## Table of Vaccine Manufacturers

| Code | Vaccine Manufacturer |
|---|---|
| AB | Abbott |
| AD | Adams |
| ALP | Alpha |
| AR | Armour |
| BA | Baxter |
| BAY | Bayer |
| BP | Berna |
| CON | Connaught |
| EVN | Evans |
| GRE | Greer |
| IUS | Immuno-US |
| KGC | Korea Green Cross |
| LED | Lederle |
| MA | Massachusetts Public Health |
| MSD | Merck |
| IM | Merieux |
| MIP | Michigan Dept Public Health |
| JPN | Microbial Dis/Osaka U |
| MIL | Miles |
| NYB | New York Blood Center |
| NAB | North American Biologicals, Inc. |
| OTC | Organon Teknika |
| PD | Parke Davis |
| PRX | Praxis Biologics |
| SCL | Sclavo |
| SKB | SmithKline |
| SI | Swiss Serum and Vaccine Inst. |
| WA | Wyeth-Ayerst |
| OTH | Other |
| UNK | Unknown manufacturer |

Revised 10/24/95