HIPAA Privacy and Security Training (2010 update)

Save to myBoK

This practice brief has been retired. It is made available for historical purposes only.

Editor's note: This update replaces the November 2003 practice brief "HIPAA Privacy and Security Training."

HIM professionals long have 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, this protection may be fragmented at best 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.

The extent of workforce 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 implemenmpmtation cost. Although implicit, these requirements for upholding the privacy and security of health information have seldom required workforce training.

The HIPAA privacy and security rules require formal education and training of the workforce to ensure ongoing accountability for privacy and security of protected health information (PHI). HIPAA's privacy and security rules independently address training requirements.[1] Like most standards, the training requirements are nonprescriptive, giving organizations flexibility in implementation. In February 2009, minor revisions to required training efforts were provided as a part of the Health Information Technology for Economic and Clinical Health (HITECH) Act. This practice brief offers guidelines to covered entities to aid in implementation of the training standards required by HIPAA and HITECH.

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.

AHIMA Summary on Privacy Training: A covered entity must train the entire workforce on HIPAA-directed privacy policies and procedures necessary to comply with the rule. Workforce training should be executed through normal or existing organizational educational operations. All covered entities must provide ongoing updates and document evidence of compliance in written or electronic form and retain it 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
- Protection from malicious software
- Log in monitoring
- Password management

AHIMA Summary on Security Training: Covered entities should train the entire workforce, including management, on security issues respective of organizational uniqueness. In addition, the covered entity periodically should provide security training updates based on technology and security risks.

HITECH Revisions

The HITECH Act raises the bar for both covered entities and their business associates. It is more important than ever before to understand both the arrangements between covered entities and business associates, as well as training expectations. The HITECH addition of new federal privacy and security provisions does not relieve covered entities of their ongoing HIPAA privacy and security training requirements that state covered entities must continue to provide HIPAA training to "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."

In addition, all workforce members who could possibly be involved with PHI must be trained, including current and new employees, as well as retraining staff when changes occur in an organization's rules, policies, or procedures. Because the HITECH Act extends some HIPAA privacy and security provisions and adds new regulations that affect all workforce members, organizations must ensure their workforce is aware of these rules, how they are to be applied, and the procedures and policies for complying with them. Covered entities should work closely with business associates to ensure privacy and security training has occurred in accordance with HIPAA requirements.

In addition, section 13403(a) of the HITECH Act (Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act) requires the Secretary of Health and Human Services (HHS) designate an individual in each regional office of HHS. This individual is to offer guidance and education to covered entities, business associates, and

individuals about their rights and responsibilities under the HIPAA privacy and security rules. Organizations and providers can contact the regional office for additional training guidelines or resources. Covered entities must pay strict attention to the requirements spelled out in the HIPAA security rule, with the increased attention to auditing compliance, the current rules being altered and new rules initiated, and the potential for investigation into issues such as breaches, and educate staff accordingly.

State Laws and Regulations

Although 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 2008 hospital standards were modified to be consistent with HIPAA. Standards addressing information integrity and technologies include:

> **Standard IM.1.10**
> The hospital plans and designs information management processes to meet internal and external information needs.
>
> **Rationale:** Hospitals vary in size, complexity, governance, structure, decision-making processes, and resources. Information management systems and processes vary accordingly. Only by first identifying the information needs can one then evaluate the extent to which they are planned for and at what performance level the needs are being met. Planning for the management of information does not require a formal written information plan but does require evidence of a planned approach that identifies the hospital's information needs and supports its goals and objectives.
>
> **Standard IM.2.20**
> Information security, including data integrity, is maintained.
>
> **Rationale:** Policies and procedures address security procedures that allow only authorized staff to gain access to data and information. These policies range from access to the paper chart to the various security levels and distribution of passwords in an electronic system. The basic premise of the policies is to provide security and protection for sensitive patient, staff, and other information, while facilitating access to data by those who have a legitimate need. The capture, storage, and retrieval processes for data and information are designed to provide for timely access without compromising the data and information's security and integrity.
>
> **Standard IM.2.30**
> Continuity of information is maintained.
>
> **Rationale:** The purpose of the business continuity disaster recovery plan is to identify the most critical information needs for patient care, treatment, services, and business processes and the effect on the hospital if these information systems were severely interrupted. The plan identifies alternative means for processing data, providing for recovery of data, and returning to normal operations as soon as possible.[2]

Recommendations

If you have HIPAA privacy and security training responsibilities in your organization, the 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. Although the training standards apply to a universal audience when other portions of the administrative simplification 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 are critical because of 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. AHIMA recommends the following best practice guidance regarding privacy and security training procedures:

- General training must be provided for all workforce members, including contract workers, as a part of new hire orientation, before the first day of work in the staff member's actual department.
- Annual training is required of all staff.
- 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.
- Privacy and security training programs should include education (knowledge and understanding), training (how-to), and ongoing awareness. They should cover PHI in all forms including verbal, written, and electronic, and they should establish timelines for training new employees according to date of hire.
- Develop a responsive communication process to address questions that arise after training and in an ongoing manner.
- Develop a reference repository of up-to-date policies and procedures.
- Develop a process for evaluating training program effectiveness, reliability, and validity.
- Develop a verification process to ensure that users have completed security awareness training before receiving access to electronic PHI.

Who Is Trained

HIPAA's privacy rule defines workforce 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 workforce members on its privacy policies and procedures, as necessary and appropriate to carry out their function." In addition, covered entities must have and apply appropriate sanctions against workforce members who violate its privacy policies and procedures or the privacy rule itself.

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.

HITECH proposed a new definition of "workforce" to include "employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity or business associate, is under the direct control of such covered entity or business associate, whether or not they are paid by the covered entity or business associate."

Although covered entities are not responsible for training workforce members of a business associate, they should work closely with business associates to ensure all workforce members have documented privacy and security training. The definition of a business associate is found in section 164.308(b) of the security rule and section 164.502(e) of the privacy rule. On July 14, 2010, the Centers for Medicare and Medicaid Services released a proposed rule that would modify the definition of a business associate further. The proposed modifications suggest that term conform to the "statutory provisions of PSQIA, 42, USC 299b-21, *et seq.*, and the HITECH Act. In addition, modifications are made for the purpose of clarifying circumstances when a business associate relationship exists and for general clarification of the definition."[3]

These modifications, if finalized, will recognize organizations such as patient safety organizations, health information organizations, e-prescribing gateways, and vendors of personal health records as business associates. These proposed rules will clearly and explicitly establish a more active role between covered entities and business associates regarding privacy and security compliance. Therefore, business associates, defined under the HIPAA privacy and security rules, and their workforce members, defined under the HITECH Act, must be trained adequately regarding the privacy and security rules. Covered entities, in their agreements with business associates, may require the business associate to attest that training is being done

and/or provide documentation to indicate that training of the business associate's workforce, including subcontractors, is part of the requirements for doing business with the covered entity.

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, which key individuals are competent, and are they appropriate for ongoing instructor-led training?
- Does management have a role? Would management conduct general or role- or 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 HIPAA 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 HIPAA 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 HIPAA privacy and security rules address minimum training that requires scalability. 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 a training outline. The HITECH Act affects an organization's customized training efforts in terms of business associate training. The business associate agreements should dictate who will provide training, how often training is required, and who will maintain documentation of the training.

As you compile policies and procedures for training purposes, it will be evident that some are universal in application, whereas others are unique to roles and select positions. Consider creating levels of training. Level 1, for example, would entail the universally important education and training topics. Level 2 would include those particular to a role or job position and would be aligned closely 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 and supervisory staff may need specific training because of 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 including contractual staff, coders, volunteers, students, and new employees	• General confidentiality • Training requirements • Patient rights (general) • Reporting known or suspected breaches • Sanctions • E-mail • Faxing • Complaints • Use of social media • Reporting potential privacy or security violations	• General security policies • Physical and workstation security • Periodic security reminders • Virus protection • Importance of monitoring log-ins • Password management • Audits
2	All employees, volunteers, and students	• Special record handling	• Department security procedures • Software discipline
2	Release of information staff and management staff	• Federal and state laws • Consents and exclusions • Psychotherapy notes • Uses and disclosures or authorizations • Patient rights • Subpoenas, court orders • Copy charges • Reporting of inappropriate disclosures	• Audit trails
3	Management staff	• Department privacy and security training • Role and position assessments • Training program evaluations • Remediation procedures • Sanctions • Investigating suspected breaches, privacy and security violations	• Monitoring procedures • Role in ongoing awareness training • Privacy and security system assessment

It is helpful to prioritize the training protocol by weighing issues and groups affected by the privacy and security rules. For example, groups handling the greatest volume, highest information sensitivity levels, and areas of heightened risk concern would require more immediate training than groups needing only periodic access.

Level 1 General Training Examples

Level 1 privacy and security training should cover general baseline knowledge required of all staff members, regardless of position. Below are examples of general privacy and security topics to cover for all staff:

- Identification of organization privacy and security officer including contact information and the procedure for reporting complaints or violations
- General confidentiality policies and procedures, including governing laws and regulations and organizational policies
- General patient rights

- General security policies—organizations should consider including a security primer to increase understanding of information security and technology
- Understanding treatment, payment, operations
- Notice of privacy practices
- Physical and workstation security
- Periodic security reminders including why they are important and how they will be accomplished
- Virus protection including potential harm—how to prevent it and how to report it
- Importance of monitoring log-in success and failure and how to report discrepancies
- Password management including keeping passwords private, procedures for creating or changing passwords, 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 and security regulations
- E-mail procedures and best practices
- Faxing procedures and best practices
- Complaint reporting and investigation
- Verbal confidentiality policies and procedures
- Mitigating identity theft
- Destruction of sensitive information
- Access to health information including how to access personal health information and the procedures for requesting copies of health information
- Sanction policies and procedures
- How to report a privacy or security violation
- Social media policies and procedures

Consider adopting level 1 training content in new employee orientation after 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 2 or job-specific training, organizations should identify the necessary details for each staff member's positions. Determine how a person in a particular position uses health information and 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, observations, 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 2 Training Topic Examples

- Facility directories
- Appropriate access by staff
- Business associate agreements
- Marketing
- Fund-raising
- Psychotherapy notes
- Photography
- Disclosure, authorizations, and routine restrictions
- Redisclosure
- Patient rights including access, amendments, accounting of disclosures, and confidential communication
- Research
- Copy charges
- Deidentification
- Records retention
- Minimum necessary
- Aggregate data, required trending reports

For appropriate groups, cover:

- Policies for geographical considerations such as on-site, remote, at home, or physician offices
- Equipment nuances for laptops, PDAs, cell phones, and pagers
- Use of social media
- How to report a privacy or security violation

Level 3 Training Examples

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
- How to investigate privacy and security violations
- Knowledge of breach notification requirements
- Knowledge of business associate requirements

Training Delivery

How the training is delivered plays a role in how staff learn and retain the information. Organizations should consider the different ways groups and individuals learn best and make an effort to use a variety of learning techniques to 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 question-and-answer sessions are desired.
- Rotate presenters in instructor-led sessions.
- Computer-based training (PC, intranet, and Internet) can be effective for reaching large groups (it can include online assessments or quizzes for immediate feedback).
- Training laboratories provide hands-on opportunity.
- Videotapes can be used for varying audiences.
- Videoconferencing can be used.
- Distance training takes advantage of teaching tools developed by others, such as webcasts, informational Web sites, and online classes.
- Frequently asked questions and discussion threads can be valuable when they are easily accessible.
- If you are using handouts, display the information differently from its presentation on 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 updated easily).

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 workforce. 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 workforce 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 section 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."

The documentation for privacy and security training that shows that training was completed is likely to be combined. It is recommended that the documentation include content, training dates, and attendee names. Methods of documenting privacy and security training efforts include the following:

- Training program sign-in sheets
- Signed confidentiality statements acknowledging receipt and understanding of any training level attended
- Electronic access trails to record computer-based training completion or quiz results
- Documenting and retaining meeting handouts, aids, 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

Covered entities and business associates should ensure that ongoing training program assessments are documented, revisions to each program are based on the assessment results, and all documents created are maintained in accordance with HIPAA's retention requirement of six years.

Red Flags Rule

In addition to HIPAA and HITECH, the Federal Trade Commission's Red Flags Rule is scheduled to go into effect December 31, 2010. The rule will require that organizations train their staff on "red flags" that signal possible identity theft. The fact that the data stolen in such a situation might also qualify as PHI suggests that organizations can and should combine their HIPAA, ARRA, and red flags training.

Notes

1. HIPAA Privacy Rule, 45 CFR 164.530; HIPAA Security Rule, 45 CFR 164.308(a)(5)(i).
2. The Joint Commission. "Safely Implementing Health Information and Converging Technologies," Standard IM.1.10 (IM.01.01.01). Available online at www.jointcommission.org/NewsRoom/PressKits/Prevent+Technology-Related+Errors/app_standards.htm#1.
3. Department of Health and Human Services. "Modifications to the HIPAA Privacy, Security, and Enforcement Rules under the Health Information Technology for Economic and Clinical Health Act; Proposed Rule." *Federal Register*, 75, no. 134, (July 14, 2010). Available online at http://edocket.access.gpo.gov/2010/pdf/2010-16718.pdf.

References

Amatayakul, Margret, Joe Gillespie, and Tom Walsh. "What's Your HIPAA ETA?" *Journal of AHIMA* 73, no. 1 (Jan. 2002): 16A—16D. Available online in the AHIMA Body of Knowledge at www.ahima.org.

Association of American Medical Colleges. "Guidelines for Academic Medical Centers on Security and Privacy." May 2001. Available online at www.amc-hipaa.org/amchipaasecurityandprivacyguidelines.htm.

Department of Health and Human Services. "Health Insurance Reform: Security Standards; Final Rule." *Federal Register* 68, no. 34 (Feb. 20, 2003). Available online at http://edocket.access.gpo.gov/2003/pdf/03-3877.pdf.

Department of Health and Human Services. "Standards for Privacy of Individually Identifiable Health Information; Final Rule." *Federal Register* 67, no. 157 (Aug. 14, 2002). Available online at http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=2002_register&docid=02-20554-filed.pdf.

"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).

Hofman, Judi. "Surviving a CMS Security Investigation: A Real Life Experience." 2009 AHIMA Convention Proceedings, October 2009. Available online in the AHIMA Body of Knowledge at www.ahima.org.

The Joint Commission. *2004 Pre-publication Web Edition Accreditation Standards for Hospitals*. Oakbrook Terrace, IL: Joint Commission, 2003.

Rhodes, Harry, and Dan Rode. "HIPAA, Too: Many ARRA Privacy Provisions Amend HIPAA, Not Create New Regulation." *Journal of AHIMA* 81, no. 1 (Jan. 2010): 38—39. Available online in the AHIMA Body of Knowledge at www.ahima.org

Rode, Dan. "Reassessing Privacy and Security Compliance: ARRA Provisions Require Organizations Re-examine Procedures and Training." *Journal of AHIMA* 80, no. 10 (Oct. 2009): 20—22. Available online in the AHIMA Body of Knowledge at www.ahima.org.

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

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

Lou Ann Wiedemann, MS, RHIA, FAHIMA, CPEHR

Acknowledgments

Cecilia Backman, MBA, RHIA, CPHQ
Nancy Davis, MS, RHIA
Angela Dinh, MHA, RHIA, CHPS
Rose Dunn, MBA, RHIA, CPA, FACHE
Judi Hofman, CAP, CHP, CHSS
Suzy Johnson, MS, RHIA
Lesley Kadlec, RHIA
Nicole Miller, RHIA
John C. Parmigiani
Mary Stanfill, MBI, RHIA, CCS, CCS-P, FAHIMA
Diana Warner, MS, RHIA, CHPS
LaVonne Wieland, RHIA, CHP

Prepared by (original)

Beth Hjort, RHIA, CHP

Acknowledgments (original)

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

Article citation:
AHIMA. "HIPAA Privacy and Security Training (2010 update)." (Updated November 2010).
