HIPAA Privacy and Security Training (2002)

Save to myBoK

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

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 final privacy rule and proposed 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 (CE) to aid in implementation of the training standards and suggests the efficacy of combining efforts.

Federal Requirements

HIPAA Final Privacy Rule

Section 164.530 of the HIPAA privacy rule states the following:

(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 docu-
mentation

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

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 while executing organizational operations. This must be done by the implementation date of April 14, 2003, (April 14, 2004, for small health plans) and provide for ongoing updates. 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.

The proposed HIPAA security rule states:

"...security training for all staff regarding the vulnerabilities of the health information in an entity's possession and procedures which must be followed to ensure the protection of that information." Implementation features required are:

- Awareness training for all personnel, including management (this is also included as a requirement under physical safeguards)
- Periodic security reminders
- User education concerning virus protection
- User education on importance of monitoring log-in success or failure and how to report discrepancies
- User education in password management

Separate sections of the security rule state, "Security awareness training (information security awareness training programs in which all employees, agents, and contractors must participate, including, based on job responsibilities, customized education programs that focus on issues regarding use of health information and responsibilities regarding confidentiality and security,)" and "assuring that system users, including maintenance personnel, receive security awareness training."

Summary: Training must be completed by the implementation date (yet to be determined by the release date of the final rule). All staff, including management, agents, contractors, and maintenance personnel are to be trained on issues specific to security and confidentiality of health information important to carrying out their respective roles in a manner that makes these practices inseparable from operations. The requirement for periodic reminders 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

- IM.2 states, "Confidentiality, security, and integrity of data and information are maintained." The intent clarifies, "The hospital is responsible for maintaining the security and confidentiality of data and information and conforming to laws and regulations as appropriate.
- IM.4 states, "The necessary expertise and tools are available for the analysis and transformation of data into information." The intent more specifically states, "Staff who generate, collect, analyze, or use data and information are educated. Education is appropriate to their responsibilities, privileges, job descriptions, and data and information needs."

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

It will be a big task to determine the best training approach for your organization.

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 Internet 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 personnel, including management," "all employees, agents, and contractors," and "maintenance personnel."

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

Organizational structure for accommodating HIPAA requirements will help to direct a logical, workable approach for identifying the trainers. 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, “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 states, “periodic security reminders, user education concerning virus protection, user education in importanceof monitoring log-in success/failure and how to report discrepancies, user education in password management.”

Customizing Training

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

As you compile policies and procedures for training purposes, it will be evident that some are universal in application. 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 of 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 information 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 information practices
- facility directories
- consents and exclusions
- 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, and 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, Internet, or links to other sites) 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 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 “periodic 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 implies the need to demonstrate training compliance: "each entity designated...must maintain documentation demonstrating the development, implementation, and maintenance of appropriate security measures that include, at a minimum, the requirements and implementation features set forth in this section. In addition, entities must maintain necessary documentation to demonstrate that these measures have been periodically reviewed, validated and updated, and kept current."

Privacy and security documentation should 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 the privacy rule'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.

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

Joint Commission on Accreditation of Healthcare Organizations. *Comprehensive Accreditation Manual for Hospitals*. Oakbrook Terrace, IL: Joint Commission, 2001.

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

"Gap and Risk Analysis: Get Started Now—and Not Just For HIPAA's Sake." *HIPPAnote* 1, no. 55 (December 5, 2001). Available online at http://www.hipaadvisory.com/notes/vol1/dec01.htm.

Security and Electronic Signature Standards. 45 CFR Part 142. *Federal Register* 63, no. 155 (August 12, 1998).

"Standards for Privacy of Individually Identifiable Health Information; Final Rule." 45 CFR Parts 160 and 164. *Federal Register* 65, no. 250 (December 28, 2000). Available at http://aspe.hhs.gov/admnsimp/.

"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.

Upham, Randa. "Educating the Organization." *HIPAA Watch* (December 2001). Available at http://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, HIM practice manager

Acknowledgments

Gordon Apple, JD
Mary Brandt, MBA, RHIA, CHE
Jill Burrington-Brown, MS, RHIA
Jill Callahan Dennis, JD, RHIA
Harry Rhodes, MBA, RHIA
David Sobel, PhD

Want to learn more about HIPAA compliance? View more HIPAA-related practice briefs in the FORE Library: HIM Body of Knowledge.

Preemption of the HIPAA Privacy Rule (February 2002)

Understanding the Minimum Necessary Standard (January 2002)

Required Content for Authorizations to Disclose (November/December 2001)

Destruction of Patient Health Information (Updated) (November/December 2001)

Accounting and Tracking Disclosures of Protected Health Information (November/December 2001)

Redisclosure of Patient Health Information (September 2001)

Transfer of Patient Health Information Across the Continuum (Updated) (June 2001)

Patient Photography, Videotaping, and Other Imaging (Updated) (June 2001)

Letters of Agreement/Contracts (Updated) (June 2001)

Facsimile Transmission of Health Information (Updated) (June 2001)

A HIPAA Privacy Checklist (June 2001)

Patient Anonymity (Updated) (May 2001)

Laws and Regulations Governing the Disclosure of Health Information (May 2001)

Consent for the Use or Disclosure of Individually Identifiable Health Information (May 2001)

Notice of Information Practices (May 2001)

Patient Access and Amendment to Health Records (May 2001)

Release of Information for Marketing or Fund-raising Purposes (May 2001)

Letters of Agreement/Contracts (Updated) (July/August 2000)

Article citation:
Hjort, Beth. "HIPAA Privacy and Security Training (AHIMA Practice Brief)." *Journal of AHIMA* 73, no.4 (2002): 60A-G.