
WEDI - Strategic National Implementation Process (SNIP)

HIPAA Security White Papers



SNIP

**HIPAA Security White Papers
July 2003**

SNIP Security and Privacy Workgroup

Workgroup for Electronic Data Interchange

12020 Sunrise Valley DR., Suite 100, Reston, VA. 20191

(t) 703-391-2716 / (f) 703-391-2759

© 2003 Workgroup for Electronic Data Interchange, All Rights Reserved

Contents

- HIPAA Security White Papers..... 1**
- Disclaimer..... 1
- HIPAA Security Regulation Outline 1
- Part 160 – General Administrative Requirements 2
- Part 164 – Security and Privacy 2
- HIPAA Security Regulations Require Covered Entities to Take Specific Steps to Protect Electronic PHI (ePHI) 3
- Serious Civil and Criminal Penalties for HIPAA Noncompliance 3
- Security of Paper-Based PHI..... 3
- HIPAA Privacy Papers 4
- HIPAA Security Websites 5
- Conclusion 5
- Other Sources of Information 5
- Acknowledgements 5

HIPAA Security White Papers

Disclaimer

This document is Copyright © 2003 by The Workgroup for Electronic Data interchange (WEDI). It may be freely redistributed in its entirety provided that this copyright notice is not removed. It may not be sold for profit or used in commercial documents without the written permission of the copyright holder. This document is provided “as is” without any express or implied warranty.

While all information in this document is believed to be correct at the time of writing, this document is for educational purposes only and does not purport to provide legal advice. If you require legal advice, you should consult with an attorney. The information provided here is for reference use only and does not constitute the rendering of legal, financial, or other professional advice or recommendations by the Workgroup for Electronic Data Interchange. The listing of an organization does not imply any sort of endorsement and the Workgroup for Electronic Data Interchange takes no responsibility for the products, tools, and Internet sites listed.

The existence of a link or organizational reference in any of the following materials should not be assumed as an endorsement by the Workgroup for Electronic Data Interchange (WEDI), or any of the individual workgroups or sub-workgroups of the Strategic National Implementation Process (SNIP).

Document is for Education and Awareness Use Only

The HIPAA Security and Privacy requirements are designed to be ubiquitous, technology neutral and scalable from the very largest of health plans, to the very smallest of provider practices. As the Privacy Rule and Security Rule relate to policies and procedures, many covered entities will find compliance not an application of exact template processes or documentation, but rather a remediation based on a host of complex factors unique to each organization.

HIPAA Security Regulation Outline

There have been a series of steps by the Department of Health and Human Services over a series of years resulting in the Security Final Rule published in the Federal Register on February 20, 2003, to get to this integrated and updated security requirements and implementation standards.

There are two Parts to the HIPAA regulations that outline the security standards and implementation specifications, 45 CFR 160, the general administrative requirements, and 45 CFR 164, Subpart A – General Provisions, and Subpart E – Privacy of the Individually Identifiable Health Information.

Part 160 – General Administrative Requirements

Subpart A – General Provisions

- 160.101 Statutory basis and purpose.
- 160.102 Applicability.
- 160.103 Definitions.
- 160.104 Modifications.

Subpart B – Preemption of State Law

- 160.201 Applicability.
- 160.202 Definitions.
- 160.203 General rule and exceptions.
- 160.204 Process for requesting exception determinations.
- 160.205 Duration of effectiveness of exception determinations.

Subpart C – Compliance and Enforcement

- 160.300 Applicability.
- 160.302 Definitions.
- 160.304 Principles for achieving compliance.
- 160.306 Complaints to the Secretary.
- 160.308 Compliance reviews.
- 160.310 Responsibilities of covered entities.
- 160.312 Secretarial action regarding complaints and compliance reviews.

Part 164 – Security and Privacy

Subpart A – General Provisions

- 164.102 Statutory basis.
- 164.103 Definitions.
- 164.104 Applicability.
- 164.105 Organizational requirements.
- 164.106 Relationship to other parts.

Subpart C – Security Standards for the Protection of Electronic Protected Health Information.

- 164.302 Applicability.
- 164.304 Definitions.
- 164.306 Security standards: General rules.
- 164.308 Administrative safeguards.
- 164.310 Physical safeguards.
- 164.312 Technical safeguards.
- 164.314 Organizational requirements.
- 164.316 Policies and procedures and documentation requirements.
- 164.318 Compliance dates for the initial implementation of the security standards.

HIPAA Security Regulations Require Covered Entities to Take Specific Steps to Protect Electronic PHI (ePHI)

All Security requirements can be defined as one of three basic safeguards; Administrative, Physical and Technical. Some of the detailed basic steps are listed below and include, but are not limited to:

- Adopt policies and procedures to protect electronic of protected health information;
- Adopt policies and procedures to protect the security of patient information, including:
 - a disaster recovery plan;
 - policy on workstation use; and
 - procedures for the storage and disposal of health information;
- Designate a security official;
- Develop and implement data access control procedures;
- Sign or amend contracts with business associates to protect the confidentiality of protected patient data exchanges electronically;
- Provide confidentiality awareness training to your personnel;
- Implement technical mechanisms to prevent unauthorized access;
- Establish a reporting and response system for confidentiality violations; and
- Develop a sanctions policy for the discipline of violations by your employees, agents and contractors.

Civil and Criminal Penalties for HIPAA Noncompliance

- General noncompliance with the HIPAA security, privacy, and EDI regulations: \$100.00 per violation and up to \$25,000.00 per person for all identical violations in a calendar year.
- Specific noncompliance with the privacy regulations:
 - \$50,000.00 fine and imprisonment for one year if you knowingly obtain or disclose individually identifiable health information;
 - \$100,000.00 fine and imprisonment for five years if you knowingly obtain or disclose individually identifiable health information under false pretenses; and
 - A maximum fine of \$250,000.00 and/or up to ten years imprisonment if you obtain or disclose individually identifiable health information with the intent to sell, transfer or use the information for commercial advantage, personal gain or malicious harm.

Other risks of noncompliance include exposure to lawsuits for breach of confidentiality, loss of accreditation, audits by the Centers for Medicare and Medicaid Services (CMS) and damage to business interests and reputation, loss of reputation, loss of patients or members.

Security of Paper-Based PHI

The Security Final Rule covers PHI maintained in an electronic format. Keep in mind that the Privacy Final Rule also requires that paper-based PHI be kept secure [see §164.530(c)(1)]. Accordingly, the security white papers address paper-based as well as electronic-based PHI.

HIPAA Privacy Papers

The SNIP Security and Privacy Work Group has an introduction and a number of white papers reviewing a number of HIPAA privacy and security implementation issues.

Currently, three new White Papers reflect the requirements of the Final Rule:

- Introduction to Security
- Addressable vs. Required
- NIST SP800 Documents

In addition, three security white papers completed prior to the release of the Final Rule are under revision:

- Security Policies and Procedures
- Evaluation
- Audit Trails

The Security and Privacy Workgroup has launched a number of sub-workgroups to complete a series of six new white papers:

Introduction to Security: This White Paper will briefly define what is security, the goals of security, how to measure security, and provide a general conceptual framework for thinking about how to approach security in the health care industry.

Risk Assessment: This White Paper will outline the how to develop a threat model and response model aligned with business goals and obligations, focus on what is required by the Security Rule, and explore the cost/risk tradeoff and the potential for litigation

E-mail and Encryption: This White Paper will address what is the state of the technology and what secure e-mail community-based demonstrations are ongoing.

Security Outside the Enterprise: This White Paper will look at the question of given the security levels within my enterprise, how and under what circumstances can I provide PHI to other CEs, BAs, and other entities? Is the lowest level of security among the entities acceptable, reasonable, and appropriate?

Small Practice Security Implementation: This White Paper will parallel the Small Practice Privacy Implementation White Paper and provide specific guidance regarding how a small practice should approach the Security Rule and what they have to do to comply with the Rule.

Enforcement Rule: This White Paper will explore the provisions of the new Enforcement Rule

Finally, the Security and Privacy Workgroup is considering development of a security tools resource document.

HIPAA Security Websites

SNIP Security and Privacy White Papers

http://www.wedi.org/snip/public/articles/dis_publicDisplay.cfm?docType=6&wptype=2

Regional SNIP Efforts

<http://www.wedi.org/snip/public/articles/index%7E2.htm>

CMS Administrative Simplification

<http://www.cms.hhs.gov/hipaa/hipaa2/default.asp>

National Institute of Standards and Technology (NIST)

<http://www.nist.gov>

Conclusion

You are invited to participate in the development of the Security White Papers. To get involved please contact Kristin Becker at KristinBecker1@aol.com.

You also are invited to join the SNIP Security and Privacy Work Group privacy listserv to ask your peers about their privacy work at <http://subscribe.wedi.org>.

Other Sources of Information

Any other URLs, papers or organizations that would be a resource for this subject need to be identified and included in the paper.

WEDI/SNIP Web Site – www.wedi.org/snip

Workgroup for Electronic Data Interchange (WEDI) – www.wedi.org

Acknowledgements

WEDI/SNIP would like to express its appreciation to the authors for their efforts in preparing this White Paper:

Susan A. Miller, Esquire
The Kearney Group, Partner
HIPAA Certified LLC, VP

Andrew H. Melczer, Ph.D.
Vice President, Health Policy Research
Illinois State Medical Society