HIPAA Privacy and Security Training (2003 update)

Save to myBoK

This practice brief has been updated. See the latest version here. This version is made available for historical purposes only.

Editor's Note: This practice brief supplants the April 2002 "HIPAA Privacy and Security Training" Practice Brief.

HIM professionals have long known and upheld the legal and ethical obligations of consumer privacy protection of health information. Advocacy of these principles within healthcare organizations has been based on professional accountability and external directives. However, depending on an organization's state of residence (state laws), program participation (such as Medicare, alcohol and drug abuse programs, and accreditation programs), and applicable federal laws, this protection may be fragmented at best.

The extent of work force awareness and degree of privacy and security restrictions for patient health information have varied due to the delicate balance of privacy with the benefits of sharing and using information, job position influence or parameters, leadership interpretation of existing directives, and implementation cost. Though implicit, these requirements for upholding privacy and security of health information have seldom required work force training.

HIPAA requires formal education and training of the work force to ensure ongoing accountability for privacy and security of protected health information (PHI). HIPAA's privacy rule and security rule independently address training requirements. Like the majority of the standards, the training requirements are non-prescriptive, giving organizations flexibility in implementation. This practice brief offers guidelines to covered entities to aid in implementation of the training standards and suggests the efficacy of combining efforts.

Federal Requirements

HIPAA Privacy Rule

Section 164.530 of the HIPAA privacy rule states:
(b) 1. **Standard: training.** A covered entity must train all members of its work force on the policies and procedures with respect to PHI required by this subpart, as necessary and appropriate for the members of the work force to carry out their function within the covered entity.

(b) 2. **Implementation specifications: training.**

> i. A covered entity must provide training that meets the requirements of paragraph (b) (1) of this section, as follows:
>
> - To each member of the covered entity's work force by no later than the compliance date for the covered entity
> - Thereafter, to each new member of the work force within a reasonable period of time after the person joins the covered entity's work force
> - To each member of the covered entity's work force whose functions are affected by a material change in the policies or procedures required by this subpart, within a reasonable period of time after the material change becomes effective in accordance with paragraph (i) of this section
>
> ii. A covered entity must document that the training as described in paragraph (b)(2)(i) of this section has been provided, as required by paragraph (j) of this section

(j) 1. **Standard: documentation.** A covered entity must:

i. Maintain the policies and procedures provided for in paragraph (i) of this section in written or electronic form
ii. If a communication is required by this subpart to be in writing, maintain such writing, or an electronic copy, as documentation
iii. If an action, activity, or designation is required by this subpart to be documented, maintain a written or electronic record of such action, activity, or designation

(j) 2. **Implementation specification: retention period.** A covered entity must retain the documentation required by paragraph (j)(1) of this section for six years from the date of its creation or the date when it last was in effect, whichever is later.

Summary: A covered entity must train the entire work force on HIPAA-directed privacy policies and procedures necessary to comply with the rule through execution of organizational operations. Small health plans have an extension to April 14, 2004, one year beyond the implementation date for most covered entities. All must provide for ongoing updates and evidence of compliance must be documented in either written or electronic form and be retained for a minimum of six years from the implementation date.

HIPAA Security Rule

HIPAA's security standard 164.308(a)(5)(i) states:
"... Implement a security awareness and training program for all members of its work force (including management)."

(ii) Implementation specifications. Implement:

- Security reminders (addressable)
- Protection from malicious software (addressable)
- Log in monitoring (addressable)
- Password management (addressable)

Section III, analysis of and responses to public comments on the proposed rule, clarifies that "the amount and type of training needed will be dependent upon an entity's configuration and security risks." It further states, "Business associates must be made aware of security policies and procedures, whether through contract language or other means. Covered entities are not required to provide training to business associates or anyone else that is not a member of their work force." Further, it states, "Training can be tailored to job need if the covered entity so desires."

Summary: The entire work force, including management, must be trained on security issues respective of organizational uniqueness. The requirement for periodic security updates ensures the ongoing nature of the effort.

State Laws and Regulations

Though few states have had regulations specifically requiring training for privacy and security, any existing regulations are preempted by HIPAA except in cases of a more stringent status designation. Organizations should be aware of state circumstances.

Accreditation

Joint Commission Standards
The 2004 hospital standards were modified to be consistent with HIPAA. The pre-publication Web edition addresses privacy and security:

IM.2.10 states, "Information privacy and confidentiality are maintained." The second element of performance addresses privacy training and updates: "The organization's policy, including significant changes to the policy, has been effectively communicated to applicable staff."

IM.2.20 states, "Information security including data integrity is maintained." The same element of performance applies for security as for privacy noted in IM.2.10 above.

The Accreditation Association for Ambulatory Health Care and the American Osteopathic Association standards do not explicitly cover privacy and security training.

Recommendations

If you have HIPAA privacy and security training responsibilities in your organization, following are considerations for program development:

General

Determining the best training approach for your organization is a significant task. Healthcare organizations may be able to reduce the administrative burden and cost of privacy and security training by making it part of a comprehensive HIPAA educational program or part of an even broader educational program. While the training standards apply to a universal audience when other portions of the administrative simplification act may not, organized planning can address audience overlap and reduce redundancies in reaching large groups with varying messages.

Obtaining support and conducting high-level training for administration and senior management is critical due to the magnitude, cost, and ongoing nature of the requirements.

Similarities in the privacy and security requirements invite combined training efforts. Both rules include training of all personnel, ongoing training, and documentation. Below are points to consider when implementing a successful training process:

- Make training your mantra-it may be your best privacy asset
- Develop an enduring program that perpetuates itself and becomes part of the culture of your organization
- Document your organizational privacy and security training program. It should cover education (knowledge and understanding), training (how-to), and ongoing awareness. The compliant approach includes PHI in all forms including verbal, written, and electronic. Timelines for initial efforts and subsequent new employee orientation according to date of hire should also be included
- Use effective training structures and methods already in place when possible
- Present an understanding of the spirit of HIPAA as it applies to the individual consumer to personalize it. Make each employee your deputy in compliance. Emphasize the need for cultural change and the need to resist the natural tendency toward curiosity
- Develop a responsive communication process to address questions that arise after training and in an ongoing manner. Implementation questions may point out holes in the program that need to be addressed.
- A reference repository of up-to-date policies and procedures is critical. A centralized composite on the Intranet can be a dependable and easily updated resource. Employer-endorsed Web sites can provide a mechanism for individuals to stay current on privacy issues and legislation
- Develop a process for evaluating training program effectiveness, reliability, and validity. This should include a provision for updating the trainers on any changes or enhancements
- Make a commitment to follow industry best practices, benchmarks, and standards regarding training as healthcare settles into this new way of life. No two programs will be identical, yet much can be gained from networking

Who Is Trained

HIPAA's privacy rule defines work force as "employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity, is under the direct control of such entity, whether or not they are paid by the covered entity." It further directs that training include "all members of its work force," "each new member of the work force," and "each member of the covered entity's work force whose functions are affected by a material change in the policies or procedures."

The security rule states, "all members of its work force (including management"). Understanding the breadth of the training audience is critical for both initial and ongoing training. An organization should define its audience according to structure and operations with particular respect for access to PHI, responsibilities presenting compliance risk, and the ripple nature of PHI access through contractual relationships. Careful evaluation may introduce the importance of including individuals outside of the rule definitions. Individuals to be considered include part-time, contractual, temporary, home-based, and remote employees,

management, board of directors, physicians (on site, in offices, and remote), educators, students, researchers, and maintenance personnel.

Who Trains

Existing organizational structure will help to direct a logical, workable approach for identifying trainers and accommodating HIPAA requirements. The need to establish clear accountability, appoint knowledgeable, qualified trainers, and clarify timelines and ongoing roles is critical in every setting. Questions to consider include:

- Who are the effective trainers in your organization now?
- Has a HIPAA oversight team been appointed?
- Do your privacy officer and security officer positions or functions work together to encourage a unified, coordinated approach?
- What role is appropriate for the human resources department, especially for reaching new hires with general training?
- If a train-the-trainer method is chosen, what key individuals are competent, and are they appropriate for ongoing instructor-led training?
- Does management have a role? Would management conduct general or role/job specific training?
- Should you use point persons for department, section, or unit training?
- Will your organization retain consultant services for training? What will be covered?

What to Cover

The privacy rule states that the following should be covered in an organization's privacy program: "policies and procedures with respect to protected health information...as necessary and appropriate for the members of the work force to carry out their function within the covered entity."

The security rule includes four "addressable" topics:

- periodic security updates
- procedures for guarding against, detecting, and reporting malicious software
- procedures for monitoring log-in attempts and reporting discrepancies
- procedures for creating, changing, and safeguarding passwords

Customizing Training

The rules address minimum training requiring scalability to be applied. Programs can and should be customized to your organization, operational nuances, and job position uniqueness. HIPAA-related gap and risk analyses are valuable references to fortify training outline.

As you compile policies and procedures for training purposes, it will be evident that some are universal in application while others are unique to roles and select positions. Consider creating levels of training. Level I, for example, would entail the universally important education and training topics. Level II would include those particular to a role or job position and would be closely aligned with the need-to-know parameters identified for varying positions.

Additional training levels may be needed when increased knowledge and skills are necessary to carry out operations in a compliant manner. For example, management/supervisory staff may need specific training due to their involvement in compliance functions. High-level training may be developed for the information systems staff who must apply privacy policies in administering technological responsibilities. Be flexible by applying as many varied levels as needed to accomplish your goals. See "Sample HIM Department Privacy and Security Training Plan," below.

Sample HIM Department Privacy and Security Training Plan			
Training Level	**Target Audience**	**Privacy Topics**	**Security Topics**

1	all employees contractual coders volunteers students new employees	• general confidentiality • training requirements • patient rights (general) • reporting known or suspected breaches • sanctions • e-mail • faxing • complaints	• general security policies • physical and workstation security • periodic security reminders • virus protection • importance of monitoring log-ins • password management • audits
2	all employees volunteers students	• special record handling	• department security procedures • software discipline
2	ROI staff management staff	• federal and state laws • consents and exclusions • psychotherapy notes • uses and disclosures/ authorizations • patient rights • subpoenas, court orders • copy charges	• audit trails
3	management staff	• department privacy and security training • role and position assessments • training program evaluations • remediation procedures • sanctions	• monitoring procedures • role in ongoing awareness training • privacy and security system assessment

It could be helpful to prioritize the training protocol by weighing issues and group impact. For example, greatest volume, information sensitivity levels, and areas of heightened risk concern would be addressed more urgently than groups needing only periodic access.

Level I/General Training Examples:

- general confidentiality: governing laws and regulations and organizational policies
- training requirements
- general patient rights
- general security policies: consider including a security primer to increase understanding of information security and technology
- physical/workstation security
- periodic security reminders: why they are important, how they will be accomplished
- virus protection: potential harm, how to prevent it and how to report it
- importance of monitoring log-in success/failure and how to report discrepancies

- password management: keeping private, procedures for creating or changing, and other access management
- ramifications of breaches to the organization and the individual
- monitoring procedures
- reporting known or suspected breaches
- sanctions (organizational and individual)
- role of the Office for Civil Rights, the agency charged with enforcing the privacy regulations
- e-mail
- faxing
- complaints
- verbal confidentiality

Consider adopting Level I training content into new employee orientation, taking over when the first wave of training is complete. Be clear in communicating to new employees plans for department or unit customized training to supplement general training.

For Level II or job-specific training, drill down to necessary detail to evaluate positions effectively. Determine how a position uses health information, then fashion training accordingly. Assessment tools can be useful in determining appropriate inclusions for specific positions. Such tools provide a list of privacy and security topics. Using available information sources, determine applicable topics, including use and sensitivity levels when appropriate. Information sources could include job descriptions, observation, and discussion. See "Sample Privacy and Security Position Assessment," below.

Sample Privacy and Security Position Assessment

Role/Position Assessment For:
Role/Job Title: _____ Behavioral Health Unit_____
Date: _____

Training Topic	Sensitivity Level (high, medium, low)	Use Level (0-5)	Include in Training? (Yes/No)
Treatment/Payment/Operations	high	5	yes
Notice of privacy practices	medium	3	yes
Marketing	low	0	no
Psychotherapy notes	high	5	yes
Business associate agreements	low	0	no
Disclosures: routine	medium	5	yes
Patient rights: access	medium	3	yes
Patient rights: amend	medium	2	yes
Photographs	low	1	yes

Level II Training Topic Examples:

- federal laws, state laws, regulations
- treatment/payment/operations
- notice of privacy practices
- facility directories
- access
- business associate agreements
- marketing
- fund raising

- psychotherapy notes
- photography
- disclosure, authorizations, routine, restrictions
- re-disclosure
- patient rights: access, amend, accounting of disclosures, confidential communication
- research
- destruction of sensitive information
- copy charges
- de-identification
- retention
- minimum necessary
- aggregate data
- mitigation

For appropriate groups, cover:

- policies for geographical considerations: on site, remote, at home, physician offices
- equipment nuances: laptops, personal digital assistants, cell phones, pagers

Level III Training Example:

Management-specific training might include:

- review of policies or specific roles in department or section training
- role and position assessments and training
- audits
- training program evaluations and modifications
- ongoing awareness training or change updates
- remediation procedures
- sanctions

Training Delivery

Delivery method is important to the understandability of the information. Make an effort to use a variety of learning techniques and considerations as they relate to targeted groups or individuals and that optimally present the material to be covered. Below are important points to consider:

- When planning audience participation, consider different knowledge levels
- Consider how you can reach the most influential people in your organization
- Recognize the potential for information overload during training
- Varying learning techniques can help address different learning styles in group presentations
- Instructor-led classrooms may work best for in-depth training and when interaction or Q&A sessions are desired
- Rotate presenters in instructor-led sessions
- Computer-based training (PC, Intranet, and Internet) can be effective for reaching large groups (this can include online assessments/quizzes for immediate feedback)
- Training labs provide hands-on opportunity
- Videotapes can be used for varying audiences
- Videoconferencing
- Distance training takes advantage of teaching tools developed by others such as Web casts, informational Web sites, and online classes
- Frequently asked questions and discussion threads can be valuable when they are easily accessible
- If using handouts, display the information differently from your slides and choose the best time to distribute them according to your approach
- Consider developing training manuals to ensure consistency of coverage among trainers (these should be easily updated)

Ongoing Training

According to the privacy rule, "a covered entity must provide training...to each member of the covered entity's work force whose functions are affected by a material change in the policies or procedures required...within a reasonable period of time after the material change becomes effective." The security rule requires "security reminders."

Ongoing training is the process of keeping the issues in front of the work force. It is important to determine how often reminders will be circulated in addition to those triggered by change or new information. It is also important to identify which part of the work force needs which communications.

Optional methods of periodic reminders include sign-on security reminders, company newsletters, meetings, training programs, lunchtime sessions, promotional products, e-mail messages, banners and screen savers, fliers or handouts, posters, cafeteria tent cards, Web pages, teachable moments, grapevine, and literature and case law circulation, if only to select groups. Ensure a mechanism for updating the content of various training levels to reflect policy and procedure changes for affected individuals.

Documentation

The privacy rule requires that "a covered entity must document that the training...has been provided." The security rule addresses documentation in a general manner for all appropriate security standards in 164.316, requiring the maintenance of policies and procedures as necessary to comply with the requirements. It further states "if an action, activity, or assessment is required by this subpart to be documented, maintain a written (which may be electronic) record of the action, activity, or assessment."

Documentation bearing evidence that training has been completed is likely to be combined for privacy and security. It is recommended that the documentation include content, training dates, and attendee names. Methods of documenting training efforts could include the following:

- training program sign-in sheets, retention of training aids, and handouts
- signed confidentiality statements acknowledging receipt and understanding of any training level attended
- electronic access trails to record computer-based training completion or quiz results
- meeting handouts and minutes
- retention of e-mail messages
- a compliance training database recording details such as broadcast e-mails, flier distribution, screen saver or banner launching, or cafeteria tent displays

Ensure a documentation provision for recording training program assessments and updates, and apply HIPAA's retention requirement of six years.

References

Amatayakul, Margret, Joe Gillespie, and Tom Walsh. "What's Your HIPAA ETA?" *Journal of AHIMA* 73, no. 1 (2002): 16A-16D.

"Five Topics to Include in Initial HIPAA Security Awareness Training Session." *Health Information Compliance Insider*, August 2001.

"Gap and Risk Analysis: Get Started Now-and Not Just For HIPAA's Sake." *HIPAAnote* 1, no. 55 (December 5, 2001).

"Guidelines for Academic Medical Centers on Security and Privacy." Association of American Medical Colleges (2001). Available online at www.aamc.org/members/gir/gasp/start.htm.

Joint Commission on Accreditation of Healthcare Organizations. *2004 Pre-publication Web edition Accreditation Standards for Hospitals*. Oakbrook Terrace, IL: Joint Commission, 2003.

"Policy for Education, Training, and Awareness of the Health Insurance Portability and Accountability Act (HIPAA)." State of Maryland Department of Health & Mental Hygiene. September 28, 2001.

"Question of the Week." hcPro's *HIPAA Weekly Advisor*, December 31, 2001. Available online at www.himinfo.com/hipaa_ezine/hipaa_arc.cfm?&content_id=19650.

Security Standards Final Rule. 45 CFR Parts 160, 162, and 164. *Federal Register* 68, no. 34 (February 20, 2003).

"Standards for Privacy of Individually Identifiable Health Information; Final Rule." 45 CFR Parts 160 and 164. *Federal Register* 67, no. 157 (August 14, 2002). Available at www.hhs.gov/ocr/hipaa.

Upham, Randa. "Educating the Organization." *HIPAA Watch* (December 2001). Available at www.healthmgttech.com/cgi-bin/arttop.asp?Page=hipaa1201.htm.

Walsh, Tom. "Building Effective Training Programs to Make Cultural and Behavioral Changes." Presented at the Joint Healthcare Information Technology Alliance Conference in La Jolla, CA, May 23, 2001.

Prepared by

Beth Hjort, RHIA, CHP

Acknowledgments

Gordon Apple, JD
Mary Brandt, MBA, RHIA, CHE
Jill Burrington-Brown, MS, RHIA
Jill Callahan Dennis, JD, RHIA
Michelle Dougherty, RHIA
Carol Quinsey, RHIA
Harry Rhodes, MBA, RHIA, CHP
David Sobel, PhD
Tom Walsh, CISSP

Source: Hjort, Beth. "AHIMA Practice Brief: HIPAA Privacy and Security Training" (Updated November 2003)
