

HIPAA Security Rules

Guidance For

Immunization Registries

Version 1, October 2004



Prepared by AIRA Technical Committee
HIPAA Security Rule Task Group

Table of Contents

HIPAA Security Rule and Immunization Registries	3
HIPAA Privacy vs. Security Rules	4
Background on the Security Rule	5
Basics of the Security Rule	6
Key Concepts in the Final Security Rule	7
Security Risk Analysis	8
Best Practices to Achieve Compliance	9
Table 1 - Administrative Safeguards	11
Table 2 - Physical Safeguards	13
Table 3 - Technical Safeguards	14
Table 4 - Policy and Documentation Requirements	15
Table 5 – Security Risk Analysis Sample Method	16
Table 6 – Security Policy & Procedure Tracking Template	17
References	19

Purpose of this document:

This document is for educational purposes for AIRA and its members about the HIPAA Security Rule and its implications for immunization registries. These materials are provided as general guidance and do not constitute legal advice. Please use good judgment and review this with your internal Information Technology staff and legal resources, making any necessary changes to deal with the specifics of your own business environment.

Why is the HIPAA Security Rule important for Immunization Registries?

- Registry partners (health plans, clinics, insurance carriers, vendors, etc.) are Covered Entities (CEs) under HIPAA and will expect registries to meet high standards in storing and transmitting data. These partners play a major role in populating registries. They expect registries to take good care of their data, in accordance with federal rules and standards.
- The HIPAA Security Rule represents security best practices that can be reviewed and implemented by immunization registries.
- HIPAA requires that CEs permit other organizations to create, receive, maintain, or transmit PHI on their behalf *only if* the organizations can appropriately safeguard the information. CEs may be unwilling to exchange Protected Health Information (PHI) with organizations that do not adequately protect patient information. This will surely apply to most immunization registries.
- Parents are increasingly aware of their rights under HIPAA and want their children's information maintained in a safe and secure environment.
- CDC Registry Functional Standard #6 requires that registries have written security policies and procedures in place and implemented, including administrative and technical practices and physical safeguards to protect health care information. The policies and procedures should be consistent with applicable state and local laws and with the HIPAA Security Rule.
- CDC requires compliance with the above standard for registry certification.
- Non-compliant CEs may be discussed in public media (newspaper, radio, television) for not adequately protecting their customers' PHI. There is increased sensitivity.

HIPAA Privacy vs. HIPAA Security Rules – what's the difference?

The HIPAA *Privacy* Rule applies to protected health information (PHI) in "any form or medium". HIPAA Privacy Rules govern the use and disclosure of PHI. The rule was enacted April 14, 2003.

The HIPAA *Security* Rule covers PHI that is electronically stored or transmitted by covered entities. Health information on paper or oral is not addressed by the Security Rule, but Department of Health and Human Services (DHHS) has indicated that it may establish standards to protect health information in other, non-electronic media in a future rule.

The primary objective of the Security Rule is to protect the confidentiality, integrity, and availability of PHI when it is stored, maintained, or transmitted

The requirements of the HIPAA Privacy and Security Rules supplement each other in important ways:

- Both rules require covered entities to take appropriate and reasonable measures to safeguard PHI. The Security Rule aims at assuring the integrity and availability of electronic PHI also. As such, the Security Rule addresses issues such as data backup, disaster recovery and emergency operations.
- Both rules require regular training to make certain all employees understand both the importance of protecting PHI and the means by which they must do so.

HIPAA Security Rules – background

Health Insurance Portability and Accountability Act (HIPAA) regulations are divided into four Standards or Rules: (1) Privacy, (2) **Security (discussed in this document)**, (3) Identifiers and (4) Transactions and Code Sets. The Final Security Standard/Rule was released in February 2003.

<i>What</i>	The HIPAA Security Rule applies to electronic protected health information (PHI or EPHI), which is individually identifiable health information in electronic form.
<i>Why</i>	The HIPAA Security Rule is intended to protect the confidentiality, integrity and availability of protected health information (PHI). Health Information that is stored on a computer system that is transmitted across computer networks, including the Internet, is vulnerable and must be protected from hacker abuse and employee misuse, untrained personnel mishandling, exploitation by anyone that does not have a “need to know”, and unplanned system outages.
<i>Who</i>	Covered Entities (CEs) must comply with the Security Rule. These include health plans (HMOs, group health plans, etc.), health care clearinghouses (billing companies, etc.), or health care providers (doctors, dentists, hospitals, etc.) who transmit any PHI. In addition, CEs may be required establish a business associate agreement with organizations that have access to the CE’s electronic PHI or to whom the CE discloses electronic PHI. CEs must assure that business associates reasonably and appropriately safeguard the electronic PHI, however, business associates are not required to comply with each specification of the Security Rule unless they are CEs in and of themselves.
<i>How</i>	CEs must maintain reasonable safeguards to protect the confidentiality, integrity, and availability of their PHI against risks. The details of these HIPAA safeguards and implementation strategies are in Tables 1, 2, 3.
<i>When</i>	The final Security Rule became effective as of April 21, 2003. Most CEs must be in compliance by April 21, 2005; small health plans (those with annual receipts of \$5 million or less) have until April 21, 2006.

Basics of the HIPAA Security Rule

The new rule on the security boils down to four sets of standards intended for CEs and the business associates, partners in data sharing, etc.

The Security Rule's requirements or standards are divided into:

- Administrative Safeguards: 12 required, 11 addressable [Table 1]
- Physical Safeguards: 4 required, 6 addressable [Table 2]
- Technical Safeguards: 4 required, 5 addressable [Table 3]
- Policies and Procedures and Documentation of the above [Table 4]

These safeguard categories are further divided into standards and implementation specifications that provide instructions.

Where the proposed rule laid out a set of safeguards that CEs would need to implement, the final rule distinguishes between "required" and "addressable" specifications. CEs have discretion on how and whether to implement addressable specifications. However, CEs are required to document and explain any addressable safeguards it chooses to scale down or forgo, and must implement an equivalent alternative measure if it is reasonable and appropriate in its environment.

While many organizations have proposed elements of a security model, DHHS has stated that it believes the HIPAA Security Rule establishes the *only "comprehensive, scalable, and technology-neutral standard" to safeguard electronically maintained or transmitted information.*

The Security Rule establishes a national "minimum standard" for security of electronic health information. Covered Entities may for various reasons need or want to exceed that. For example, state law, which is not preempted unless it is less stringent, may establish a higher benchmark. Organizations may choose to implement safeguards that exceed the HIPAA standards - and, in fact, may find that their business strategies require stronger protections.

Key concepts in the Final HIPAA Security Rule

Scalability - All sizes of CEs must be able to comply with the rule, from the one-person doctor office to the insurance company with thousands of employees.

Technology neutral - The published rule does not dictate specific solutions that would be usable by all the affected entities because they are "so varied in terms of installed technology, size, resources and relative risk." The rule further notes "many comments also supported the concept of technological neutrality, which would afford affected entities the flexibility to select appropriate technology solutions and to adopt new technology over time."

Internal and external security threats - CEs must protect their PHI against both internal and external threats.

Security Threats – activities that are associated with unauthorized access, either accidental or intentional, to PHI. Security threats can take the form of people (workforce, outside hackers, etc.) or events (storms, fire, floods, etc.)

Risk analysis – This is the cornerstone of the final security rule. CEs must regularly conduct thorough and accurate risk analysis. The risk analysis should determine a baseline measure of security gaps. CEs are expected to determine if an implementation specification is reasonable and appropriate. This does not imply that organizations are given complete discretion to make their own rules. [Table 5]

Reasonableness - CEs must take appropriate measures to mitigate all reasonably anticipated risks to their PHI. "Reasonableness" and "appropriateness" are not specifically defined. How security requirements are to be satisfied and which technologies to use are "business decisions that each entity [has] to make ... reviewing and modifying the measures as needed to continue the provision of reasonable and appropriate protections."

Documentation – CEs must formally document and approve a wide variety of security processes, policies, and procedures.

Ongoing compliance - CEs must provide regular security training and awareness to its workforce and revise its security policies and procedures as needed.

Security Risk Analysis

Determine:

- What needs to be protected – data, hardware, software? Do an inventory.
- What are the internal and external interfaces of information systems?
- What are the current technical controls? (e.g., hardware or software access controls mechanisms, encryption, audit trail, alarm). The analysis should define what security controls are being used to protect PHI, how they're being used, and any gaps between how they're being used and how they're supposed to be used.
- What are the possible threats?
 - Natural: Floods, earthquakes, tornados, etc.
 - Human: Unintentional (incorrect data entry or accidental deletion of data)
 - Human: Intentional (denial of service attack, installing malicious software)
 - Environmental: Power failures, hazardous material spill, etc.
- What are the vulnerabilities that can be exploited by the threats? Vulnerability sources include review of information systems, audit reports, and information system test and evaluation reports. See References for web links.
- What is the likelihood of the threat?
- What is the impact, consequence, or loss to the organization?
- What are the non-technical controls? (e.g., security policies, employee training)

The analysis should reveal:

Technical and non-technical controls you need to reduce the risk

Refer to Tables 1-4 for HIPAA Security Standards and related Implementation Specifications

Table 5 shows a sample method tool to help calculate security risk.

Best practices toward achieving compliance with the HIPAA Security Rule

1. **Become familiar with the rule** and how it applies to your registry and your relationship with CEs. Providers, plans, insurers, vendors, etc. play a major role in populating registries. They expect registries to take good care of their data, in accordance with federal rules and standards. Understand Required vs. Addressable standard. [Tables 1, 2, 3,4]
2. **Form a team to help with security efforts** including staff from information technology organizations. Designate a security lead.
3. **Obtain Management Support:** If possible, managers should be project sponsors for Security Rule compliance projects.
4. **Conduct an inventory of your registry data:** It is important to identify and document the flow of registry data in, out, and throughout your organization.
 - Do you regularly exchange data with certain providers or health plans?
 - Do other internal data systems (i.e., Vital Records, county health data systems) regularly submit data to the registry?
 - Does your registry regularly send data over the Internet?
5. **Gap and Risk Analysis:** "Risk" can be simply defined as *"the likelihood that a specific threat will exploit a certain vulnerability, and the resulting impact of that event."* Risk analysis is an analytical approach that identifies and assesses risks and provides recommendations to reduce risk to a reasonable and appropriate level. Determine your own organization's vulnerabilities and respective levels of risk. Establish a baseline, and document your results and decisions. [Table 5]
6. **Determine What is Appropriate and Reasonable** - Use risk analysis as the basis for developing a baseline assessment and implementing appropriate and reasonable protections for your entity. The Security Rule does not expect CEs to protect their electronic PHI against all possible risks or to have "perfect" security. Nor does the Security Rule assume that CEs have unlimited time, money and resources for protecting electronic PHI. Rather, the rule expects CEs anticipate risks to the PHI and to develop and implement security measures.
7. **Establish and Implement Security Policies and Procedures** - Identify and define what security policies you need to develop and implement to ensure that your data are protected from internal and external threats. The Security Rule requires CEs to document a wide variety of security policies and procedures. [Table 6]

Best Practices (continued)

8. **Involve and Educate the Workforce** - Make sure all employees are trained on their roles related to electronic PHI, and on threats and vulnerabilities and how to report them. Soliciting workforce member feedback and review on proposed security policies and processes could also help.
9. **Document Remediation** - Document security events and threats to improve processes for the future. This includes detailing how each addressable specification is handled.
10. **Prepare for ongoing compliance** - Regularly conduct security awareness training and review security documentation, policies, procedures, processes, and controls with the understanding that they must be modified as necessary.

Table 1

Administrative Safeguards §164.308		
Administrative safeguards make up 50% of the Security Rule's standards. They require documented policies and procedures for managing day-to-day operations, the conduct and access of workforce members to PHI, and the selection, development, and use of security controls. CEs must assign responsibility for oversight to a single person. That person must manage the overall security process, implement a contingency plan, conduct training, develop external contracts as needed, and evaluate the program.		
HIPAA Standard	Implementation Specifications	♦
<p>Security management process</p> <p>An overall requirement to implement policies and procedures to prevent, detect, contain, and correct security violations. This includes periodic system activity review of internal security controls, logs, access reports and incident tracking.</p>	<ul style="list-style-type: none"> <input type="checkbox"/> Risk Analysis <input type="checkbox"/> Risk Management <input type="checkbox"/> Sanction Policy <input type="checkbox"/> Information system activity review 	<p>R R R R</p>
<p>Assigned security responsibility</p> <p>A single individual must be designated as having overall responsibility for the security of PHI, and the implementation of policies and procedures.</p>	<ul style="list-style-type: none"> <input type="checkbox"/> Assign responsibility 	<p>R</p>
<p>Workforce Security</p> <p>Policies, procedures, and processes that ensure only properly-authorized workforce members have access to PHI.</p>	<ul style="list-style-type: none"> <input type="checkbox"/> Authorization or supervision <input type="checkbox"/> Workforce clearance procedure <input type="checkbox"/> Termination procedures 	<p>A A A</p>
<p>Information Access Management</p> <p>Policies, procedures, and processes for authorizing, establishing, and modifying access to PHI. If a healthcare clearinghouse is part of a larger organization, the clearinghouse must protect electronic PHI from unauthorized access by the larger organization.</p>	<ul style="list-style-type: none"> <input type="checkbox"/> Isolate health care clearinghouse functions <input type="checkbox"/> Access authorization <input type="checkbox"/> Access modification 	<p>R A A</p>

♦ R= required standard; S=Addressable standard

Table 1 (continued)		
HIPAA Standard	Implementation Specification	*
<p>Security Awareness and Training</p> <p>Security awareness and training program for a CE's workforce must be developed and implemented.</p>	<ul style="list-style-type: none"> <input type="checkbox"/> Security Reminders <input type="checkbox"/> Virus Protection <input type="checkbox"/> Log-in monitoring <input type="checkbox"/> Password management 	<p>A A A A</p>
<p>Security Incident Procedures</p>	<ul style="list-style-type: none"> <input type="checkbox"/> Policies and Procedures 	<p>R</p>
<p>Contingency plan</p> <p>Documented plan to maintain continuity of operations in an emergency or disaster, and to enable recovery of data following disaster.</p>	<ul style="list-style-type: none"> <input type="checkbox"/> Data backup plan <input type="checkbox"/> Disaster Recovery Plan <input type="checkbox"/> Emergency mode Operation Plan <input type="checkbox"/> Testing and Revision Procedure <input type="checkbox"/> Applications, Data Criticality Analysis 	<p>R R R A A</p>
<p>Evaluation</p> <p>Perform a periodic technical and non technical evaluation based on standards implemented and any changes as a response to environmental or operational threats.</p>	<ul style="list-style-type: none"> <input type="checkbox"/> Periodic review 	<p>R</p>
<p>Business Associate Contracts</p> <p>An agreement between a covered entity and all other entities with whom health information is shared, to "protect the integrity and confidentiality" and safeguard the data they exchange.</p>	<ul style="list-style-type: none"> <input type="checkbox"/> Written Contract, Other Arrangements 	<p>R</p>

Table 2

Physical Safeguards §164.310		
This category of security standards is focused on preventing unauthorized individuals from gaining access to electronic information. Limiting access to PHI improves security. CEs must protect the facility, workstations, and the data within the workstations (includes laptops and portable computing devices). Limiting access and protecting PHI becomes more difficult as mobility increases.		
HIPAA Standard	Implementation Specification	♦
<p>Facility Access Controls</p> <p>An overall requirement to implement policies, procedures, and processes that limit physical access to electronic information systems while ensuring that properly-authorized access is allowed.</p>	<ul style="list-style-type: none"> <input type="checkbox"/> Contingency operations <input type="checkbox"/> Facility Security Plan <input type="checkbox"/> Access control, validation procedures <input type="checkbox"/> Maintenance records 	<p>A A A A</p>
<p>Workstation Use</p> <p>Implement policies and procedures that specify the proper functions to be performed and the physical attributes of the surroundings of a class of workstation used to access PHI.</p>	<ul style="list-style-type: none"> <input type="checkbox"/> Procedures for workstation functions 	<p>R</p>
<p>Workstation Security</p> <p>Implement physical safeguards for all workstations that can access PHI in order to limit access to only authorized users.</p>	<ul style="list-style-type: none"> <input type="checkbox"/> Procedures for workstation security 	<p>R</p>
<p>Device and Media Controls</p> <p>Formal procedures for controlling and tracking the handling of hardware and software, and for data backup, storage and disposal. This includes the receipt and removal of hardware and electronic media that contain PHI into and out of a CE, and the movement of those items within a CE.</p>	<ul style="list-style-type: none"> <input type="checkbox"/> Data Disposal <input type="checkbox"/> Media Reuse <input type="checkbox"/> Accountability <input type="checkbox"/> Data Backup and Storage 	<p>R R A A</p>

♦ R= required standard; S=Addressable standard

Table 3

Technical Safeguards §164.312		
Technology safeguards are often governed by the particular technologies and data systems in use. CEs are expected to balance the need for timely access to needed health information with the need to protect its confidentiality and integrity. Organizations that transmit health information over open networks must keep it from being easily intercepted by third parties via external entry points. CEs must manage access to PHI while at rest, ensure that it's protected while in transit, and gain access to it during an emergency situation.		
HIPAA Standard	Implementation Specification	♦
<p>Access controls</p> <p>Implement technical policies and procedures to allow access to information systems only to those persons that have been granted access under Information Access Management.</p>	<ul style="list-style-type: none"> <input type="checkbox"/> Unique user identification <input type="checkbox"/> Emergency access procedure <input type="checkbox"/> Automatic logoff <input type="checkbox"/> Encryption and decryption 	<p>R R A A</p>
<p>Audit controls</p> <p>System mechanisms that record and monitor activity.</p>	<ul style="list-style-type: none"> <input type="checkbox"/> Procedures to examine system activities 	<p>R</p>
<p>Integrity</p> <p>Policies, procedures, and processes that protect PHI from improper modification or destruction.</p>	<ul style="list-style-type: none"> <input type="checkbox"/> Mechanism to authenticate electronic PHI 	<p>A</p>
<p>Person or Entity authentication</p> <p>Policies, procedures, and processes that verify persons or entities seeking access to PHI are who or what they claim to be.</p>	<ul style="list-style-type: none"> <input type="checkbox"/> Verification procedures 	<p>R</p>
<p>Transmission security</p> <p>Policies, procedures, and processes that prevent unauthorized access to PHI that is being transmitted over an electronic communications network (e.g., the Internet).</p>	<ul style="list-style-type: none"> <input type="checkbox"/> Integrity Controls <input type="checkbox"/> Encryption 	<p>A A</p>

♦ R= required standard; S=Addressable standard

Table 4

Policy and Procedure and Documentation Requirements §164.316

CEs must maintain all documentation (e.g., policies, procedures) required by the Security Rule for a period of six years from the date of its creation or the date when it last was in effect, whichever is later.

Such documentation must be made available to the workforce members responsible for implementing the policies and procedures.

Additionally, CEs must periodically review such documentation and revise and update it as needed to ensure the confidentiality, integrity, and availability of PHI.

Table 5 - Example of a tool used for Security Risk Analysis

Likelihood Level	Likelihood Definition
High	Threat is highly capable, motivated, or likely and current security controls are ineffective.
Medium	The threat is high but controls are in place that may impede the threat.
Low	The threat source is not high, controls are in place to significantly impede the threat.

Magnitude of Impact Level	Impact Definition
High	Exercise of the vulnerability may result in costly loss of data or significantly violate an organization's mission or reputation. Security controls should be implemented or improved as quickly as possible.
Medium	Exercise of the vulnerability may result in loss of data or impede an organization's mission. Security controls should be implemented or improved in a reasonable amount of time.
Low	Exercise of the vulnerability may result in relatively small loss of data or may noticeably affect an organization's mission or reputation. The impact is short term. Existing security controls are likely adequate or the risk is acceptable.

Example of risk score method (many other methods are available):

IMPACT	High	3	6	9
	Medium	2	4	6
	Low	1	2	3
Likelihood		Low	Medium	High

The higher the number, the greater the risk.

Example of how risk score can be used:

The Assessment of Contingency Plan reveals the following:

- Data backup plan is outdated, and there is no emergency mode operation plan.
- The likelihood of a data threat is Medium but the Impact is High.
- The risk score is 6.

The Security Team has determined that any standard above a risk level of 2 or 3 needs to have priority attention for security policies and procedures.

Table 6 Worksheet: Security Policy and Procedure Tracking

R = required element of HIPAA Security Rule for Covered Entities

A = addressable; implement if reasonable or document alternative

Title		Team Members	Status P=in progress A=approved
Administrative Safeguards			
Security Management Process <ul style="list-style-type: none"> a. Risk analysis assessment b. Risk Management Plan c. Sanction Policy d. Information system activity review (audits logs, access reports, incident reports) 	R R R R		
Assigned security responsibility <ul style="list-style-type: none"> a. Designate a team and a security lead 	R		
Workforce security <ul style="list-style-type: none"> a. Authorization and/or supervision procedures b. Workforce clearance procedures c. Termination procedures 	A A A		
Information Access Management <ul style="list-style-type: none"> a. Isolate health care clearinghouse function b. Access authorization procedures c. Access modification procedures 	R A A		
Security Awareness and Training <ul style="list-style-type: none"> a. Security Reminders b. Virus Protection c. Log-in monitoring d. Password management 	A A A A		
Security Incident Procedures <ul style="list-style-type: none"> i. Response and reporting 	R		
Contingency Plan <ul style="list-style-type: none"> a. Data backup plan b. Disaster Recovery Plan c. Emergency mode Operation Plan d. Testing and Revision Procedure e. Applications, Data Criticality Analysis 	R R R A A		

Title		Team Members	Status P=in progress A=approved
Evaluation a. Periodic review by internal or external team	R		
Business Associate Contracts or Data Sharing Agreements with partners a. Written contract or other agreement	R		
Physical Safeguards			
Facility access controls a. Contingency operations procedures b. Facility Security Plan c. Access control, validation procedures d. Maintenance records documentation	A A A A		
Workstation Use a. Procedures for workstation security	R		
Workstation Security a. Physical safeguards	R		
Device and Media Controls a. Data Disposal Procedures b. Media Reuse Procedures c. Accountability and records d. Data Backup and Storage Procedures	R R A A		
Technical Safeguards			
Access Control a. Unique user identification tracking b. Emergency access procedure c. Automatic logoff procedures d. Encryption and decryption mechanisms	R R A A		
Audit controls a. Procedures to examine system activities	R		

Title		Team Members	Status P=in progress A=approved
Integrity controls a. Mechanism to authenticate electronic PHI to ensure that it is not altered or destroyed in an unauthorized manner	A		
Person or Entity Authentication a. Methods to determine that an entity is who it claims to be	R		
Transmission Security a. Integrity Control Measures b. Encryption Mechanisms	A A		

References

Federal Register, 45 CFR Parts 160, 162 and 164
 Health Insurance Reform: Security Standards; Final Rule
 February 20, 2003

National Institute of Standards and Technology (NIST) SP 800-30, "*Risk Management Guide for Information Technology Systems*", chapters 3 and 4, January 2002
<http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf>

NIST vulnerability database - Vulnerability sources include system and data owner questionnaires, on-site review of information systems, audit reports, and information system test and evaluation reports.
<http://icat.nist.gov>

Valuable resources include the Workgroup for Electronic Data Interchange (WEDI) and the Strategic National Implementation Project (SNIP), a collaborative healthcare industry-wide process resulting in the implementation of standards.
<http://wedi.org/snip/public/articles/>

This publication was prepared by the American Immunization Registry Association (AIRA), an organization founded in July 1991 to advocate for the support of immunization registry development.

Production of this publication was supported by the Cooperative Agreement Number U38/CCU222349 from the Centers of Disease and Control (CDC). Its contents are solely the responsibility of AIRA and do not necessarily represent the official views of the CDC.



American Immunization Registry Association (AIRA)
c/o Citywide Immunization Registry
NYC Department of Health and Mental Hygiene
125 Worth Street, CN 64R
New York, NY 10013
(212) 676-2325

www.immregistries.org