Privacy and Security Training (2013 update) - Retired

Save to myBoK

Editor's note: This update replaces the November 2010 practice brief "HIPAA Privacy and Security Training."

On January 25, 2013, the U.S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR) published the long-awaited Health Insurance Portability and Accountability Act (HIPAA) Privacy Omnibus Rule in the Federal Register. As anticipated, the Omnibus Rule includes some of the most significant changes to patient privacy since HIPAA was first enacted in 2003. The Omnibus Rule went into effect on March 26, 2013, and covered entities must ensure compliance by September 23, 2013.

The good news is that the Omnibus Rule gives HIM professionals the opportunity to expand upon their already well-honed abilities to ensure the privacy and protection of patient health information. HIM professionals have always advocated for patient privacy within their healthcare organizations by insisting upon professional accountability and implementation of external directives. Many HIM professionals now serve in the role of Chief Privacy Officer, providing education to all members of the workforce as well as volunteers, trainees, temporary workers, students, subcontractors, and contractors. This education is critical to the ongoing organizational efforts to ensure patient privacy protection. However, this protection may be fragmented at best, depending on an organization's state of residence (i.e., state laws), program participation (e.g., Medicare, alcohol and drug abuse programs, and accreditation programs), and applicable federal laws.

Protecting patient privacy requires a delicate balance between restricting information to ensure confidentiality while also giving providers and others access to that information for patient care. Workforce awareness about sharing and using protected health information (PHI) is essential. In the past, employees may or may not have received training regarding confidentiality and privacy. However, today, most healthcare organizations provide some level of training—either formal or informal—in light of increased patient privacy regulations and awareness. The HIPAA privacy and security rules require formal education and training of the workforce to ensure ongoing accountability for privacy and security of PHI. HIPAA's privacy and security rules independently address training requirements. Like most standards, the training requirements are non-prescriptive, giving organizations flexibility in implementation.

The Health Information Technology for Economic and Clinical Health (HITECH) Act, published in February 2009, includes minor revisions to required training efforts. However, the HIPAA Omnibus Rule includes more substantive changes. This practice brief offers guidance to covered entities to aid in implementation of the training standards required by both HIPAA (including the Omnibus Rule) and the HITECH Act.

Note: The Omnibus Rule broadens the application of HIPAA privacy and security requirements to include both covered entities as well as business associates.

Federal Requirements

HIPAA Privacy Rule

Section 164.530 of the HIPAA privacy rule states:

(b) **1. Standard: training.** A covered entity and business associates 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 and business associates 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 and business associates 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 and business associates 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 and business associates 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 and its business associates must train their respective workforces 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 and business associates 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 and business associates should provide security training to their respective workforces, including management. In addition, covered entities and business associates should provide period security training updates via newsletters, email alerts, and pop-up screens.

Covered entities and their business associates must pay strict attention to the requirements spelled out in the HIPAA security rule. Covered entities should educate staff accordingly, particularly in light of increased breach investigations and compliance audits.

Omnibus Rule and HITECH Act Revisions

The HIPAA Omnibus Rule imposes more stringent privacy and security requirements upon both covered entities and their business associates. It's important to understand the relationship between the two entities as well as training expectations.

The HITECH addition of new federal privacy and security provisions doesn't relieve covered entities of their ongoing HIPAA privacy and security training requirements. These requirements state that 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."

All workforce members who use and access PHI, including current and new employees, must be trained. Staff members must receive re-training when changes occur to an organization's rules, policies, or procedures. An example is the HITECH new requirements for Right to Restrictions. The HITECH Act extends some HIPAA privacy and security provisions, and it also adds new regulations that affect all workforce members. Thus, organizations must ensure that members of their workforce are aware of these rules and their application as well as any relevant policies and procedures. Covered entities should work closely with business associates to ensure that privacy and security training occurs in accordance with HIPAA requirements.

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) to designate an individual in each regional office of HHS to offer guidance and education to covered entities, business associates, and individuals regarding their rights and responsibilities under the HIPAA privacy and security rules. Organizations and providers can contact their HHS regional office for additional training guidelines or resources.

State Laws and Regulations

Few states have regulations specifically requiring privacy and security training. However, any existing state regulations are preempted by HIPAA with the exception of cases with a more stringent status designation. Covered entities should be aware of any state regulations and ensure that training addresses the highest level of privacy and security requirements.

Accreditation

Joint Commission Standards

The 2013 standards are modified to ensure consistency with HIPAA requirements. The standards addressing information integrity and technologies include:

Standard IM.02.01.01: The organization protects the privacy of health information.

> Standard Introduction: The privacy of health information is a critical information management concern. Privacy of health information applies to electronic, paper and verbal communications. Protecting the privacy of health information is the responsibility of the entire organization. Organizations protect privacy by limiting the use of the information to only what is needed to provide care, treatment or services.*
>
> Privacy, along with security, results in the confidentiality of health information. Health information is kept confidential when the information is secure (kept from intentional harm) and its use is limited (privacy). The end result of protecting the security and privacy of the information system is the preservation of confidentiality. To illustrate this relationship, confidentiality is violated in situations when a patient's health information is used or accessed by an individual who does not have permission to access the information or uses it for purposes outside of delivering care, treatment or services. A confidentiality violation occurs when an individual is able to bypass security measures and system to gain access to health information.
>
> Footnote*: For additional guidance about limiting the use of information, refer to 45 CFR 164.502(b) and 164.514(d) under "Minimum Necessary" within the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

Standard IM.02.01.03: The organization maintains the security and integrity of health information.

> Standard Introduction: The integrity and security of health information are closely related. Health information is collected and processed through various information sources and systems throughout the organization. As a result, breaches in security can lead to the unauthorized disclosure or alteration of health information. When this occurs, the integrity of the data and information is compromised. Even simple mistakes, such as writing the incorrect date of service or diagnosis, can undermine data integrity just as easily as intentional breaches. For these reasons, an examination of the use of paper and electronic information systems is considered in the organization's approach to maintain the security and integrity of health information. Regardless of the type of system, security measures should address the use of security levels, passwords, and other forms of controlled access. Because information technology and its associated security measures are continuously changing, the

organization should do its best to stay informed about technological developments and best practices that can help it improve information security and therefore protect data integrity.

Monitoring access to health information can help organizations be vigilant about protecting health information security. Regular security audits can identify system vulnerabilities in addition to security policy violations. For example, as part of the process, the organization could identify system users who have altered, edited, or deleted information. The results from this audit process can be used to validate that user permissions are appropriately set. Conducting security audits can be particularly effective in identifying when employee turnover causes vulnerabilities in security because use access and permissions were not removed or updated.

Recommendations

HIM professionals who are responsible for providing HIPAA privacy and security training within their organizations can use the following information for program development.

General

Determining the most effective approach to training approach is a significant task. Healthcare organizations may be able to reduce the administrative burden and cost of privacy and security training by making such training part of a comprehensive HIPAA educational program or part of an even broader educational program. The privacy and security training standards apply to a universal audience; however, other portions of the administrative simplification (such as encryption protocols) may not. Planning and foresight can address audience overlap, reduce redundancies, and prevent multiple or conflicting messages.

Administration and senior management must receive management-level training so they can provide ongoing support and better understand the magnitude, cost, and complexity of the HIPAA requirements.

Similarities in the HIPAA privacy and security requirements invite combined training efforts. Both rules include ongoing training of all personnel as well as documentation of all training sessions provided. AHIMA recommends the following best practice guidance regarding HIPAA privacy and security training procedures:

- Provide general training for all workforce members, including contract workers.
- Establish timelines for training new employees according to their date of hire as a part of new hire orientation and before the staff member's first day of work in his or her department.
- Require annual training for all staff members.
- 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.
- Include in-depth education, how-to training, and ongoing awareness. The program should cover PHI in all forms, including verbal, written, and electronic.
- 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 privacy and security awareness training before receiving access to paper and 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 states that all workforce members must receive training on any "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 privacy policies and procedures or the privacy rule itself.

The HIPAA security rule states that a covered entity's training audience includes, "all members of its workforce (including management)." Understanding the breadth of the training audience is critical for both initial and ongoing training. A covered entity and business associate should define its training audience according to its operational structure and through careful consideration of a workforce member's access to PHI, responsibilities that present potential compliance risk, and contractual relationships that rely on access to PHI. Careful evaluation may introduce the importance of including individuals outside of

the rule definitions. These individuals may include part-time, contractual, temporary, home-based, and remote employees. They may also include management, the board of directors, physicians (on-site, in offices, and those working remotely), educators, students, researchers, and maintenance personnel.

The HITECH Act includes a new definition of workforce that encompasses "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 privacy and security training has been documented. Section 164.308(b) of the HIPAA security rule and Section 164.502(e) of the HIPAA privacy rule both define business associate. The Centers for Medicare and Medicaid Services (CMS) released a modification to this definition, suggesting that the term conform to the "statutory provisions of PSQIA, 42, USC 299b-21, et seq., and the HITECH Act." The modification also states that "modifications are made for the purpose of clarifying circumstances when a business associate relationship exists and for general clarification of the definition."

These modifications recognize certain entities (e.g., patient safety organizations, health information organizations, e-prescribing gateways, and vendors of personal health records) as business associates. Omnibus clearly and explicitly establishes 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)—as well as their workforce members (defined under the HITECH Act)—must receive adequate training regarding privacy and security. Covered entities may require a business associate to confirm that training, including subcontractor training, is performed. A business associate agreement may also require training as a prerequisite to be able to perform work with the covered entity.

Who Trains

Existing organizational structure will dictate a logical and workable approach for identifying trainers and accommodating HIPAA requirements. It's critical to establish clear accountability, appoint knowledgeable and qualified trainers, and clarify timelines and ongoing roles. Questions to consider include:

- Who are currently the most effective trainers in the organization?
- Has the organization appointed a HIPAA oversight team?
- Do the privacy officer and security officer positions or functions work together to encourage a unified and coordinated approach to compliance?
- What role should the human resources department play, particularly in terms of providing general training to new hires?
- If the organization implements a train-the-trainer model, what individuals will be involved in this method, and can they provide ongoing instructor-led training?
- What role does management play? Will it provide general training or more specialized job-specific or role-specific training?
- Will the organization designate point persons for department, section, or unit training?
- Will the organization retain consultant services for training? If so, what topics will those consultants cover?

What to Cover

The HIPAA privacy rule states that a covered entity's privacy program should include "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 an organization's operational nuances as well as specific job responsibilities. 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.

Consider creating levels of training. Level 1, for example, would entail the universally important education and training topics. Level 2 would include those topics that are particular to a role or job position and would be aligned closely with the need-to-know parameters identified for various positions.

Additional training levels may be necessary when increased knowledge and skills are required to carry out operations in a compliant manner. For example, management and supervisory staff members may need specific training because of their involvement in compliance functions. High-level training may be developed for the information systems staff members who must apply privacy policies in administering technological responsibilities. Be flexible by applying as many varied levels as necessary to accomplish training 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	• Monitoring procedures

		• Role and position assessments • Training program evaluations • Remediation procedures • Sanctions • Investigating suspected breaches, privacy and security violations	• Role in ongoing awareness training • Privacy and security system assessment

It's helpful to prioritize the training protocol so those who require training most urgently receive it as soon as possible. For example, groups handling the greatest volume of PHI or the most sensitive PHI, e.g. nursing, physicians, would require more immediate training than groups needing only periodic access to PHI, e.g. housekeeping.

Level 1 Training Examples

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

- Identification of the organization's privacy and security officers, including their 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 the potential for harm, how to prevent it, and how to report it when it does occur
- 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 (i.e., 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 PHI and the procedures for requesting copies of health information
- Sanction policies and procedures
- Non-retaliatory policy
- How to report a privacy, security, or potential breach incident
- Social media policies and procedures
- Individual accountability and responsibilities for organizational privacy and security
- Use of personal mobile devices (e.g., email, text, and photos)
- Risk of harm threshold and 4-step risk assessment to be completed in the determination of a breach

Consider incorporating Level 1 training content into a new employee's orientation after the first wave of training is complete upon hire (general orientation). Clearly communicate to new employees any plans for department- or unit-customized training

to supplement general training.

For level 2 or job-specific training, organizations should identify the each staff member's responsibilities that require access to and use of PHI. Determine how each employee uses health information and then develop training accordingly. Assessment tools, job descriptions, observations, and discussions with employees are important in developing job-specific training. See "Sample Privacy and Security Position Assessment" below.

Level 2 Training Examples

- Accessing facility directories
- Identifying appropriate staff member access to PHI
- Business associate agreements
- Changes to marketing and fundraising regulations
- Access to psychotherapy notes
- Photography
- Disclosure, authorizations, and routine restrictions
- Opting out (i.e., paying for services out-of-pocket)
- Redisclosure of PHI
- Patient rights, including access, amendments, accounting of disclosures, and confidential communication
- Research and authorization
- Charges and costs related to copies of PHI
- Deidentification of PHI
- Records retention
- Minimum necessary concept
- Reports with patient information
- Refresher training that covers all of the above with a focus on what is new in the HIPAA Omnibus Rule

Some individuals may require training on these topics:

- Policies with special geographical considerations, such as on-site, remote, at home, or physician offices that have to use VPN or other technologies
- Access Reports to monitor all patient care documentation accessed within a patient record
- Equipment requirements for safeguarding data on laptops, PDAs, cell phones, and pagers
- Use of social media
- Law enforcement regulations
- Release of information protocols for individuals who are deceased
- How to report a privacy or security violation

Level 3 Training Examples

Management-specific training should address these topics:

- How to conduct assessments to determine job-specific training for employees
- Conducting internal audits
- Accounting of disclosures
- Training program evaluations and modifications
- Ongoing awareness training or change updates
- Exceptions/accommodations made by special requests for communication under the Confidential Communications HIPAA requirement
- Remediation procedures
- Sanctions
- How to investigate privacy and security violations
- Breach notification requirements
- Business associate requirements
- Breach notification response team
- Changes to marketing and fund raising regulations
- Genetic Information Nondiscrimination Act (GINA)

- Opting out (paying for services out-of-pocket)
- Encryption practices
- Mobile devices (e.g., email, text, SMS, IM)

Training Delivery

The method of delivering information is a crucial part of whether and how workforce members learn and retain that information. Organizations should consider the different ways in which individuals learn and make an effort to use a variety of learning techniques to optimally present the material. Following are important points to consider:

- When planning audience participation, consider different knowledge levels.
- Recognize the potential for information overload to occur during training.
- Incorporate various learning techniques to address different learning styles, e.g. face to face, computer based, paper based, on the job.
- Ensure instructor-led discussions for in-depth training and when facilitating question-and-answer sessions.
- Rotate presenters during instructor-led sessions.
- Consider computer-based training (PC, intranet, and Internet) to reach large groups of individuals more easily. This training can include online assessments or quizzes for immediate feedback.
- Consider training laboratories to provide hands-on opportunity.
- Incorporate videotapes, webcasts, online classes, and videoconferencing, when necessary.
- Make frequently-asked questions and discussion threads easily accessible to staff members via a HIPAA intranet site or library.
- Ensure that any handouts are different from formal presentation slides to keep audience members' attention. For example, consider summarizing key points or including unique graphics on handouts provided.
- Consider developing training manuals to ensure consistency among trainers..
- Develop and deliver periodic updates that provide important reminders of core knowledge areas in HIPAA privacy, security, and breach notification.

Ongoing Training

According to the HIPAA privacy rule, "a covered entity and business associates must provide training to each member of their 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 helps to ensure ongoing compliance. It's important to determine how often members of the workforce will receive training reminders or refreshers and what will trigger those reminders. Most organizations will hold annual HIPAA or compliance refresher training.

For example, periodic reminders could include sign-on security prompts, information in company newsletters, lunchtime information sessions, information e-mail messages, or informational fliers or posters. Ensure a mechanism for updating the content of various training levels to reflect policy and procedure changes for affected individuals.

Documentation

The HIPAA 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."

Organizations will likely combine any documentation that demonstrates if privacy and security training has been completed. It's 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 for computer-based training completion or quiz results

- Meeting handouts, aids, and minutes
- E-mail messages
- A compliance training database recording details such as broadcast e-mails, flier distribution, launching of screen savers or banners, or cafeteria tent displays

Covered entities and business associates should ensure that ongoing training program assessments are documented. Revisions to each program should be based on the assessment results, and all documents created should be maintained in accordance with 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 (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). 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). 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.

The Joint Commission E-dition. July 1, 2013 *Accreditation Requirements Information Management.*Oakbrook Terrace, IL: The Joint Commission, 2013.

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.

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.

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

Kathy Downing, MA, RHIA, CHPS, PMP
Susan Lucci, RHIT, CHPS, CMT, AHDI-F
Diane M. Lerch, RHIA, CHPS, CCS, CHA

Acknowledgements

Becky Buegel, RHIA, CHP, CHC
Debbie Case, MBA, RHIT
Marlisa Coloso, RHIA, CCS
Angela Dinh Rose, MHA, RHIA, CHPS, FAHIMA
Kelly McLendon, RHIA, CHPS
Kim Turtle Dudgeon, RHIT, CHTS-IS/TS, CMT

Prepared by (2010)

Lou Ann Wiedemann, MS, RHIA, FAHIMA, CPEHR

Acknowledgments (2010)

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:
Downing, Kathy; Lucci, Susan; Lerch, Diane M. "Privacy and Security Training (2013 update) - Retired" (AHIMA Practice Brief, October 2013)
