

---

WEDI - Strategic National Implementation Process (SNIP)

# Security and Privacy Workgroup Introduction



**SNIP**

**Security and Privacy Workgroup  
Introduction – April 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

**Introduction** **1**

- Disclaimer ..... 1
- Security and Privacy Intersections ..... 1
- Overview ..... 2
- SNIP Security and Privacy Deliverables ..... 2
- Getting Started with HIPAA Security ..... 3
  - The Key Security Provisions ..... 3
- Getting Started with HIPAA Privacy ..... 3
  - The Key Privacy Provisions ..... 4
- Impact of HIPAA Privacy and Security Will Vary ..... 5
- General HIPAA Security and Privacy Guidelines ..... 5
- HIPAA Security and Privacy Policies & Procedures ..... 7
  - Implementation Considerations and Issues ..... 7
  - Risk Considerations ..... 7
- General Thoughts about a HIPAA Timeline ..... 7
  - Some Good Questions to Ask of Vendors ..... 8
- Outreach ..... 8
- Acknowledgments ..... 9

# Introduction

---

## Disclaimer

This document is Copyright © 2002/2003 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.

---

## Security and Privacy Intersections

The Workgroup for Electronic Data Interchange (WEDI) Strategic National Implementation Process (SNIP) made the decision to combine Privacy and Security into one workgroup in large part because these two HIPAA rules exhibit many parallel and crossover issues. The privacy and security areas would be difficult to coordinate across separate workgroups.

While we have maintained the Privacy verses Security distinction for the purposes of organizing the outcomes of the SNIP Security and Privacy Workgroup, each of the individual Sub-Workgroups have addressed both of the HIPAA rules where they determined that crossover or intersection of privacy and security exists.

---

## Overview

The effects of published and pending HIPAA rules are likely to vary in as many ways as there are different organizations within the health care community. Yet within this varied landscape there are common issues and concerns that will influence each organization's strategic and tactical planning in order to become "HIPAA ready." WEDI SNIP is driven to provide the information and tools that will enable such organizations to be fully aware of all factors that will enable them to be "HIPAA ready" and do so by disseminating, at a national level, information on matters that touch us all.

Two such factors are the security of electronic data that is in transit and at rest, and the privacy of protected healthcare information, electronic or paper and oral communication. These are the subject of the Security Final Rule published in February 2003, and the Privacy Final Rule, which was published on December 28, 2000, with an effective date of April 14, 2001. In addition, they are subject to the Privacy Modification Final Rule published on August 14, 2002.

**SNIP Security Focus:** The initial charge was to determine what in the proposed rule WEDI SNIP should address in order to provide guidance at the national level. This guidance would enable an individual organization to avoid duplicating effort, as well as reduce the risk of omitting a crucial component in their HIPAA strategic plan. We are now moving into the issues and implementation barriers with in the Security final rule.

**Security Sub-Workgroups:** Representing a broad cross-section of the health care community, the participants in the Security and Privacy Workgroup's deliberations sought to identify those parts of the proposed Security Rule that could pose significant challenges to effective and timely implementation of the proposed standard. The security sub-workgroups are now turning to a review and analysis of the Security Final Rule.

**SNIP Privacy Focus:** As with the SNIP Security focus, the initial charge of the privacy efforts was to determine what WEDI SNIP could address in the pending rule in order to provide guidance at the national level.

**Privacy Sub-Workgroup:** Representing a broad cross-section of the health care community, the participants in the Security and Privacy Workgroup's deliberations sought to identify those parts of the proposed Privacy rule that could pose significant challenges to effective and timely implementation of the proposed standard.

The sub-workgroups updated the white papers based on the publication of the Privacy Final Rule and the Privacy Modification Final Rule. Following this review, a number of the privacy white papers will now be considered final.

---

## SNIP Security and Privacy Deliverables

The initial deliverables of each of the Security and Privacy Sub-Workgroups was a series of "white papers" which summarized their findings and suggested implementation ideas. The white papers are now outlined in separate outlines, one outlining the privacy white papers and one outlining the security white papers.

**Fourth Major Release of the White Papers:** In April and May of 2003 the Security and Privacy Work Group published a fourth major release of the white papers in three years. All the white papers in existence at this time were thoroughly reviewed against both the Privacy Modification final rule and the Security final rule.

New areas in the security area are anticipated given the changes in the final rule, and other areas for privacy will be developed as the industry outlines implementation barriers through feedback from the healthcare community.

Comments or suggestions on these papers and other information contained herein are welcome, and should be directed to the Privacy and Security Co-Chairs.

---

## Getting Started with HIPAA Security

The following information is provided to facilitate understanding of the HIPAA Security standards and the “white papers” that have been prepared. Now that we have a final security rule you need to begin additional or continuing work for your environment.

Keep in mind that the privacy provisions that were implemented by April 14, 2003 includes a mini-security rule in 45 CFR 164.530(c) Safeguards. The industry cannot afford to wait any longer now that we have a Security final rule. Security measures must be implemented in order to keep the protected information private.

### The Key Security Provisions

While most health care organizations have security programs and are providing “due diligence,” HIPAA will greatly expand those programs by requiring specific administrative and technology related security practices and procedures with the expressed goal of providing for the security and availability of protected health care information. The security requirements are very comprehensive and extend far beyond the information technology environment. Most of the rule’s security standards impact administrative areas and cannot be solved by technology alone.

The Security Rule provides for compliance actions structured within the following basic categories:

- Administrative Safeguards: formal practices to manage security and personnel.
- Physical Safeguards: protection of computer systems.
- Technical Safeguards: safeguards to control and monitor information access (data-at-rest), including technology to secure data-in-transit.
- Organizational Requirement: including business associate contracts
- Policies and Procedures and Documentation Requirements: similar to those within the privacy final rule

---

## Getting Started with HIPAA Privacy

As with Security, the HIPAA Privacy Rule has far reaching effects on health care organizations, generally requiring increased accountability to patients and members, increased complexity of administrative operations, and new privacy policies and procedures. The compliance deadline was April 14, 2003 (2004 for small health plans). Covered entities should continue their work to ensure compliance with the

HIPAA Privacy requirements.

## **The Key Privacy Provisions**

While the confidentiality of health care records was once maintained by family doctors, which kept records of care sealed away in file cabinets, today the use and disclosure of this information is distributed and protected by a myriad of state laws. This led to large gaps in the protection of patients' privacy and confidentiality. The Privacy regulations of HIPAA are established to meet the pressing need for national standards to control the flow of sensitive patient information and to establish real penalties for the misuse or improper disclosure of this information.

### **Privacy General Rules**

- Use and disclosure for treatment, payment, and healthcare operations
- Minimum necessary use and disclosure
- Creation of de-identified information or a limited data set
- Application to business partners through contract
- Application to information about deceased persons
- Adherence to the notice of information practices
- Application as covered entities components of organizations that are not covered entities

### **Privacy Establishes Rights of Individuals**

- Right of confidential communications
- Right to request restriction of use and disclosure
- Right and procedure for a written notice of information practices
- Right and procedure for access for inspection and copying
- Right and procedure with respect to an accounting of disclosures
- Right and procedure for amendment and correction
- Right of accounting of uses and disclosures beyond payment, treatment and healthcare operations

### **Administrative Requirements**

- Designation of privacy official
- Training
- Safeguards
- Internal complaint process
- Sanctions
- Duty to mitigate

### **Uses and Disclosures with Individual Authorization**

- Authorization requirements
- Plain language requirement
- Prohibition on conditioning treatment or payment
- Revocation of an authorization by the individual
- Expired, deficient, or false authorization

### **Uses and Disclosures without Individual Authorization**

- Use and disclosure for public health activities
- Use and disclosure for health oversight activities
- Use and disclosure for judicial & administrative proceedings
- Disclosure to coroners and medical examiners
- Disclosure for law enforcement
- Use and disclosure for governmental health data systems
- Disclosure for directory information
- Disclosure for banking & payment processes
- Use and disclosure for research, emergency circumstances, next-of-kin, and as required by other laws

---

## Impact of HIPAA Privacy and Security Will Vary

Designed to be very broad and capable of being adopted across the Health Care Industry, the effects of HIPAA implementation issues encountered will vary across the industry from providers to payers. Organizational issues will also vary, often dramatically, based minimally on the following factors:

- Size and structure
- Technology foundations
- Business and trading partner arrangements
- Role of identified healthcare information

The Security and Privacy Workgroup white papers address the issues that need to be considered by a variety of organizations. The Small Provider Privacy Implementation white paper provides information for the smallest covered entities.

HIPAA will have the greatest effect on health care organizations within the following key impact areas:

- Requirement for Security Evaluation
- Requirements for the designation of privacy official
- Assessment of risks
- Implementation of a written Security and Privacy Plans
- Implementation of specific personnel, physical and operational security and privacy measures
- Use of access control rules
- Development and maintenance of audit trails
- Use of “approved” security technologies
- Requirements for use and disclosure
- Requirements for Patient Rights and Access to Information
- Policies and procedures for both security and privacy requirements

---

## General HIPAA Security and Privacy Guidelines

One of the best ways to get started with HIPAA is to use the many resources and links available on the World Wide Web. Many of the best of these resources are presented here on the WEDI/SNIP site, [snip.wedi.org](http://snip.wedi.org), and will serve as an effective way to get started, or enhance your understanding of HIPAA. As with any information available on the Internet, it is always a good idea to attempt to validate the information against multiple sources for accuracy. Web resources are only one area to gain information

and ideas. If you require legal advice, you should consult with an attorney.

What follows are suggestions for actions that every organization subject to HIPAA should be undertaking *NOW!* Hopefully, most organizations already are moving forward actively to implement the HIPAA requirements.

- Become familiar with the proposed HIPAA Security and Privacy provisions. Start at a high level and work into the detail. The level of detail will depend on the type, size and sophistication of your organization.
- Assign someone in your organization to lead the HIPAA effort and to be responsible for security and as required someone who will be responsible for privacy. In many organizations this will be a single person.
- Conduct a business impact analysis that includes:
  - a preliminary risk and exposure assessment;
  - a baseline assessment of current security and privacy capabilities;
  - a gap analysis between your current environment and that required for HIPAA compliance; and
  - a risk management assessment based on a risk-benefit analysis.
- Examine partnerships with similar organizations to establish baseline guidelines and work plans. Consider working with local regional SNIP affiliates.
- Start planning for an enterprise wide interdisciplinary approach to HIPAA security and privacy compliance (keep in mind that even smaller organizations must consider the following issues):
  - let senior management and other decision-makers know the cost impact and related systems;
  - start identifying both the internal and external resources you may require;
  - plan for greater administrative processes and meetings than technology implementations;
  - start querying Vendors for HIPAA compliance plans and dates (see expanded list below);
  - plan for HIPAA security being included in any new hardware, software and telecommunications;
  - plan for how you will establish for the expanded model of a “Business Associate” contracts with business associates;
  - develop and/or revise existing security and privacy polices and processes;
  - budget for HIPAA;
  - validate and revise enterprise-level security architecture; and
  - validate and revise organizational privacy effectiveness.
- Consider a minimal enterprise-wide security and privacy program consisting of:
  - administrative support for all implementation components;
  - administrative processes and policies and personnel procedures;
  - education and training;
  - physical site and system security;
  - technical security with recursive testing, validation and revisions; and
  - vendor and trading partner guidelines and training; and audit processes, procedures and mechanisms.

---

# HIPAA Security and Privacy Policies & Procedures

Both the final Privacy Rule and the final Security Rule call for a covered entity to develop policies and procedures to implement the requirements of the rules. While it is not the intent of the WEDI SNIP Privacy and Security workgroup to provide sample policies and procedures, the workgroup established the Policies and Procedures sub-workgroup to provide substantial assistance in developing policies and procedures. There are two policy and procedure white papers, one for privacy and one for security.

## Implementation Considerations and Issues

Each covered entity is required to establish policies and procedures to ensure compliance with the HIPAA privacy and security requirements. Individual differences such as size and technological sophistication will influence the specific policies and procedures an entity develops. Since the Privacy and Security rules are intended to be flexible and scalable, larger, more technologically sophisticated entities are required to implement more extensive and more stringent privacy policies and procedures.

## Risk Considerations

A health care entity's decisions regarding the scope of its policies and procedures can be influenced by physical factors such as its size and by business factors such as acceptable levels of risk. However, please note that even the smallest entity must implement the policies and procedures required to protect the health information in its care. However, larger and more sophisticated entities will be expected to implement policies and procedures that reflect their size and complexity.

**State Regulations:** With certain limited exceptions, the privacy provisions preempt state law if: 1) the HIPAA provisions are more stringent than the state laws; 2) it would be impossible for a covered entity to comply with both the state law and the HIPAA regulations; or 3) the state law creates an obstacle to accomplishment of the goals of HIPAA. Covered entities must be aware of state laws that are more stringent than the HIPAA provisions and must meet the higher standards in every instance. (This has been addressed by the Preemption sub-workgroup.)

While all covered entities must comply with the policies and procedures standards, entities with a history of compliance issues with DHHS related to other programs should be particularly careful to demonstrate compliance with the standards, as they are most likely to come under further DHHS scrutiny. In addition, entities have to be sensitive to any particular needs and concerns of their communities. To the extent possible, entities should meet the expectations of their clients.

---

## General Thoughts about a HIPAA Timeline

While the SNIP Security and Privacy Awareness and Education Sub-Workgroup white paper covers this in more detail, it should be noted that when taken as major items, it is easy to see how any timeframe can easily and quickly pass. The simple reality is that the larger and more complex the organization, the more time the recommended activities are likely to take. Every organization should conduct an initial risk and exposure evaluation and baseline planning with a focus on determining how much of the implementation timeframe will be needed. As can be seen from the sample timeline, it could actually take some organizations longer than the allowable two years included in the rules to become complaint.

Remember that HIPAA is a rolling set of deadlines for compliance. We have just passed the April 14,

2003, deadline for Privacy, and now we must begin the next two year now for the HIPAA security requirements.

As the deadline draws near, the more costly and scarce knowledgeable resources become. Realistically, only smaller provider and practice management operations will be able to afford to wait to start acting on their HIPAA compliance efforts.

## **Some Good Questions to Ask of Vendors**

If you are not already doing so, start talking to vendors and trading partners right away. **DO NOT** assume that they are working towards compliance. Make certain that all your business partners are "HIPAA-Aware." The following are initial questions to ask:

- Does the vendor know what HIPAA is and can they demonstrate an understanding of the proposed rules?
- Will the vendor provide enhanced security features to meet HIPAA?
- Will the enhancements be handled under normal maintenance agreements and as part of the application or hardware upgrade cycle, if not what are the additional costs associated with the enhanced features?
- Will the enhancements introduce new applications or other technology partnerships into your operations?
- How do the enhanced features impact the existing security foundations and applications?
- When will the enhancements be available?
- How have they been tested and how will the "Test-to-QA-to-Production" migration path be handled?
- What types of access controls are enabled (e.g., user, role or context-based access)?
- How have the security administration features been implemented and have they enhanced the complexity of the application or system? Support or training?
- If the Internet is used, does it have encryption and does it meet at minimum HCFA's Internet Policy?
- If used or required, how does encryption effect the application? The network? The user community?
- Can the application or system support digital certificates?

---

## **Outreach**

WEDI/SNIP continues to have quarterly meetings to inform and involve the health care community in the implementation of HIPAA. For more information on these meetings go the WEDI/SNIP website: [wedi.snip.org](http://wedi.snip.org).

WEDI/SNIP also invites the community to be involved in the development of its white papers – security and privacy, transactions, and education. To get involved on various white papers sign up at the WEDI/SNIP site.

There are a number of regional groups working on implementation of HIPAA. A list of the Regional SNIP Affiliates can be found on the SNIP site. While HIPAA is national in scope, it must be implemented at the local level, and individuals are encouraged to be involved at both the national and local levels.

---

# Acknowledgments

WEDI/SNIP would like to express its appreciation to those who participated in preparing this White Paper:

## **SNIP Security and Privacy Work Group Co-Chairs**

Lesley Berkeyheiser The Clayton Group, LLC  
Walt Culbertson Availity  
Susan A. Miller, Esq. HIPAA Certified LLC  
Andrew H. Melczer, Ph.D. Illinois State Medical Society

## **Introduction Author**

Walt Culbertson

## **Introduction Editors**

Lesley Berkeyheiser  
Andrew Melczer  
Sue Miller

## **Editor April 2003 Version**

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