





Information Security Program

Health Insurance Portability and Accountability Act (HIPAA) Compliance Guide

September 14, 2005

SECURE ONE HHS

KEEP AMERICA'S HEALTH AND HUMAN SERVICES SECURE

Table of Contents

Preface

As the Department of Health and Human Services (HHS) Information Technology Security Program evolves, this document will be subject to review and update, which will occur annually or when changes occur that signal the need to revise the *HHS Health Insurance Portability and Accountability Act (HIPAA) Compliance Guide*. These changes may include the following:

- Changes in roles and responsibilities;
- Release of new executive, legislative, technical, or Departmental guidance;
- Identification of changes in governing policies;
- Changes in vulnerabilities, risks or threats; and/or
- HHS Inspector General findings that stem from a security audit.

The HHS Chief Security Officer (CSO) must approve all revisions to the *HHS Health Insurance Portability and Accountability Act (HIPAA) Compliance Guide*. Revisions are to be highlighted in the Document Change History table. Each revised guidance document is subject to HHS' document review and approval process before becoming final. When it is approved, a new version of the *HHS Health Insurance Portability and Accountability Act (HIPAA) Compliance Guide* will be issued, and all affected parties will be informed of the changes made.

The procedures outlined in the *HHS HIPAA Compliance Guide* are proven practices that will provide guidance to the Department in meeting or exceeding the mandatory policies identified in the *HHS Information Security Program Policy* document. The *HHS HIPAA Compliance Guide* provides specific information for the recommended implementation of HIPAA compliance. While the specifics of how to undertake the implementation are not mandatory, any security implementation undertaken by an OPDIV must result in security controls and processes that are equal to or stronger than those articulated in the Policies, Handbooks, and related Guides. If an OPDIV or STAFFDIV chooses not to adopt the baseline guidance set forth in this *HHS HIPAA Compliance Guide*, it must document this decision and assume responsibility for the creation of procedures of equal or greater stringency.

Document Change History

Version Number	Release Date	Summary of Changes	Section Number/ Paragraph Number	Changes Made By
1.0	10/29/2003	Initial document release	NA	NA
2.0	09/14/2005	Updated to reflect new regulatory requirements	Throughout	HHS CSO

1. Introduction

The Department of Health and Human Services (HHS) is responsible for implementing and administering an information security program to protect its information resources, in compliance with applicable public laws, federal regulations, and Executive Orders. These directives include the *Federal Information Security Management Act of 2002* (FISMA); the Office of Management and Budget (OMB) Circular A-130, *Management of Federal Information Resources*, dated November 28, 2000; and the *Health Insurance Portability and Accountability Act of 1996* (HIPAA). To meet these requirements, the Department has instituted the *HHS Information Security Program Policy* document and accompanying *HHS Information Security Program Handbook* document.

This *HHS Health Insurance Portability and Accountability Act (HIPAA) Compliance Guide* was created as part of the HHS Information Security Program to act as a guide for handling specific aspects of HIPAA security and privacy compliance. This guide may be used along with other security-related guidance documents to assist in FISMA and other regulatory compliance efforts.

1.1 Purpose

This document provides a summary of the requirements of the *HIPAA Privacy Final Rule* and the *HIPAA Security Final Rule*. It also provides a general outline to use as a first step in designing a HIPAA Privacy and Security compliance program.

1.2 Background

Congress passed HIPAA (Public Law 104-191) in part to simplify and standardize health care administrative processes to reduce costs and other burdens in the health care industry. HIPAA charges HHS and the Operating Divisions (OPDIVs) with adopting national uniform standards for handling certain individually identifiable health information (IIHI). In addition to its effect on the portability of health insurance, HIPAA requires all covered entities that deliver health care to follow standard practices related to recording, storing, and processing information. These requirements are often referred to as HIPAA's "Administrative Simplification" requirements or provisions. According to the HIPAA statute, HHS has published final standards related to unique health identifiers, code sets, security, privacy, electronic signatures, and the transfer of information among health plans. (See Figure 1.)

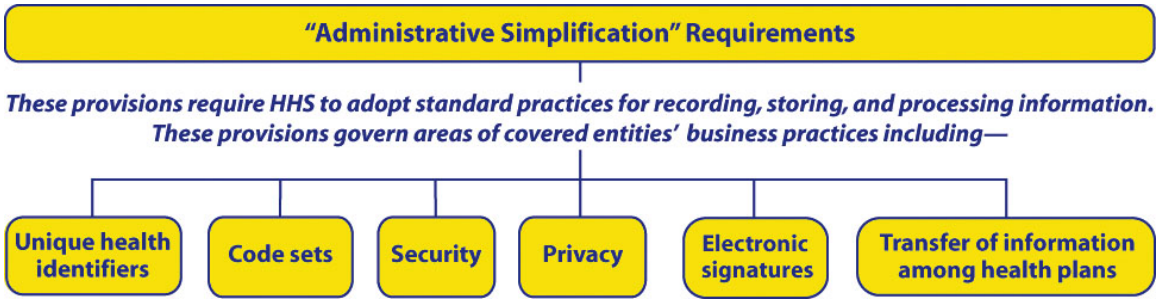

Figure 1. HIPAA "Administrative Simplification" Requirements

Security and Privacy have presented particular challenges to many "covered entities" (as defined in Section 2.1.2). Unlike some other categories of HIPAA's Administrative Simplification requirements, specific steps and activities for complying with the Privacy and Security requirements will require covered entities to analyze their organizational structure, goals, and activities, and determine what measures are "reasonable and appropriate" to ensure the security of protected health information under their control.

HIPAA requires HHS and the OPDIVs to adopt regulations setting privacy and security standards for all covered entities to follow. The privacy standards as modified (also referred to in this document as "the Privacy Final Rule"[1]) define appropriate and inappropriate disclosures of certain IIHI and indicate requirements for policies and practices that protect patients' privacy rights. Similarly, compliance with the HIPAA Security Final Rule (also referred to in this document as "the Security Final Rule") will enable covered entities to improve the protection of the confidentiality, integrity, and availability of certain IIHI before, during, and after electronic transmission.

1.3 Scope

This guide sets forth requirements under HIPAA as they apply to federal agencies that are also covered entities under the HIPAA Rules. Although FISMA applies to all federal agencies and all information types, only a subset of agencies is subject to the HIPAA Privacy and Security rules based on their functions and use of IIHI. A number of the OPDIVs, and/or their contractors, may have obligations under the HIPAA Privacy and Security rules. These obligations are based on the nature of their business and whether they create, receive, maintain, or transmit any IIHI that must be protected against reasonably anticipated threats, hazards, and impermissible uses and/or disclosures. Some of the security risk assessment activities undertaken as

[1] While this document refers to the "HIPAA Privacy Final Rule," readers should be aware that the HIPAA Privacy Final Rule that initially appeared in the Federal Register on December 28, 2000, was modified by an amendment that appeared in the Federal Register on August 14, 2002. The HHS Office for Civil Rights provides further links (http://www.hhs.gov/ocr/hipaa/) to the full text of the Privacy Final Rule, the 2002 amendments, and an unofficial integrated version that combines the rule as originally published and its amendments. http://www.hhs.gov/ocr/hipaa/

part of the FISMA process may assist in the HIPAA compliance efforts.[2] Figure 2 outlines the individuals that may be most interested in this guide.

Figure 2. HIPAA Guide Audience

[2] HIPAA also applies to some federal organizations outside of the HHS organization, including the Veterans Administration and the Department of Defense Military Health Services. While the information in this guide may be useful and applicable to these organizations, this guide was prepared exclusively for the use of HHS and the OPDIVs.

1.4 Document Organization

The remainder of this guide is structured as follows:

- Section 2 discusses HIPAA Administrative Simplification requirements with particular attention to the Privacy Final Rule, the Security Final Rule, and their relationship to each other; HHS guidance available for help in complying with HIPAA; and other useful references.
- Section 3 describes steps toward compliance with HIPAA Administrative Simplification requirements, outlines a timeline for compliance, and provides a list of possible noncompliance consequences.

This guide also contains the following appendices:

- Appendix A provides a feedback form to submit comments on the document.
- Appendix B lists the references used in this document.
- Appendix C lists the acronyms used in this document.
- Appendix D defines terms frequently used in this document.
- Appendix E provides a list of the guidance associated with the HHS Information Security Program.

2. HIPAA Administrative Simplification Requirements

2.1 General Overview

As required by Congress under HIPAA, HHS and the OPDIVs have adopted security and privacy standards, which are published in the Privacy Final Rule and the Security Final Rule. These regulatory requirements are discussed in Sections 2.2 and 2.3, respectively.

2.1.1 HIPAA Administrative Simplification Goals and Objectives

HIPAA provisions, presented in Figure 3, are designed to meet the following goals and objectives:

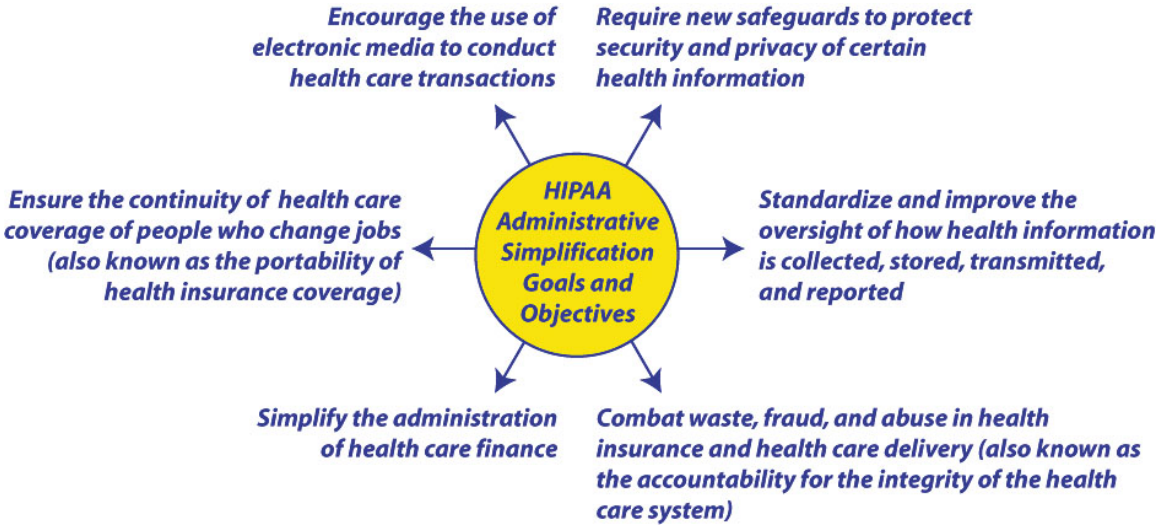

Figure 3. HIPAA Administrative Simplification Goals and Objectives

2.1.2 HIPAA Definitions

HHS' Office for Civil Rights has published an interactive tool to help entities determine whether they are covered entities and thus subject to HIPAA rules. Appendix B provides a link to this tool at the Centers for Medicare & Medicaid Services (CMS) website.

2.1.2.1 Covered Entity

Under HIPAA, "covered entities" are as follows:

- Health care providers who transmit any health information in electronic form in connection with certain financial and administrative transactions,[3] and
- Health plans and health care clearinghouses, as defined in section 160.103 of the Privacy Rule,[4] that process or facilitate the processing of health information received from another entity to a standard format for purposes of complying with HIPAA standard transaction requirements.

In addition to these entities, the HIPAA Privacy and Security Final rules may have implications for the business associates of covered entities. Business associates are independent entities that assist in performing a function that involves using or disclosing IIHI on behalf of a covered entity or on behalf of an organized health care arrangement in which the covered entity participates.[5] While the HIPAA rules do not regulate business associates, they charge HIPAA-covered entities with "obtain[ing] satisfactory assurance that the business associate will appropriately safeguard the information." Business associates may be HIPAA-covered entities in their own right. For more information on requirements of covered entities relative to their business associates, see section 164.314 of the HIPAA Security Final Rule (to be codified at 45 Code of Federal Regulation (CFR) 164.314).

2.1.2.2 Hybrid Entity

Some covered entities may have some business activities that are covered by the HIPAA Privacy and/or Security rules and other business functions that are not. Some of these entities may be able to designate certain components of their business as health care components. Hybrid entities that choose to designate certain components as health care components:

- Must assign the designation to any component that would meet the designation of covered entity if it were a separate legal entity; and
- May only designate a component as a "health care component" to the extent that it performs health care functions or activities that would make it a "business associate" of one of the covered entity's other components that performs covered functions, if the two components were separate legal entities.

Hybrid entities must consider their status as such in designing a HIPAA Administrative Simplification compliance plan. For more information on hybrid entities, see section 164.105 of the HIPAA Security Final Rule (to be codified at 45 CFR 164.105).

---

3 Such covered transactions include "all transactions covered by this Subchapter" (see Privacy Rule section 160.102 and Security Rule section 164.104). For a list of these transactions, see the definition of "transaction" included in the Privacy Rule 160.103 (to be codified at 45 CFR 160.103, applicable to both the Privacy and Security Rule).

4 The definition of "health care clearinghouse" at section 160.103 of the Final Privacy Rule is also applicable to the Security Final Rule, as the definition will appear in 45 CFR 160.103 which applies to both rules.

5 For a full definition of "business associate," see section 160.103 of the HIPAA Privacy Final Rule.

2.1.2.3 Affiliated Covered Entity

Another type of entity that may have special considerations in designing a HIPAA Administrative Simplification compliance program is an affiliated covered entity. An affiliated covered entity is legally separated from one or more covered entities that are all under common control.

Affiliated covered entities must consider their status as such in designing a HIPAA Administrative Simplification compliance plan. For more information on affiliated covered entities, see section 164.105 of the HIPAA Security Final Rule (to be codified at 45 CFR 164.105).

2.1.2.4 Medicare Prescription Drug Card Sponsors

The Medicare Prescription Drug Improvement and Modernization Act of 2003 (Public Law 108-173) added an additional covered entity for whom the HIPAA Privacy and Security rules are applicable. A Medicare prescription drug card sponsor is a nongovernmental entity that offers an endorsed discount drug program under the Medicare Modernization Act. This fourth category of covered entity will remain in effect until the drug card program ends in 2006.

2.1.3 Protected Health Information

HIPAA rules apply to covered entities that collect, store, transfer, or use IIHI; however, not all IIHI is covered by the rules. Health care providers, for example, are covered by the Privacy Final Rule and the Security Final Rule only if they handle IIHI that is also protected health information (PHI), which is information that is:

- Transmitted by electronic media;
- Maintained in any media covered by the rules' definition of "electronic media"; or
- Transmitted or maintained in any other form.

The standards of the Privacy Rule apply to all PHI. The standards of the Security Rule apply only to the first two kinds, information that is transmitted or maintained via electronic media. This type of PHI is referred to as electronic protected health information (EPHI).

2.1.4 HIPAA Exceptions

Some health information is not covered by the HIPAA rules. For example, the Privacy Rule specifically exempts health information that has been "de-identified" for research purposes. Information may be de-identified by aggregating it into a data report or by removing all information from the record that may enable it to be attributed to a specific individual. For more information on these exceptions, see sections 164.502(d) and 164.514(a) of the Privacy Final Rule.

2.2 HHS Regulatory Guidance for Compliance with the HIPAA Privacy Final Rule

2.2.1 History of the Privacy Final Rule

The Privacy Final Rule initially appeared in the Federal Register on December 28, 2000, beginning at page 82,461, and was modified August 14, 2002. The regulatory text itself appears between pages 82,798 and 82,829 of 65 Fed. Reg. 82462 and between pages 53,266 and 53,273 of 67 Fed. Reg. 53182. Appendix B provides a link to a web page hosted by the HHS Office for Civil Rights that provides additional links to the full text of the Privacy Final Rule, the 2002 modifications, and an unofficial integrated version that combines the rule as originally published with its modifications.

2.2.2 Goals of the Privacy Final Rule

The Privacy Final Rule provides the first comprehensive federal protection for the privacy of certain health information. The rule balances an individual's interest in keeping health care information confidential against improving the efficiency and effectiveness of health care delivery and the quality of health care in the United States.

2.2.3 Provisions of the Privacy Final Rule

As required by HIPAA, the Privacy Final Rule applies to health plans, health care clearinghouses, and those health care providers who conduct certain financial and administrative transactions (e.g., billing and funds transfers) electronically. All IIHI held by a covered entity in any form, whether in electronic, paper, or oral form, are covered by the Privacy Final Rule's provisions.

Under the Privacy Final Rule, patients have significant new rights that will permit them to receive information about their health information and control how it is used. Patients must be directly informed of the following rights:

- **Patient education on privacy protections.** Providers and health plans are required to give patients or members a clear, written explanation of how they can use, keep, and disclose patient PHI.
- **Ensuring patient access to their medical records.** Patients must be able to see and get copies of their designated record sets and request amendments (e.g., corrections) to those records. In most cases, patients must be informed of disclosures that the plan or provider makes to third parties, although some exceptions to this principle apply.
- **Receiving notification of how information is released.** Health care providers are required to notify patients concerning the use and disclosure of patient information for treatment, payment, and operations (TPO) purposes.

Patients have the right to request restrictions on the use and disclosure of their PHI.

- **Ensuring that consent is not coerced.** Providers and health plans generally cannot predicate treatment on a patient's agreement to allow for the disclosure of their PHI for non-treatment, payment, or other operations uses.
- **Providing recourse if privacy protections are violated.** Patients have the right to complain to a covered provider, to a health plan, or to the Secretary of HHS about perceived violations of the provisions of this rule or on the policies and procedures of the covered entity.

The Privacy Final Rule also grants rights of access to health care consumers to their PHI, notifies consumers on how their PHI is used and to whom it is disclosed, and amends consumers' designated record sets. The HIPAA Privacy Final Rule specifies that patients must be notified that they have the following rights to:

- Receive notice of the uses and disclosures of their protected health information;
- Request restrictions on certain uses and disclosures of their health information;
- Receive confidential communications related to their health information;
- Request and receive access to their medical records;
- Request amendments to their medical records;
- Receive an account of disclosures of their protected health information; and
- Receive a notice of these rights.

The Privacy Final Rule also places restrictions on the use of PHI. With few exceptions, an individual's PHI can be used only for TPO purposes. The following restrictions apply:

- **Ensuring limited uses of PHI.** Patient information can generally only be used or disclosed by a health plan, provider, or clearinghouse for purposes of TPO. PHI cannot be used for purposes unrelated to health care, such as employers making personnel decisions, without explicit authorization from the subject individual.
- **Providing the minimum amount of information necessary.** Disclosure of information must be limited to the minimum necessary. However, this provision does not apply to the transfer of medical records for purposes of treatment since physicians, specialists, and other providers need access to the full record to provide the best quality care.
- **Ensuring informed and voluntary authorization.** Nontreatment, payment, or operations disclosures with patient authorization must meet standards that ensure the authorization is truly informed and voluntary.

The regulation establishes the privacy safeguard standards that covered entities must meet, but it leaves detailed policies and procedures for meeting these standards to the discretion of each covered entity. In this way, implementing the

standards will be flexible and scalable to account for the nature of each entity's business, its size, and its resources. Covered entities must include the following:

- **Adopting written privacy procedures.** These procedures must state who has access to PHI, how it will be used within the entity, and when the information will or will not be disclosed to others. Covered entities must also take steps to ensure that their business associates protect the privacy of PHI they receive from the covered entity.
- **Training employees and designating a privacy officer.** Covered entities must provide sufficient training to their employees to ensure that they understand an employer's HIPAA privacy protections and designate an individual, sometimes called a chief privacy officer (CPO), who will be responsible for ensuring an employer's HIPAA privacy procedures are followed.
- **Establishing grievance processes.** Covered entities must provide a means for patients to make inquiries or complaints on the privacy of their records.

Under the Privacy Final Rule, certain PHI disclosures are permitted that do not require individual authorization, including information that is vital to public policy interests as well as certain activities that assist in the smooth operation of the health care system. The Privacy Final Rule states that covered entities may disclose information as necessary for the following:

- Statutory and other legal requirements;
- Public health activities;
- Protecting likely victims of abuse, neglect, or domestic violence;
- Certain health oversight activities;
- Certain judicial and administrative proceedings;
- Certain law enforcement purposes;
- Certain activities related to deceased persons, including identification (ID) and determining the cause of death;
- Cadaver organ, eye, or tissue donation;
- Research;
- Protecting the health or safety of a person or the public;
- Specialized military or government functions; and
- Workers' compensation.

Many restrictions and exceptions apply to these permitted disclosures. For more specifics on these categories, see section 164.512 of the Privacy Final Rule.

2.3 HHS Regulatory Guidance for Compliance with the HIPAA Security Final Rule

2.3.1 History of the Security Final Rule

The Security Final Rule was published in Volume 68 of the Fed. Reg. on February 20, 2003. Appendix B provides a link to the full text of the Security Final Rule.

2.3.2 Goals of the Security Final Rule

The main goal of the Security Final Rule is to protect the confidentiality, integrity, and availability of EPHI, which is certain "individually identifiable health information…that is…transmitted by electronic media or maintained in electronic media."[6]

- Confidentiality is "the property that data or information is not made available or disclosed to unauthorized persons or processes."
- Integrity is "the property that data or information has not been altered or destroyed in an unauthorized manner."
- Availability is "the property that data or information is accessible and useable upon demand by an authorized person."[7]

2.3.3 Provisions of the Security Final Rule

It is the intent of HHS to afford covered entities "the flexibility to select appropriate technology and to adopt new technology over time."[8] The Security Final Rule requirements are "technology-neutral," which means that covered entities will have many options in selecting technology and software packages that are compatible with the HIPAA Administrative Simplification requirements.

2.3.3.1 Standards and Implementation Specifications

The Security Final Rule sets out 18 "standards" and 36 "implementation specifications" as shown in Table 1.

---

6 Some types of IIHI are exempt from the definition of PHI, and therefore from the definition of EPHI. These exemptions are: "(i) Education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. 1232g; (ii) Records described at 20 U.S.C. 1232g(a)(4)(B)(iv); and (iii) Employment records held by a covered entity in its role as an employer." See definition of "Protected Health Information" at 45 CFR 160.103.

7 See Health Insurance Reform: Security Standards; Final Rule, 68 Fed. Reg. 8334 (2003) at 8376 (to be codified at 45 CFR section 160.304).

8 See Health Insurance Reform: Security Standards; Final Rule, 68 Fed. Reg. 8334 (2003) at 8335.

Table 1. Standards and Implementation Specifications

Safeguards	Standards	Implementation Specifications
Administrative	9	21
Physical	4	8
Technical	5	7
Total	18	36

- A “standard” is a requirement that must be met by all covered entities.
- An “implementation specification” is a specific requirement or instruction for implementing a “standard.”

According to the Security Final Rule, six standards “[include] all the necessary instructions for implementation” and have no associated implementation specifications; three standards have only one implementation specification; and the remaining nine standards have more than one implementation specification associated with them.

Note that in some cases, a covered entity may implement all the “implementation specifications” but must still look to the wording of the standard and assess whether it must also take further steps to comply with the letter and spirit of the standard. For example, the “Security Awareness and Training” standard has four implementation specifications, but none explicitly require a training program or manual for new hires. Obviously, for most covered entities, some initial training activity would be critical to instituting a meaningful Security Awareness and Training Program.

2.3.3.2 Required and Addressable Measures of the Security Final Rule

To comply with the Security Final Rule, “required” measures must be implemented by all covered entities. All 18 standards are required and must be implemented by all covered entities. Fourteen of the 36 implementation specifications are required, and the other 22 are addressable.

For the addressable implementation specifications, each covered entity must determine whether each measure (or some equivalent alternative measure) is “reasonable and appropriate” for that entity. This determination is based on the covered entity’s:

- Risk analysis;
- Risk mitigation structure;
- Existing security measures;
- Organizational size, complexity, and capability; and

- Cost of implementation.

Each covered entity is required to develop its own methodology for determining whether it needs to comply with each addressable implementation specification. The covered entity's methodology must incorporate the five considerations listed above, and the covered entity must document the methodology and show how it was applied to each implementation specification.

If an addressable implementation specification is deemed not "reasonable and appropriate," the covered entity must:

- Implement the alternative and document its decision and rationale if an alternative measure that accomplishes the same goal as the addressable implementation specification is reasonable and appropriate; or
- Document its decision to implement neither the addressable implementation specification or an equivalent measure and provide its rationale if no alternative measure that accomplishes the same goal as the addressable implementation specification is reasonable and appropriate.

2.3.4 Security Safeguards

Table 2 lists the three categories of security safeguards—Administrative, Physical, and Technical—and their respective standards.

Table 2. Summary of Security Safeguards

STANDARD	Implementation Specifications		
	Required	Addressable	Total
Security Management Process	4	0	4
Assigned Security Responsibility	+ 0	+ 0	+ 0
Work Force Security	+ 0	+ 3	+ 3
Information Access Management	+ 1	+ 2	+ 3
Security Awareness and Training	+ 0	+ 4	+ 4
Security Incident Procedures	+ 1	+ 0	+ 1
Contingency Plan	+ 3	+ 2	+ 5
Evaluation	+ 0	+ 0	+ 0
Business Associate Contracts and Other Arrangements	+ 1	+ 0	+ 1
SUBTOTALS—ADMINISTRATIVE SAFEGUARDS	*= 10*	*= 11*	*= 21*
Facility Access Controls	0	4	4
Workstation Use	+ 0	+ 0	+ 0
Workstation Security	+ 0	+ 0	+ 0
Device and Media Controls	+ 2	+ 2	+ 4
SUBTOTALS—PHYSICAL SAFEGUARDS	*= 2*	*= 6*	*= 8*
Access Controls	2	2	4
Audit Controls	+ 0	+ 0	+ 0
Integrity	+ 0	+ 1	+ 1
Person or Entity Authentication	+ 0	+ 0	+ 0
Transmission Security	+ 0	+ 2	+ 2
SUBTOTALS—TECHNICAL SAFEGUARDS	*= 2*	*= 5*	*= 7*
GRAND TOTALS	*14*	*22*	*36*

2.3.4.1 Administrative Safeguards

Administrative safeguards are defined as the "administrative actions, and policies and procedures, to manage the selection, development, implementation, and maintenance of security measures to protect electronic-protected health information and to manage the conduct of the covered entity's workforce in relation to the protection of that information."[9]

The Security Final Rule includes nine standards under the heading "Administrative Safeguards":

- **Security Management Process**—implement policies and procedures to prevent, detect, contain, and correct security violations. The Security Management Process standard has four implementation specifications:
  - **Risk Analysis (required):** conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of EPHI held by the covered entity.
  - **Risk Management (required):** implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level.
  - **Sanction Policy (required):** apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity.
  - **Information Activity System Review (required):** implement procedures to regularly review the records of information system activity such as audit logs, access reports, and security incident tracking reports.
- **Assigned Security Responsibility**—identify the security official who is responsible for developing and implementing the policies and procedures that are required by this subpart.
- **Workforce Security**—implement policies and procedures to ensure that all members of the entity's workforce have appropriate access to EPHI and to prevent those workforce members who do not have access from obtaining EPHI. The Workforce Security standard has three implementation specifications:
  - **Authorization and/or Supervision (addressable):** implement procedures for authorizing or supervising workforce members who work with EPHI or who work in locations where EPHI might be accessed.
  - **Workforce Clearance Procedure (addressable):** implement procedures to determine that the access of a workforce member to EPHI is appropriate.
  - **Termination Procedures (addressable):** implementing procedures for terminating access to EPHI when a workforce member's employment ends or when employee access to EPHI is not appropriate.

[9] See Health Insurance Reform: Security Standards; Final Rule, 68 Fed. Reg. 8334 (2003) at 8376 (to be codified at 45 CFR section 160.304).

- **Information Access Management**—implement policies and procedures for authorizing access to EPHI. The Information Access Management standard has three implementation specifications:

  - **Isolating Health Care Clearinghouse Function (required):** if a health care clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the EPHI of the clearinghouse from unauthorized access by the larger organization.
  - **Access Authorization (addressable):** implement policies and procedures for granting access to EPHI, for example, through access to a workstation, transaction, program, process, or other mechanism.
  - **Access Establishment and Modification (addressable):** implement policies and procedures that, based upon the entity's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process.

- **Security Awareness and Training**—implement a security awareness and training program for all members of the entity's workforce (including management). The Security Awareness and Training standard has four implementation specifications:

  - **Security Reminders (addressable):** implement periodic security updates.
  - **Protection from Malicious Software (addressable):** implement procedures for guarding against, detecting, and reporting malicious software.
  - **Log-in Monitoring (addressable):** implement procedures for monitoring log-in attempts and reporting discrepancies.
  - **Password Management (addressable):** implement procedures for creating, changing, and safeguarding passwords.

- **Security Incident Procedures**—implement policies and procedures to address security incidents. The Security Incident Procedures standard has one implementation specification:

  - **Response and Reporting (required):** identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity; and document security incidents and their outcomes.

- **Contingency Plan**—set policies and procedures for responding to an emergency or other occurrence that threatens EPHI. The Contingency Plan standard has five implementation specifications:

  - **Data Backup Plan (required):** establish and implement procedures to create and maintain retrievable exact copies of EPHI.

- **Disaster Recovery Plan (required):** establish (and implement as needed) procedures to restore any loss of data.
- **Emergency Mode Operation Plan (required):** establish (and implement as needed) procedures to continue critical business processes for protecting the security of EPHI while operating in emergency mode.
- **Testing and Revision Procedure (addressable):** implement procedures for periodic testing and revision of contingency plans.
- **Applications and Data Criticality Analysis (addressable):** assess the relative criticality of specific applications and data in support of other contingency plan components.

- **Evaluation**—perform periodic technical and nontechnical evaluations of security policies and procedures.
- **Business Associate Contracts (BAC) and Other Arrangements**—obtain satisfactory assurances that business associates with access to EPHI will appropriately safeguard it. The Business Associate standard has one implementation specification:

  - **Written Contract or Other Arrangement (required):** document satisfactory assurances of the adequate protection of the confidentiality, integrity, and availability of the EPHI through a written contract or other arrangement.[10]

2.3.4.2 Physical Safeguards

Physical safeguards are defined as the "physical measures, policies and procedures to protect a covered entity's electronic information systems and related buildings and equipment from natural and environmental hazards, and unauthorized intrusion."[11]

The Security Final Rule includes four standards under the heading "Physical Safeguards":

- **Facility Access Controls**—implement policies and procedures to limit physical access to electronic information systems and the facilities in which they are housed. The Facility Access Controls standard has four implementation specifications:

  - **Contingency Operations (addressable):** establish (and implement as needed) procedures that allow facility access in support of restoring lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency.

[10] For further information on the specifics required of a BAC or other arrangement, see 45 CFR 164.306, 164.308(b)(1), and 164.314(a).

[11] See Health Insurance Reform: Security Standards; Final Rule, 68 Fed. Reg. 8334 (2003), at 8376 (to be codified at 45 CFR section 160.304).

- **Facility Security Plan (addressable):** implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.
- **Access Control and Validation Procedures (addressable):** implement procedures to control and validate a person's access to facilities based on his or her role or function, including visitor control and control of access to software programs for testing and revision.
- **Maintenance Records (addressable):** implement policies and procedures to document repairs and modifications to the physical components of a facility, which are related to security (for example, hardware, walls, doors, and locks).

- **Workstation Use**—implement policies and procedures that specify the use, functions, and physical attributes of workstations that can access EPHI.
- **Workstation Security**—implement physical safeguards for all workstations that access EPHI.
- **Device and Media Controls**—implement policies and procedures that govern the internal movement and external transfer, receipt, and removal of hardware and electronic media. The Device and Media Controls standard has four implementation specifications:

  - **Disposal (required):** implement policies and procedures to address the final disposition of EPHI, and/or the hardware or electronic media on which it is stored.
  - **Media Reuse (required):** implement procedures for removal of EPHI from electronic media before the media are made available for reuse.
  - **Accountability (addressable):** maintain a record of the movements of hardware and electronic media and any person responsible thereof.
  - **Data Backup and Storage (addressable):** create a retrievable, exact copy of EPHI, when needed, before moving equipment.

2.3.4.3 Technical Safeguards

Technical safeguards are defined as "the technology and the policy and procedures for its use that protect EPHI and control access to it."[12]

The Security Final Rule includes five standards under the heading "Technical Safeguards":

- **Access Controls**—implement technical policies and procedures that restrict access to EPHI. The Access Controls standard has four implementation specifications:

  - **Unique User ID (required):** assign a unique name and/or number for identifying and tracking user identity.

[12] See Health Insurance Reform: Security Standards; Final Rule, 68 Fed. Reg. 8334 (2003), at 8376 (to be codified at 45 CFR section 160.304).

  - **Emergency Access Procedure (required):** establish (and implement as needed) procedures for obtaining necessary EPHI during an emergency.
  - **Automatic Logoff (addressable):** implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.
  - **Encryption and Decryption (addressable):** implement a mechanism to encrypt and decrypt EPHI.

- **Audit Controls**—implement hardware, software, and/or procedural mechanisms that record and examine activity occurring in information systems.
- **Integrity**—implement policies and procedures to protect EPHI from improper alteration or destruction. The Integrity standard has one implementation specification:

  - **Mechanism to Authenticate EPHI (addressable):** implement electronic mechanisms to corroborate that EPHI has not been altered or destroyed in an unauthorized manner.

- **Person or Entity Authentication**—implement procedures to confirm the identity of a person or entity seeking access to EPHI.
- **Transmission Security**—implement technical security measures to guard against unauthorized access to EPHI that is being transmitted over an electronic communications network. The Transmission Security standard has two implementation specifications:

  - **Integrity Controls (addressable):** implement security measures to ensure that transmitted EPHI is not improperly modified without detection until its disposal.
  - **Encryption (addressable):** implement a mechanism to encrypt EPHI whenever deemed appropriate.

2.3.5 Policies, Procedures, and Documentation Requirements

The Security Rule requires all covered entities to implement reasonable and appropriate policies and procedures to comply with the standards, implementation specifications, or other requirements of the HIPAA Security Final Rule. This requirement does not permit or excuse an action that violates any other standard, implementation specification, or other requirement of the Security Rule, the Privacy Rule, or any of the other Administrative Simplification provisions. A covered entity may change its policies and procedures at any time, provided that the changes are documented and are implemented in accordance with the HIPAA Security Final Rule.

Covered entities must also maintain the policies and procedures implemented to comply with the Security Rule in written (which may include electronic) form. If an action, activity, or assessment is required by this subpart to be documented, the covered entity must maintain a written (which may be electronic) record of the action, activity, or assessment. Documentation must be retained for six years from

the date of its creation or from the date when it was last in effect, whichever is later. Covered entities must make that documentation available to those persons responsible for implementing the procedures to which the documentation pertains. Covered entities must also review documentation periodically and update it as needed in response to environmental or operational changes affecting the security of the EPHI.

2.4 Relationship Between Privacy Final Rule and the Security Final Rule

Privacy and security are linked concepts, and the Privacy Final Rule and the Security Final Rule address some of the same business functions and practices (see Figure 4). In announcing the Security Final Rule, HHS stated, "[it] is likely that covered entities will meet a number of the requirements in the security standards through the implementation of the privacy requirements." For example, both the Privacy Final Rule and the Security Final Rule require all staff (including management) to receive training on the covered entity's HIPAA Administrative Simplification compliance policies and practices. The Privacy Final Rule also requires "appropriate administrative, technical, and physical safeguards to protect the privacy of PHI" and to "reasonably safeguard PHI from any intentional or unintentional use or disclosure that is in violation" of the Privacy Final Rule. For most entities, compliance with the far more specific requirements of the Security Final Rule will also satisfy the requirements of the Privacy Final Rule. Both rules also require entities to:

- Ensure that business associates and other third parties adequately safeguard EPHI;
- Appoint a single, identifiable individual to be accountable for compliance with HIPAA Administrative Simplification requirements; and
- Identify and secure all processes in which PHI is collected, stored, used, or transmitted.

Because these processes are similar in their requirements and required resources, most covered entities should conduct their assessments and compliance programs for HIPAA Security and Privacy in a coordinated fashion.

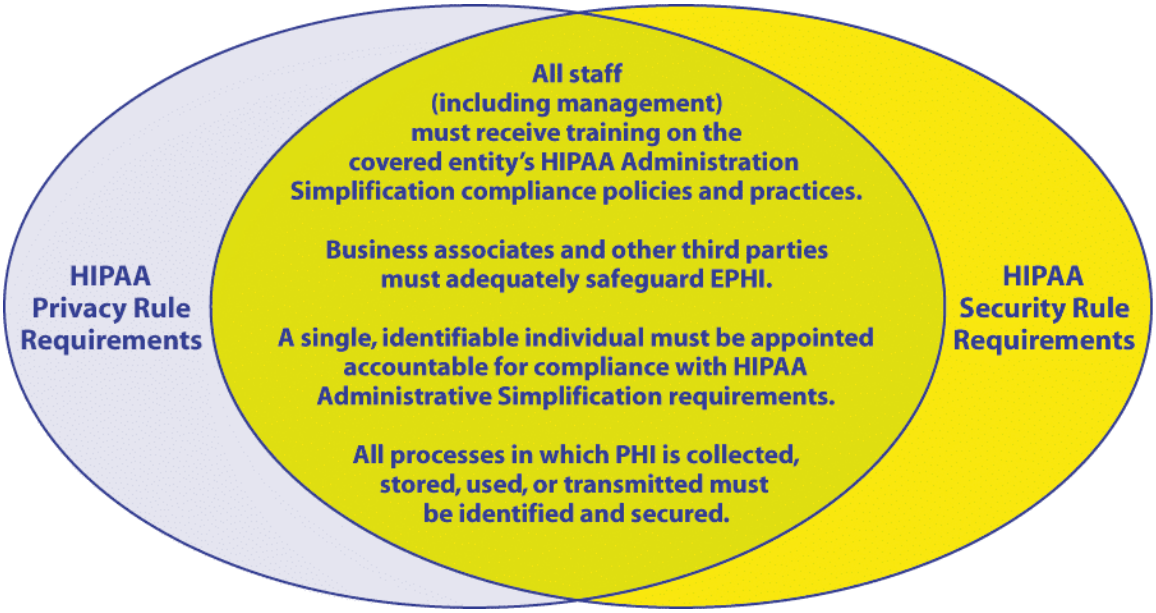

Figure 4. Overlap Between Requirements in the Privacy Final Rule and the Security Final Rule

2.5 Relationship Between the Security Final Rule and Other Security Requirements

Under FISMA, Congress linked information security with enterprise architecture. FISMA also updates requirements for federal agencies to perform a privacy impact assessment (PIA) on every information system and program, and codifies OMB's policy that agencies place clearly marked privacy policies on their websites.

By analyzing and comparing the requirements of the Security Final Rule and FISMA, it is possible to identify Security Final Rule standards that might be partly or wholly satisfied by compliance with FISMA. For these measures, compliance with FISMA may reduce or even satisfy the level of effort required to comply with the Security Final Rule.

Conducting HIPAA Security Final Rule and FISMA compliance activities in a coordinated manner may reduce duplication and the burden associated with compliance. In Section 3, we recommend that, as a preliminary step to organizing a HIPAA Administrative Simplification compliance program, covered entities conduct a gap analysis. Agencies would benefit from coordinating the activities that are covered by FISMA as well as HIPAA, and by paying special attention to compliance efforts that are covered by only the Security Final Rule.

Note also that certain FISMA activities, specifically the requirement to conduct PIAs, may also overlap with some HIPAA Privacy requirements. In addition, there are other security best practices that already may be in place within HHS and/or the OPDIVs that might partly or wholly satisfy the requirements of the Security Final Rule. A

coordinated review of the enterprise-wide security practices may reduce the level of effort and eliminate the duplication of effort required to comply with the Security Final Rule.

The National Institute of Standards and Technology (NIST) is another potential source of guidance for entities that are researching and developing a HIPAA Administrative Simplification compliance program. NIST is responsible for developing standards and guidelines, including minimum requirements, used by the OPDIVs in providing adequate information security for protecting HHS operations and assets. According to this mission, NIST's Information Technology Laboratory (ITL) has developed guidance to improve the efficiency of IT planning, implementation, management, and operation. These NIST Special Publications (SP) in the 800 series and Federal Information Processing Standards (FIPS) may be used by HHS to help provide a structured, yet flexible framework for selecting, specifying, employing, and evaluating the security controls in information systems. The information provided by these publications can make a significant contribution toward satisfying the requirements of FISMA and HIPAA.

NIST SP 800-66, *An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule*, summarizes the HIPAA security standards and explains some of the structure and organization of the Security Rule. NIST SP 800-66 also helps to educate readers about information security terms used in the HIPAA Security Rule and to improve understanding of the meaning of the security standards set out in the rule. Readers can use these publications for consideration in implementing the Security Rule.

NIST SP 800-66 also provides a crosswalk of the Administrative, Technical, and Physical standards and implementation specifications of the HIPAA Security Rule to the requirements of FISMA, which contains requirements relevant to the HHS Information Security Program. In many areas, both FISMA and the HIPAA Security Rule specify similar requirements.

3. HIPAA Administrative Simplification Compliance

There are numerous methods of performing the tasks associated with HIPAA Compliance. There is no one approach or single “best practice” that guarantees compliance with the HIPAA Privacy and HIPAA Security rules. However, these steps outline suggested activities covered entities could take in their situation, if applicable.

3.1 Step One: Determine Whether the Entity is Covered by HIPAA

The first step in HIPAA Administrative Simplification compliance is determining whether the entity under consideration is a covered entity under HIPAA. Appendix B cites a link to the tool at the CMS website that will assist a potentially HIPAA-covered entity in making this determination.

3.2 Step Two: Identify Applicable Information

Once step one is completed, the covered entity must identify all information that it collects, discloses, accesses, maintains, transmits, or manipulates that may be subject to either or both the Privacy Final Rule and Security Final Rule. Covered entities must determine whether any information under consideration qualifies as PHI for purposes of the Privacy Rule or qualifies as EPHI for the purposes of the Security Rule.

Covered entities should ask the following questions of each manager at each level of the organization:

- What activities or programs do you conduct?
- What information do you control or have access to that might be covered by the rules?
- How is the information obtained?
- How is the information stored?
- Who within your division has regular access to that information?
- What persons or external entities have regular access to or are routinely provided with that information?
- What persons or external entities request access to that information on an ad hoc basis?
- How is that information used, processed, or manipulated?

3.3 Step Three: Conduct Gap Analysis

Having identified what information, personnel, and processes must be considered in developing a compliance program, the covered entity should assemble and assess existing relevant policies that pertain to information security and privacy and to procedures and actual practices. The covered entity must then compare existing policies, procedures, and compliance efforts with those of the HIPAA rules. Government entities should incorporate the FISMA requirements into their analyses and crosswalks to determine whether efficiencies can be realized in complying with the two authorities.

Most covered entities will find it necessary to develop a comparison chart or tool to evaluate their current practices with those required by HIPAA. Many HIPAA-specific tools that may assist in this process are available commercially. Alternatively, covered entities may wish to develop their own tools, using common spreadsheet, word processing, or program management tools.

3.4 Step Four: Document Policies and Procedures

Both the Privacy Final Rule and the Security Final Rule require that covered entities develop policies and procedures to implement the rules' requirements. Policies and procedures must be documented and updated whenever changes are made.

Developing policies and procedures governing how PHI or EPHI is handled is the most critical step of developing a HIPAA Privacy and Security compliance process. Since the Privacy Final Rule and the Security Final Rule establish new requirements, existing HHS policies and procedures may not address handling PHI or EPHI to the required level.

In the Security Final Rule, HHS described developing and implementing policies and procedures as "the foundation on which all of the [other steps] depend." This step, then, should be conducted only after steps one through three have been completed, since step four depends on the thoroughness of the information collected in the preceding steps. As such, steps one through three must be accomplished with as much attention to detail and comprehensiveness as possible.

Once these three steps have been completed, the covered entity must draft new documents and modify existing ones as appropriate. Many entities will want to compile their privacy and security documents into a single guidance document for easy reference. The document should describe and provide guidance on all required privacy and security policies and practices and on any others that:

- Are specifically required of HHS;
- Address requirements and practices that are specific to the particular nature of HHS or its functions; and

- Relate to any other policies and practices that HHS, its security and privacy officers, and its management believe are necessary to the smooth and effective operation of HHS.

The covered entity should institute a process by which policies and procedures are regularly reviewed and periodically updated as necessary.

3.5 Step Five: Define Compliance Methodology

Once current gaps in an OPDIV's HIPAA Administrative Simplification compliance are identified, the OPDIV can design an overall compliance strategy that will permit it to address those gaps and be fully compliant by the deadlines for compliance discussed in Section 3.6.

Figure 5 provides a sample timeline for establishing a HIPAA Administrative Simplification compliance program that can be started at any quarter in the fiscal-year cycle and completed within a 12-month time frame.

In establishing their compliance programs, agencies should be mindful of the deadlines established by the various Administrative Simplification Rules, as summarized in Section 3.6. Until a covered entity completes steps one through four, it cannot know the number of areas that require attention, or schedule the time to address these problem areas.

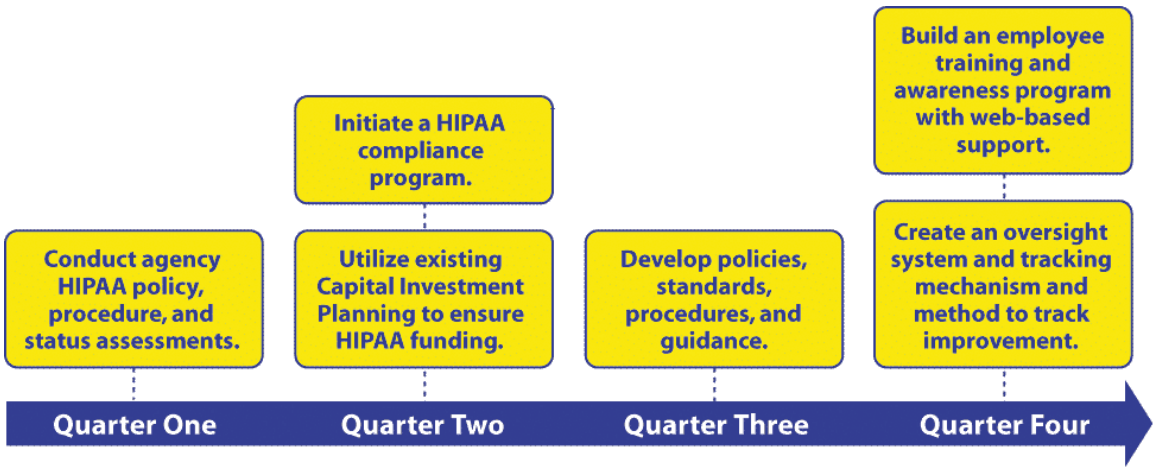

Figure 5. Sample Timeline for Establishing a HIPAA Administrative Simplification Compliance Program

3.6 HIPAA Timelines and Deadlines

Consistent with timeframes established by the HIPAA statute, the HIPAA Administrative Simplification Rules state the deadlines for covered entities to comply with each rule. These requirements are presented in Table 3.

Table 3. Standards and Deadlines for Compliance

Standards	Description	Deadline
Privacy	▸ Establishes rights of individuals regarding PHI and administrative requirements ▸ Standardizes authorized and required uses and disclosures ▸ Applies to records in all forms	April 14, 2003 (all covered entities except small health plans) April 14, 2004 (small health plans)
Transactions and Code Sets	▸ Standardizes format and data sets for electronic data interchange of health care information in certain transactions	Mandatory October 2002 Extensions granted to October 2003 October 15, 2002 (to submit a compliance extension form) October 16, 2002 (all covered entities except those that filed for an extension and are not a small health plan) April 16, 2003 (all covered entities must have started software and systems testing) October 16, 2003 (all covered entities that filed for an extension and small health plans)
Security	▸ Includes standards for: – Administrative procedures – Physical safeguards – Technical security provisions	April 21, 2005 (all covered entities except small health plans) April 21, 2006 (small health plans)
National Identifiers	▸ Standardizes identifiers for employers, providers, and health plans	Deadlines for Provider Identifier Standards and Health Plan Identifier Standards will be determined by the date of publication of the Final Rule governing each standard July 30, 2004 (Employer Identifier Standard—all covered entities except small health plans) August 1, 2005 (Employer Identifier Standard—small health plans)

3.7 Consequences of HIPAA Noncompliance

Penalties for covered entities that misuse protected health information are outlined in the text of the HIPAA statute. The following are the civil and federal penalties for violating the HIPAA privacy rules:

- **Civil penalties.** Health plans and health care providers and clearinghouses that violate these standards are subject to civil penalties. The maximum penalty that may be imposed on any person is $100 per violation, and the maximum aggregate penalty for identical violations during a calendar year is $25,000.
- **Federal criminal penalties.** Violations of HIPAA standards carry federal criminal penalties for covered entities that knowingly and improperly obtain, use or cause to be used, or disclose a unique health identifier or IIHI, or obtain information under false pretenses. Penalties would be higher for actions designed to generate monetary gain. Criminal penalties are set at up to $50,000 and one year in prison for obtaining or disclosing PHI; up to $100,000 and up to five years in prison for obtaining PHI under "false pretenses"; and up to $250,000 and up to 10 years in prison for obtaining or disclosing PHI with the intent to sell, transfer, or use it for commercial advantage, personal gain, or malicious harm.

On April 18, 2005, the Secretary of HHS proposed rules for imposing civil monetary penalties on entities that violate rules adopted by the Secretary to implement the Administrative Simplification provisions of HIPAA. The proposed rule would amend the existing rules relating to investigating noncompliance to make them apply to all of the HIPAA Administrative Simplification rules, rather than exclusively to the privacy standards. It would also amend the existing rules relating to the process for imposing civil monetary penalties. Among other matters, the proposed rules would clarify and elaborate on the investigation process, basis for liability, determination of the penalty amount, grounds for waiver, conduct of the hearing, and the appeal process. The final rules will be forthcoming after public comment and consideration by HHS.

Other potential consequences to noncompliance include:

- **Enforcement and oversight by HHS.** Enforcement and oversight of HIPAA rules may involve such actions as increased on-site investigations, requests for information and documents, and demands for written action plans if the extent or nature of noncompliance so warrants.
- **Loss of public trust.** Americans value privacy, and once public trust is lost, it’s difficult to regain.
- **Private lawsuits.** While HIPAA does not create a private right of action based on compliance or noncompliance with its provisions, its standards may serve as evidence of the measure of confidentiality protections that individuals may expect and demand of their providers.

Appendix A: Document Feedback Form

This form is for reviewer-suggested corrections, revisions, or updates and is intended to improve the usefulness of the document for possible inclusion in future versions. Please forward recommended changes and comments to the U.S. Department of Health and Human Services (HHS), Office of Chief Information Officer (OCIO).

By E-mail: <insert e-mail address>
Subject Line: Guidance Feedback
By Phone: <insert telephone number>

Document Title:
>
Section Number:
>
Category of Comment:

A	Administrative. Administrative comments correct what appear to be inconsistencies between sections, typographical errors, or grammatical errors.
S	Substantive. Substantive comments are provided because sections in the publication appear to be or are potentially incorrect, incomplete, misleading, or confusing.
C	Critical. Critical comments will cause non-concurrence with the publication if concerns are not satisfactorily resolved.
M	Major. Major comments are significant concerns that may result in a non-concurrence of the entire document if not satisfactorily resolved. This category may be used with a general statement of concern with a subject area, thrust of the document, etc., followed by detailed comments on specific entries in the publication which, taken together, constitute the concern.

Category	**Comment**

Name of Submitting Operating Division (OPDIV):
>
Your Name and Title:
>
Telephone:
>
E-mail:
>
Note: Use an additional blank sheet if needed.

Appendix B: References

Medicare Prescription Drug Improvement and Modernization Act of 2003 (Public Law 108-173).

Office of Management and Budget (OMB) Circular A-130, *Management of Federal Information Resources*, November 28, 2000.

OMB Circular A-130, *Management of Federal Information Resources, Appendix III, Security of Federal Automated Information Resources*, November 28, 2000.

Public Law 104-191, *Health Insurance Portability and Accountability Act of 1996* (HIPAA), August 21, 1996.

Public Law 107-347 [H.R. 2458], *The E-Government Act of 2002 Title III of this Act is the Federal Information Security Management Act of 2002 (FISMA)*, December 17, 2002.

National Institute of Standards and Technology (NIST), Special Publication (SP) 800-66, *An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule*, March 2005.

Resources: the *HIPAA Privacy Final Rule*

General Overview of Standards for Privacy of Individually Identifiable Health Information:
http://www.hhs.gov/ocr/hipaa/guidelines/overview.pdf

HIPAA Privacy Final Rule, available at the HHS Office for Civil Rights Web page "Medical Privacy – National Standards to Protect the Privacy of Personal Health Information".
http://hhs.gov/ocr/hipaa/finalreg.html

HIPAA Privacy Final Rule as it appears at Title 45 of the CFR, Part 164.
http://www.access.gpo.gov/nara/cfr/waisidx_02/45cfr164_02.html

Resources: the *HIPAA Security Final Rule*

View the HIPAA Security Final Rule at:
http://cms.hhs.gov/hipaa/

Resources: General HIPAA Resources

The Centers for Medicare & Medicaid Services' interactive tool for entities to determine whether they are covered by the HIPAA Administrative Simplification Rules:
http://www.cms.hhs.gov/hipaa/hipaa2/support/tools/decisionsupport/default.asp

Analysis and updates on HIPAA issues:
http://www.hipaadvisory.com/

Appendix C: Acronyms

BAC	Business Associate Contract
CFR	Code of Federal Regulations
CIO	Chief Information Officer
CMS	Centers for Medicare & Medicaid Services
CPO	Chief Privacy Officer
CSO	Chief Security Officer
DAA	Designated Approving Authority
EPHI	Electronic Protected Health Information
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act of 2002
HHS	Department of Health and Human Services
HIPAA	Health Insurance Portability and Accountability Act of 1996
ID	Identification
IIHI	Individually Identifiable Health Information
ISSO	Information Systems Security Officer
IT	Information Technology
ITL	Information Technology Laboratory
NIST	National Institute of Standards and Technology
OCIO	Office of the Chief Information Officer
OMB	Office of Management and Budget
OPDIV	Operating Division
PHI	Protected Health Information
PIA	Privacy Impact Assessment
SP	Special Publication
TPO	Treatment, payment, and operations
U.S.	United States
U.S.C.	United States Code

Appendix D: Glossary

Administrative Safeguards—administrative actions, policies, and procedures to manage the selection, development, implementation, and maintenance of security measures to protect EPHI and to manage the conduct of the covered entity's workforce in relation to protecting that information. See Health Insurance Reform: Security Standards; Final Rule, 68 Fed. Reg. 8334 (2003), at 8376 (to be codified at 45 CFR section 160.304).

Accountability—assigned responsibility for ensuring that entities operate in a lawful manner that protects against waste, fraud, and abuse of the health care system and its resources.

Addressable—as applied to an implementation specification of the Health Insurance Portability and Accountability Act of 1996 (HIPAA); describes a feature that is mandatory for all HIPAA-covered entities unless the entity concludes the measure is not "reasonable and appropriate" after conducting a required analysis. The covered entity may still be required to implement an equivalent measure if the equivalent measure is "reasonable and appropriate" and achieves the same end as the addressable implementation specification.

Affiliated Covered Entities—legally separated covered entities that are under common ownership or control and that have all designated themselves as single affiliated covered entities for the purposes of the Privacy and the Security rules (more precisely, those parts of the rules appearing at 45 CFR, Part 160, Subparts C and E). See Health Insurance Reform: Security Standards; Final Rule, 68 Fed. Reg. 8334 (2003) at 8376 (to be codified at 45 CFR section 164.105).

Authentication—the corroboration that a person is the one claimed. See NIST SP 800-66, *An Introductory Resource Guide for Implementing the HIPAA Security Rule* (to be codified at 45 C.F.R section 164.304).

Availability—the property that data or information is accessible and useable on demand by an authorized person. See Health Insurance Reform: Security Standards; Final Rule, 68 Fed. Reg. 8334 (2003) at 8376 (to be codified at 45 CFR section 160.304).

Business Associate—an entity independent of a HIPAA-covered entity that handles IIHI received from or provided to the covered entity. For examples of the kinds of activities conducted by business associates, as well as certain exceptions to the definition, see Standards for Privacy of Individually Identifiable Health Information; Final Rule, 65 Fed. Reg. 82462 (2000) at 82798 (to be codified at 45 CFR section 160.103).

Confidentiality—the property that data or information is not made available or disclosed to unauthorized persons or processes. See Health Insurance Reform:

Security Standards; Final Rule, 68 Fed. Reg. 8334 (2003) at 8376 (to be codified at 45 CFR section 164.304).

Contingency—an event with the potential to disrupt computer operations, thereby disrupting critical mission and business functions; for example, a power outage, hardware failure, fire, or storm. If the event is very destructive, it is often called a disaster. See NIST SP 800-12, *An Introduction to Computer Security: The NIST Handbook*.

Controls—the management, operational, and technical controls (safeguards or countermeasures) prescribed for an information system and the security controls in place or planned for meeting those requirements. See NIST FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*.

Countermeasures—actions, devices, procedures, techniques, or other measures that reduce the vulnerability of an information system. Synonymous with security controls and safeguards. See Committee for National Security System No. 4009.

Covered Entities—entities that must comply with any or all of the HIPAA rules; in this document that means certain providers, health plans, and health care clearinghouses that are regulated by the HIPAA Security Rule and/or the HIPAA Privacy Rule. See Standards for Privacy of Individually Identifiable Health Information; Final Rule, 65 Fed. Reg. 82462 (2000) at 82799 (to be codified at 45 CFR section
160.103).

Draft Rule—proposed requirements for compliance with a statute that is published for public comment by HHS empowered to do so by the relevant statute. Draft rules are not binding (e.g., covered entities will not be subject to penalty for not complying with a draft rule).

Electronic Protected Health Information —individually identifiable health information that is transmitted or maintained electronically. EPHI excludes information transmitted or maintained in media that are not electronic. Some other categories of information included in "IIHI" are excluded by PHI, such as some educational and employment records. For specifics, see Health Insurance Reform: Security Standards; Final Rule 68 Fed. Reg. 8334 (2003), at 8376 (to be codified at 45 CFR section 160.103).

Final Rule—the version of the specific requirements for compliance with a statute published by HHS empowered to do so by the relevant statute. Final Rules are published after a public comment period and are usually redrafted to account for issues identified by these public comments. The Final Security and Privacy Rules set compliance deadlines, after which they are enforceable by law.

Gap Analysis—a process that entities can use to identify the differences between the practices, policies, and procedures required by a law and current practices,

policies, and procedures; or to identify the differences between best practices and current practices, policies, and procedures.

Health Care Clearinghouse—a public or private entity that processes or facilitates the processing of health information received from another entity to or from a standard format. See Standards for Privacy of Individually Identifiable Health Information; Final Rule, 65 Fed. Reg. 82462 (2000) at 82799 (to be codified at 45 CFR section 160.103).

Health Care Provider—a provider of medical or health services and any other person who furnishes, bills, or is paid for health care in the normal course of business. See Standards for Privacy of Individually Identifiable Health Information; Final Rule, 65 Fed. Reg. 82462 (2000) at 82799 (to be codified at 45 CFR section 160.103).

Health Information—any information, whether oral or recorded, in any form or medium that is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and relates to the past, present, or future physical or mental health of an individual, the provision of health care to an individual, or the past, present or future payment of the provision of health care to an individual. See Standards for Privacy of Individually Identifiable Health Information; Final Rule, 65 Fed. Reg. 82462 (2000) at 82799 (to be codified at 45 CFR section 160.103).

Health Plan—an individual or group plan that provides or pays the cost of medical care. See Standards for Privacy of Individually Identifiable Health Information; Final Rule, 65 Fed. Reg. 82462 (2000) at 82799 (to be codified at 45 CFR section 160.103).

Hybrid Entity—a single legal entity that is a covered entity, whose business activities include both covered and noncovered functions, and that has designated one or more of its components as health care components in accordance with 45 CFR section 164.105(a)(2)(iii)(C). See Health Insurance Reform: Security Standards; Final Rule, 68 Fed. Reg. 8334 (2003), at 8375 (to be codified at 45 CFR section 164.103)

Implementation Specification—specific requirements or instructions for implementing a standard. See Standards for Privacy of Individually Identifiable Health Information; Final Rule, 65 Fed. Reg. 82462 (2000) at 82800 (to be codified at 45 CFR section 160.103).

Individually Identifiable Health Information—information that is a subset of health information, including demographic information collected from an individual, that identifies the individual or provides a reasonable basis to believe the information can be used to identify the individual. See Standards for Privacy of Individually Identifiable Health Information; Final Rule, 65 Fed. Reg. 82462 (2000) at 82804 (to be codified at 45 CFR section 160.103).

Information Security—protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide (1) confidentiality, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; (2) integrity, which means guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity; and (3) availability, which means ensuring timely and reliable access to and use of information. See NIST SP 800-66, *An Introductory Resource Guide for Implementing the HIPAA Security Rule* (to be codified at 44 U.S.C. section 3542).

Information System—an interconnected set of information resources under the same direct management control that shares common functionality. A system normally includes hardware, software, information, data, applications, communications, and people.[13] See NIST SP 800-66, *An Introductory Resource Guide for Implementing the HIPAA Security Rule* (to be codified at 45 CFR section 164.304).

Information Technology—any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. For purposes of this definition, equipment is used by an OPDIV whether the OPDIV uses the equipment directly or it is used by a contractor under a contract with the OPDIV which (1) requires the use of such equipment or (2) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. Information technology includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources. It does not include any equipment that is acquired by a federal contractor incidental to a federal contract. (Defined in the Clinger Cohen Act of 1996, §§5002, 5141 & 5142) See NIST SP 800-66, *An Introductory Resource Guide for Implementing the HIPAA Security Rule* (to be codified at 40 U.S.C. section 1401).

Integrity—the property that data or information has not been altered or destroyed in an unauthorized manner. See Health Insurance Reform: Security Standards; Final Rule 68 Fed. Reg. 8334 (2003), at 8376 (to be codified at 45 CFR section 164.304).

Measures—the management, operational , and technical controls (safeguards or countermeasures) prescribed for an information system and the security controls in place or planned for meeting those requirements. See NIST FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*.

[13] FISMA defines "information system" as "a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information." 44 U.S.C., Sec. 3502.

Mitigate—to select and implement security controls to reduce risk to a level acceptable to management, within applicable constraints. See NIST SP 800-12, *An Introduction to Computer Security: The NIST Handbook*.

Physical Safeguards—physical measures, policies, and procedures to protect a covered entity's electronic information systems, related buildings, and equipment from natural and environmental hazards, and unauthorized intrusion. See Health Insurance Reform: Security Standards; Final Rule 68 Fed. Reg. 8334 (2003) at 8376 (to be codified at 45 CFR section 164.304).

Protected Health Information—individually identifiable health information that is transmitted or maintained electronically or by using any other medium. Some categories of information included in "IIHI" are not considered to be PHI, such as some educational and employment records. See Health Insurance Reform: Security Standards; Final Rule 68 Fed. Reg. 8334 (2003) at 8376 (to be codified at 45 CFR section 160.103).

Portability—assurance of continuity of health care coverage for people who change jobs, which is required of health care coverage providers by provisions of HIPAA.

Required—addressable to a HIPAA implementation specification; mandatory for all covered entities to comply with HIPAA rules.

Risk—the level of impact on agency operations (including mission, functions, image, or reputation), agency assets, or individuals resulting from operating an information system given the potential impact of a threat and the probability of that threat occurring. See NIST SP 800-30, *Risk Management Guide for Information Technology Studies.*

Safeguard—an action, policy, or procedure intended to protect information or another asset. Both "standards" and "implementation specifications" are "safeguards."

Security—protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide (1) confidentiality, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; (2) integrity, which means guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity; and (3) availability, which means ensuring timely and reliable access to and use of information. See NIST SP 800-66, *An Introductory Resource Guide for Implementing the HIPAA Security Rule* (to be codified at 44 U.S.C. section 3542).

Security Controls—the management, operational, and technical controls (safeguards or countermeasures) prescribed for an information system and the security controls in place or planned for meeting those requirements. See NIST FIPS

199, *Standards for Security Categorization of Federal Information and Information Systems*.

Standard—a rule, condition, or requirement that must be met by a covered entity. See Standards for Privacy of Individually Identifiable Health Information; Final Rule, 65 Fed. Reg. 82462 (2000) at 82800 (to be codified at 45 CFR section 160.103).

Technical Safeguards—the technology used and the policy and procedures for its use that safeguard electronic-protected health information and control access to it. See Health Insurance Reform: Security Standards; Final Rule 68 Fed. Reg. 8334 (2003), at 8376 (to be codified at 45 CFR section 164.304).

Threat—the potential for a threat source to exercise (accidentally trigger or intentionally exploit) a specific vulnerability. See NIST SP 800-30, *Risk Management Guide for Information Technology Studies*.

Threat Source—either (1) a method targeted at the intentional exploitation of a vulnerability, or (2) a situation and method that may accidentally trigger a vulnerability. See NIST SP 800-30, *Risk Management Guide for Information Technology Studies.*

User—a person or entity with authorized access. See NIST SP 800-66*, An Introductory Resource Guide for Implementing the HIPAA Security Rule* (to be codified at 45 CFR section 164.304).

Vulnerability—a flaw or weakness in the design or implementation of an information system (including the security procedures and security controls associated with the system) that could be intentionally or unintentionally exploited to adversely affect an organization's operations or assets through a loss of confidentiality, integrity, or availability. See NIST SP 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*.

Appendix E: Information Security Program Documents

The HHS IT Security Program is supplemented by a series of HHS Information Security documents, including:

- HHS Information Security Program Policy
- HHS Information Security Program Handbook
- HHS Information Security Program Rules of Behavior
- Baseline Security Requirements Guide
- Certification and Accreditation (C&A) Guide
- Configuration Management Guide
- Contingency Planning for Information Security Systems Guide
- Critical Infrastructure Protection (CIP) Planning Guide
- Data Cryptography Guide
- Disaster Recovery Planning Guide
- Firewall Configuration Guide
- Health Insurance Portability and Accountability Act (HIPAA) Compliance Guide
- Incident Response Planning Guide
- Information Privacy Program Policy
- Information Privacy Program Handbook
- Information Technology (IT) Penetration Testing Guide
- IT Personnel Security Guide
- IT Physical and Environmental Security Guide
- IT Privacy Impact Assessment Guide
- IT Security Capital Planning Guide
- Machine-Readable Privacy Policy Guide
- Plan of Actions and Milestones (POA&M) Guide
- Risk Assessment Guide
- Security Test and Evaluation (ST&E) Planning Guide
- Web Security Guide
- Wireless Security Program Development Guide

Acknowledgements

Pat Higgins, Carla Dancy Smith, and Daniel Steinberg were instrumental in developing this document.