

---

WEDI - Strategic National Implementation Process (SNIP)

# HIPAA Privacy White Papers



**SNIP**

**HIPAA Privacy White Papers  
August 2004**

**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*

© 2002-2004 Workgroup for Electronic Data Interchange, All Rights Reserved

# Contents

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

# HIPAA Privacy White Papers

---

## Disclaimer

This document is Copyright © 2002-2004 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 Privacy Regulation Outline

There have been a series of steps by the Department of Health and Human Services over a series of years to get to this integrated and updated privacy requirements and implementation standards. The five documents listed below must be read together to understand the nuances of implementing the requirements for your covered entity:

- Privacy Final Rule published in the Federal Register on December 28, 2000;
- First Privacy Guidance published by the Office of Civil Rights on July 6, 2001;
- Privacy Modification NPRM published in the Federal Register on March 21, 2002;
- Privacy Modification Final Rule published in the Federal Register on August 14, 2003; and
- Further Privacy Guidance published by the Office of Civil Rights on December 4, 2002.

There are two Parts to the HIPAA regulations that outline the privacy 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 E – Privacy of Individually Identifiable Health Information

- 164.500 Applicability.
- 164.501 Definitions.
- 164.502 Uses and disclosures of protected health information: general rules.
- 164.504 Uses and disclosures: organizational requirements.
- 164.506 Uses and disclosures to carry out treatment, payment, and health care operations
- 164.508 Uses and disclosures for which an authorization is required.

164.510	Uses and disclosures requiring an opportunity for the individual to agree or to object.
164.512	Uses and disclosures for which an authorization or opportunity to agree or object is not required.
164.514	Other requirements relating to uses and disclosures of protected health information.
164.520	Notice of privacy practices for protected health information.
164.522	Rights to request privacy protection for protected health information.
164.524	Access of individuals to protected health information.
164.526	Amendment of protected health information.
164.528	Accounting of disclosures of protected health information.
164.530	Administrative requirements.
164.532	Transition requirements.
164.534	Compliance dates for initial implementation of the privacy standards.

---

## The HIPAA Privacy Regulations Require Covered Entities to Take Specific Steps to Protect PHI

Some of the basic steps include:

- Adopt policies and procedures to protect the privacy of protected health information;
- Adopt policies and procedures giving individuals specific rights to their health information, including:
  - the right of access and copying;
  - the right to an accounting of certain disclosures,;
  - the right to request corrections/amendments;
  - the right to request limits on disclosures your office makes; and
  - the right of confidential communication;
- Create a written notice describing how your office uses and discloses protected health information and provide it to each patient or member;
- Designate a privacy official to handle privacy complaints and questions about your notice of privacy practices;
- Sign or amend contracts with your business associates who use or create protect protected health information;
- Provide policies and procedures training to your personnel;
- Implement safeguards to protect patient information from improper disclosure;
- Establish a reporting and response system for privacy violations; and
- Develop a sanctions policy for the discipline of privacy violations by your employees, agents and contractors.

### Serious 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 Office of Civil Rights (OCR) and damage to business interests and reputation, loss of reputation, loss of patients or members.

---

## 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.

The privacy white papers are:

- Privacy Policies and Procedures
- Small Practice Privacy Implementation
- Minimum Necessary
- Paper versus Electronic Records
- Preemption
- De-identification and Limited Data Set
- Access and Amendment
- Notice and Authorization
- Accounting of Disclosures
- Oral Communications
- Business Associate Example: Medical Transcription

---

## HIPAA Privacy Websites

SNIP Security and Privacy White Papers

[http://www.wedi.org/snip/public/articles/dis\\_publicDisplay.cfm?docType=6&wptype=2](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>

Office of Civil Rights (OCR)

<http://www.os.dhhs.gov/ocr/hipaa/>

OCR Privacy Complaint FAQ

<http://www.os.dhhs.gov/ocr/howtofileprivacy.htm>

OCR Compliant Form

<http://www.os.dhhs.gov/ocr/howtofileprivacy.doc>

OCR Technical Guidance

<http://www.os.dhhs.gov/ocr/hipaa/assist.html>

CMS Administrative Simplification

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

Georgetown Health Privacy Project

<http://www.healthprivacy.org/>

---

## Conclusion

You 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 – [wedi.org/snip](http://wedi.org/snip)

Workgroup for Electronic Data Interchange (WEDI) – [www.wedi.org](http://www.wedi.org)

---

## Acknowledgments

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

Susan A. Miller, Esquire  
Optimal Practice Solutions

Andrew H. Melczer, Ph.D.  
VP, Illinois State Medical Society