
WEDI - Strategic National Implementation Process (SNIP)

Security and Privacy Workgroup



SNIP - Security and Privacy Workgroup
“White Papers” DRAFT Version 3.1
**Awareness Training
and Education**

December 2001

Workgroup for Electronic Data Interchange

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

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

Contents

- Introduction** **2**
 - Disclaimer 2

- Awareness Training and Education** **3**
 - Background 3
 - Definition 3
 - Objectives 4
 - Implementation Considerations and Issues 4
 - Development Suggestions 5
 - What Needs to Happen – NOW! 5
 - Long Term Development Program 5
 - Risk Considerations 6
 - Timeline 7
 - Additional Sources of Information 7
 - Acknowledgments 7

Introduction

Disclaimer

This document is Copyright © 2001 by The Workgroup for Electronic Data Interchange. 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 Security and Privacy Workgroup members 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 a majority of the proposed Security Rule relates 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.

The work in Version 3 was completed before the Privacy Guidance of July 6, 2001, was released by the Department of Health and Human Services. The next version of the white papers will include review of the guidance document.

Awareness Training and Education

Background

As healthcare organizations prepare and brace themselves for the impact of HIPAA, there is an overwhelming need to ensure a consistent message is communicated throughout an organization relative to the interpretation, impact, strategies and communications, which will lead an organization to a level of strategic HIPAA readiness. Communication and education will be the foundation and process for creating a security culture at an organization. These building blocks will foster the necessary information dissemination and dialogue to integrate security throughout an organization's business processes and roles.

Definition

As defined within the Security NPRM, all covered entities will be required to develop, maintain and demonstrate their efforts to communicate, build awareness and educate their employees, trading partners, contractors and agents necessary for compliance with HIPAA regulations. These requirements specifically state that an entity must educate and train all employees, agents and contractors on:

- Requirements of HIPAA inclusive of but not excluding:
 - Health Care Information Security
 - Virus Protection
 - Risk Management
 - Media Management
 - Chain of Trust
 - Personal
 - Security Management
 - Incident Reporting
 - Configuration Change Management
- Policies and Procedures Required to Comply with HIPAA rules
- Technical Infrastructure and Operation Required to Support the Security NPRM

Although this definition within the NPRM is specific as to the required outcomes and mandatory requirements, it does not specify how an entity will develop and communicate their awareness and education program. Due to the extreme variability in both scope and role of covered entities, this lack of clarification actually provides the best means for compliance by allowing organizations to craft methodologies or strategies which scale well based on entity type and size.

Objectives

- HealthCare entities must develop and implement a security awareness program that:
 - Ensures compliance with HIPAA Security awareness regulations
 - Solicits and achieves executive support necessary for program implementation
 - Builds a culture around security
 - Identifies the issues and challenges, which will drive an organization's tactical plan for HIPAA compliance
- HealthCare entities must develop and implement a security education program that:
 - Ensures compliance with HIPAA Security education regulations
 - Supports an organizations strategic and tactical implementation strategies for HIPAA compliance
- Develop a timeline for all phases of an organization's security awareness and education program.
- Create a process and measurement for determining the overall effectiveness of an organization's security awareness and education training program.
- Determine the integration points and implementation windows required to effectively coordinate security awareness and education with an organization's overall HIPAA compliance tactical plan.
- Build the multi-disciplinary approach and coalescing across the organizational business units necessary to achieve optimal program implementation.
- Performance of a risk assessment and the resulting gap analysis will be the baseline and establish the tactical objectives of the security awareness and education program.
- The development, implementation, communication and enforcement of policies and procedures to mitigate the risk and ensure on-going compliance with HIPAA security regulations must be coordinated and delivered within the context of the Security Awareness and Education program.

Implementation Considerations and Issues

- Communications, planning and pre-implementation efforts will directly correlate to the total cost (both financially and resources allocated) that an organization must bring to bear for HIPAA compliance.
- Development and delivery of a consistent message, which is relative to all employees across an organization, will reduce the amount of confusion and variability of interpretation of the regulations and an organization's strategy for compliance.
- Awareness training and communication builds the "baseline" of what HIPAA is who is affected and what it means.
- Organizations will be required to "build" and deliver a security awareness and education program that addresses their interpretation of HIPAA and supports the activities necessary to mitigate risk based on the results of an organization wide assessment.
- Communication of HIPAA impact, organizational security education requirements and implementation plan will be specific to organizational business roles. The message must be consistent yet relevant and appropriate to the organizational business line and staff support role.

- An organization's communication and education curriculum development will be the feedback mechanism and refinement process for an organization's tactical implementation to achieve HIPAA compliance.
- Organizations must qualify and integrate into their awareness and education programs their respective return or value proposition in supporting and meeting the requirements of HIPAA.
- Creation and delivery of a common message, interpretation of the regulations and process for addressing and communicating issues will speed the implementation and reduce the overall cost in complying with HIPAA.
- Security awareness and education training will increase the probability an organization will be ready for HIPAA.
- Identification and communication of problems will reduce the likelihood the same problem and resolution process will be addressed in multiple iterations.
- HealthCare entities must be proactive in reducing variability across business units in developing and implementing their respective tactical strategies for HIPAA compliance.

Development Suggestions

What Needs to Happen – NOW!

- Initiate security awareness communication and education now. The proposed rules are not revolutionary in the area of patient privacy and confidentiality. The standards proposed by HIPAA are basic to the healthcare delivery process, which we expect all healthcare professionals to follow – today. The value and effectiveness of the risk assessment performed by an organization is directly linked to organizational commitment and communication relative to HIPAA compliance.
- Achieve executive buy-in as early on as possible. Establishing an executive owner to help champion and maintain senior level involvement will prove crucial in getting the message across and securing support throughout the organization.
- Form cross-organizational HIPAA implementation teams. Get middle management to participate and craft the message and curriculum that will directly impact their business line, product or service.
- Create a project plan and timeline as outlined in the Suggested Development section to structure, define the resources and establish dates for the organizational security awareness and education program.
- Begin evaluating current business and technical training curriculum to determine appropriate integration of security awareness and education program requirements.

Long Term Development Program

It is recommended that organizations follow industry guidelines for developing, implementing, assessing and refining their security awareness and education program.

- Assess the organization's readiness and perceived requirements for HIPAA compliance
- Define the required outcomes and objectives of the security awareness and education program necessary to support the strategic and tactical implementation plan.

- Determine if the organization has the key resources necessary to develop and deliver a security awareness and education program.
- Allocate or contract resources necessary to develop security awareness and education program. In the event external resources are required or an outsource arrangement is desired, an organization should follow recommended guidelines for qualifying a contractor or vendor for development of their security awareness and education program.
- Identify and qualify the message and curriculum for each business unit and role across the organization.
- Develop and test the communication strategies and education delivery methodologies, which will best meet the desired outcomes and objectives of the program.
- Implement an assessment process to determine the effectiveness of the communications and education programs.
- Sequence the communication, learning and feedback processes with the tactical implementation plan to ensure the plan evolves and remains achievable throughout the implementation process.
- Follow a structured process for communications and education program development:
 - M – Message (why, value, strategic approach, policies)
 - A – Desired Action (tactical outcomes)
 - D – Details of what will be done (tactical activities and tasks)
 - E – Examples of case studies or industry suggestions.
- Continue to assess, refine and update communications and education program throughout the assessment, implementation and support phases of bringing and maintaining an organization achievement of HIPAA compliance.

Risk Considerations

- HIPAA Awareness and Security education will directly compete with an organization's business and technology curriculum development and delivery resources. It is imperative that the healthcare entity determines early on their ability to redirect or allocate the resources necessary to build, deliver and maintain the security and awareness education program.
- Change management workflow development and implementation will challenge many organizations as these issue crosses organizational business lines and staff support roles.
- Appropriate and effective delivery mechanisms for the communication and implementation of an education program must be flexible and capable of reaching and communicating the message the healthcare organization is attempting to communicate. The organization must assess the current education and communication programs to identify those that will be effective in meeting the needs of the HIPAA requirements.
- Organizations must create a culture and embrace security as an integral component of delivering or supporting healthcare business processes. This is a fundamental change in the thought process, activities and roles of the majority of individuals responsible for healthcare delivery and support.
- Security awareness and security education must be integrated into the core business-training curriculum.

- Business partner relationships and contract structures will evolve to meet HIPAA requirements. Organizations will have to understand, communicate and assess the impact of those evolving contractual and business partner relationships.

Timeline

- **Phase I** – Awareness communication and risk assessment must start NOW! (3 to 6 months) – Prioritization of awareness program delivery: Executive management; Technologists; HealthCare Delivery Personnel
- **Phase II** – Education program and curriculum development (pending organizational size and complexity (3 to 12 months)
- **Phase III** – Training and Education (12 to 24 months)
- **Phase IV** – Training and Education Certification (18 months to 24 months)
- **Phase V** – Training and Education Refinement (20 to 24 months)
- **Phase VI** – Continued development, enhancement and delivery of security awareness and education as a core component of a healthcare entity’s clinical and business processes.

Additional Sources of Information

3Com's CPRI toolkit http://www.3com.com/healthcare/securitynet/hipaa/4_9_1.html

[For the Record: Protecting Electronic Health Information \(1997\)](#)

Excellent book on Maintaining Privacy and Security in Health Care Applications of the National Information Infrastructure by the National Research Council

Information Technology Security Awareness Workgroup (ITSA) - <http://www.cio.ufl.edu/~itsa/>

The Center for Security Awareness Information - <http://www.dtic.mil/dodsi/csai.html>

Information Systems Security Association (ISSA) - <http://www.issa-intl.org/awareness.htm>

Building Security Awareness - <http://www.cert.org/sepg99/tsld023.htm>

Acknowledgments

White Paper Authors

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

Chuck Henck, Awareness Training and Education Sub-Group Chairman
University Physicians Inc.

Irene Doucette
Blue Shield of California