

EDUCAUSE Center for Applied Research

Research Bulletin

Volume 2008, Issue 8

April 15, 2008

Regulatory Compliance Training: Public Jobs, Private Data

Ross T. Janssen, University of Minnesota

Greg C. Sales, Seward Incorporated



Faculty, staff, and students in institutions of higher education create, use, access, store, and share private data. Multiple types and staggering volumes of private data are shared as individuals carry out their various missions. Institutions must comply with a multitude of federal¹ and state² regulatory frameworks that affect the collection and use of private data including, but not limited to, student data, financial information, information about employees, information about individuals treated by university health care providers, and information about insurance benefits. Researchers are also increasingly subject to privacy and confidentiality regulations. The Federal Policy for Protection of Human Research Subjects, adopted by 17 federal agencies as a common regulatory framework (the "Common Rule") for most federally sponsored human-subjects research, mandates that institutional review boards (IRBs) address privacy and confidentiality concerns.³ The Common Rule requires IRBs to explicitly find that a researcher has proposed adequate protections to minimize the possibility of a breach of privacy or confidentiality.⁴ The Health Insurance Portability and Accountability Act (HIPAA) also establishes regulations for the use of health information in research.⁵

In spite of the proliferation of regulations, laws, and mandates, many institutions still experience significant data breaches.⁶ Security breaches that compromise private data can involve institutions in expensive,⁷ time-consuming, embarrassing, and complex recovery efforts. Some breaches even require the involvement of federal authorities.⁸

As the scope, breadth, and number of laws that regulate private data expand and evolve, institutions of higher education face a particularly daunting challenge in developing and implementing appropriate policies, procedures, and training to address the various regulatory requirements. Institutions must educate their community members about expectations around the collection, use, and disclosure of private data. Developing programs that provide education and awareness about the various compliance requirements can be costly and time-intensive. Even identifying who works with what type of data in order to deliver appropriate training to each individual is a major challenge.

For the University of Minnesota, several factors combined to highlight the need for raising awareness and educating its workforce about good data security and management practices. The HIPAA security regulations went into effect on April 14, 2003, requiring policies and procedures for securing electronic, protected health information and, like the HIPAA privacy regulations, mandating education and awareness about data security. In the summer of 2005, a new Minnesota law⁹ went into effect that requires the university to notify individuals if their data are compromised in a security breach. The breach notification law requires a process for reporting security breach incidents and developing criteria to determine when a notification of the incident would be required. Additionally, security breaches had been headline news on a regular basis, emphasizing the risks to the institution and the related costs. These events solidified the university's need to ensure that its community members understand what university data is private and how that data needs to be managed.

University faculty and administrative management decided to be proactive and provide individuals with a training and awareness program that incorporates the information they need to manage private data in a way that not only complies with the various laws and institutional policies but also meets the expectations of its constituents. The information is provided in “real life” examples of how data are used at a university. Information about how to securely manage private data is delivered in terms of best practices. The university wants its community to be able to spot security issues and have information and resources to resolve the issues in a way that best protects private data.

This research bulletin details the procedures and processes undertaken by the University of Minnesota to ensure that all employees, from student workers and custodial staff through senior research faculty and administrators, receive training about keeping private data secure, tailored to their roles and responsibilities. It illustrates how the implementation of the training resulted in improvements in incident reporting and response procedures, awareness of institutional private data and expectations for securing them, and many other aspects of data security.

Highlights of Employee Training Development and Implementation

To accomplish the required employee training, the University of Minnesota wanted to leverage existing online training developed to meet HIPAA privacy training requirements to develop a similar program that addressed not only HIPAA security requirements but also data security issues for other regulated, private university data. HIPAA is the first federal regulation that holds a covered entity¹⁰ accountable to train its employees and volunteers about the regulations’ requirements and the entity’s policies regarding health information privacy and security. For many large organizations, especially academic institutions that provide health care services, educate health professionals, and conduct medical research, the implications for implementing HIPAA training raise significant challenges. The university was forced to carefully examine the many complex relationships both within the institution and between the institution and affiliated organizations. These included the relationships between its clinical faculty and the hospitals and clinics in which they practice and teach, as well as the large number of workforce members and students in multiple disciplines who interact with protected health information (PHI). For HIPAA privacy training designed for individuals who deal with PHI, this meant that nearly 17,000 workforce members (including approximately 5,700 health professions students) across 252 university departments in more than 50 schools, colleges, and programs spread across four campuses in five cities needed to be educated about HIPAA based on their specific roles in the institution.

Having identified the need for broad-based data security training and an existing delivery model and platform, and seeking the best possible learning solutions, the university engaged an external instructional design consulting firm, Seward Incorporated, to work with the institution in a process known as the systematic design of instruction.¹¹ The first stage in this process was to conduct an analysis to determine what information needed to be included in the training program;¹² how the curriculum should be designed; what

the content should include, considering the diverse audience and skill set; how the content would be developed; and how and to whom the different program components should be delivered. The analysis process and findings are described below.

Front-End Analysis

A front-end analysis was conducted to produce a comprehensive understanding of the project's roots, its relationship to the earlier HIPAA e-learning efforts, the target audience(s), standards for success, and related information and expectations. The university, working with its consultants, undertook extensive and broad-reaching efforts to gather these data, recognizing their importance to the successful design, production, and implementation of the training program.

Meetings, focus groups, phone interviews, a review of existing university e-learning software, a review of online resources, and related activities were conducted in an effort to clearly identify training needs. Seven focus groups were convened. Participants in the focus groups represented a broad sampling of interested university offices, campuses, and end-user groups. Discussions addressing a series of training, security, and technology use questions were documented.

Individuals identified as having particular expertise that might inform the development of training content were contacted by e-mail and phone. They were interviewed to gather relevant information related to their specific areas of expertise, such as work processes, technology, or legal issues related to data security and training.

Existing online resources were examined, including HIPAA e-learning modules (<http://www.ahc.umn.edu/privacy/>), university policies and documents (<http://www.ahc.umn.edu/privacy/policies.html>), and public sites covering security, data privacy, and related topics (<http://www.cms.hhs.gov/>). This research was conducted both to identify training resources and to provide guidance for the design of an online training solution.

Data on measures of success for the e-learning projects, content areas and supporting resources, strategies for implementation and presentation of lessons, the readiness of university employees for e-learning, and anticipated levels of acceptance among employees for e-learning were gathered through these efforts.¹³ Major findings from the analysis and recommendations for creating an e-learning data security training program were contained in the consultant's report and presented to the project's leadership team.

Key recommendations included the following:

- The software design and development should be conducted in such a way as to allow the university to maintain and support the software with minimal effort.
- The e-learning product should be repeatedly and rigorously tested during development. Testing should address usability and user acceptance as well as functionality and operation within the variety of identified end-user environments.

- A formal, structured, multichannel, staged campaign would be the most effective method of promoting interest in e-learning and sustaining interest in the concepts it addresses.
- User access to the training modules should be as direct and easy as possible.
- Brief modules containing information relevant to all employees should be presented first.
- Modules should be delivered on a schedule that provides sufficient time between lessons for learners to process what they are learning.
- By the end of the three introductory modules, each learner should self-identify the remaining curriculum (for example, student records, financial data, personnel records, health information, or research data) by responding to questions about their roles and responsibilities at the university.
- A formal plan for ongoing maintenance and support should be developed by the university's project coordinators.

Development Process

Based on the findings from the front-end analysis, the university solicited proposals from e-learning consulting firms for the design and development of the training program. The winning proposal was written by Seward Incorporated. Seward's role was to work with university experts to design and develop the data management and security e-learning curriculum.

A collaborative development process was undertaken by the university and vendor, with each taking on significant roles. The core team consisted of representatives from the consulting firm with specializations in instructional design and e-learning development, project coordinators from the Academic Health Center, and individuals from the Offices of the Registrar, Comptroller, General Counsel, VP for Research, Information Technology, and Academic and Distributed Computer Services. External representatives from the Minnesota State Colleges and Universities system, which was also looking for a method of providing employee training, joined the team.

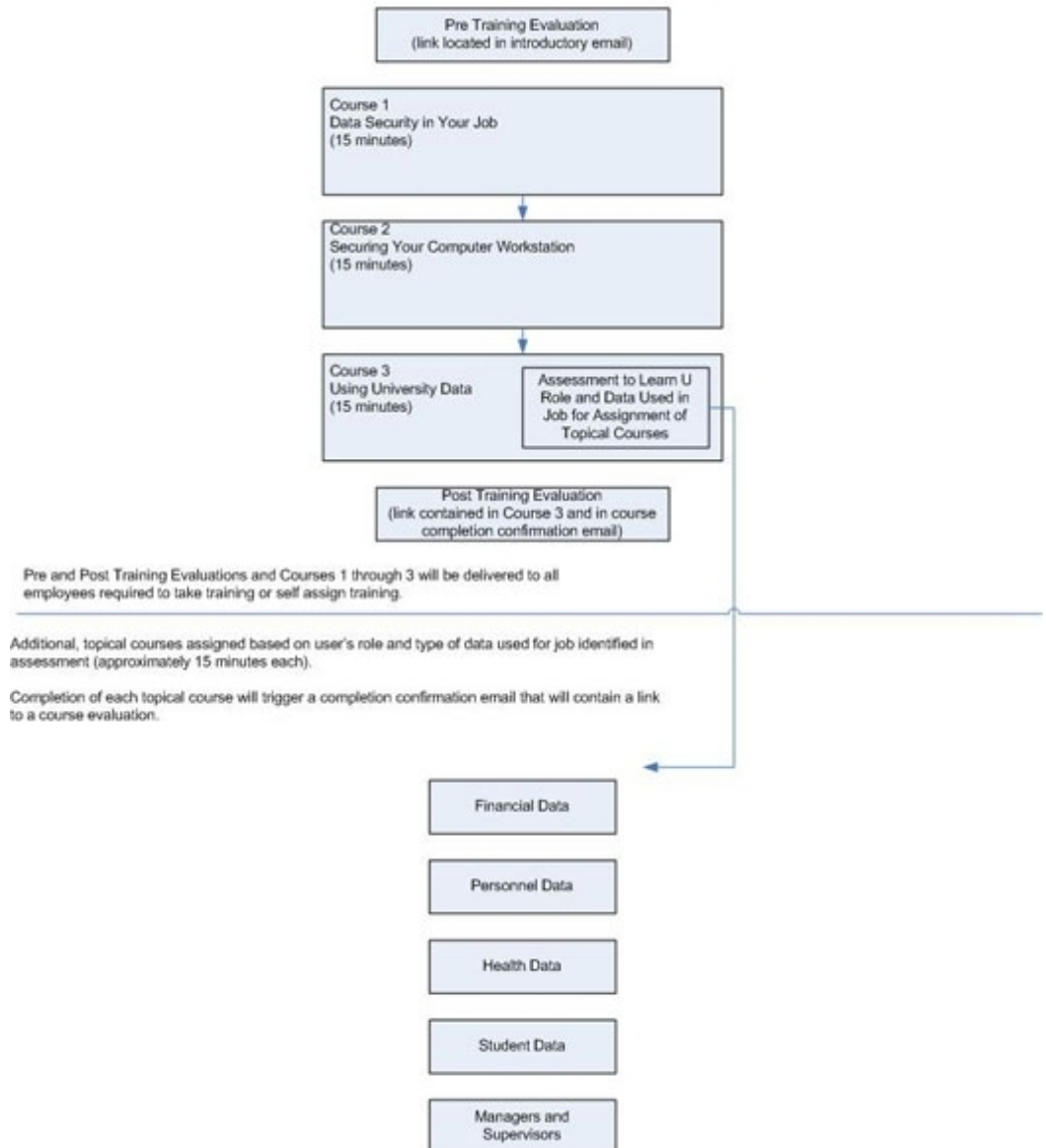
The core team worked to resolve a number of important process-, production-, and implementation-related challenges. These included determining what topics should be addressed in the training, deciding where the content would be "housed," specifying the process for writing content, reviewing and approving the training modules, addressing technical considerations, developing a dissemination plan, and articulating who would coordinate the release of the training and how the training would be tracked and reported.

For many of these tasks, the core team sought expertise from others within the university. These subject-matter experts provided input on security issues related to student, personnel, financial, and health data. This included "real life" scenarios where data security was or could be compromised, best practices, regulations, policies, and other resources.

A prototype of the software design was ready for usability testing within a few months of the project initiation. Five university employees representative of the end-user audiences (faculty member, civil servant, researcher, supervisor, student worker) were recruited to participate in the test. Testing was conducted in the university's Usability Services Lab. Results of the testing indicated users would benefit from a few minor modifications to the software design, such as more of an overview of the entire curriculum and more direct access to the training.

Development continued for nearly a year, resulting in an eight-course curriculum (see Figure 1). Three of the courses addressed general information that all university employees needed to know. The remaining courses focused in specialized areas and were required to be completed only by employees whose roles and responsibilities indicated the content would be relevant. In addition, surveys of employees' roles and responsibilities and confidence in data protection were developed.

Figure 1. University of Minnesota Privacy Training Curriculum



Delivery and Success of the Training Program

An online delivery approach was used to disseminate the system-wide training to and track its use by the 30,000-plus workforce of the University of Minnesota.¹⁴ The delivery effort needed to accommodate workers on multiple campuses in multiple cities across the state. Many technologies and processes were leveraged to develop a comprehensive and integrated course-delivery and tracking system. These included:

- **Identify, organize, and maintain groups of workforce members and students:** Completion of this task was required before we could assign training. An automated process was created to identify existing workforce members in the university's PeopleSoft Human Resource Management System and move them into groups defined within a tracking database. New employees and internal transfers are also identified and added to their respective group as soon as they are entered to the PeopleSoft system.
- **Assign coordinators to each group:** Once in the tracking system, each group is reviewed by local collegiate or departmental staff member to ensure accuracy, assist in coordinating communications, and monitor the training process.
- **Assign training courses:** Once individuals are in the tracking system, they are automatically assigned courses. All workforce members receive the first three primary courses. The courses are assigned at two-week intervals. Between course assignments, other awareness and communications materials are delivered to these individuals. The content of these communications coincides with content in the next course to be assigned.

At the end of the third course, each individual is required to complete a brief assessment that asks the person to identify his role at the university (faculty, staff, student, and volunteer). The assessment also asks individuals to identify what types of private data they work with (student, personnel, health, and financial). Based on the responses to the questions in the assessment, individuals are assigned additional topical courses for each type of private data they work with in their roles. There is also a course for those individuals who identify their role as a supervisor. This activity is also an informal and interesting assessment of how many people work with particular types of data, in what roles, and where in the organization.

- **Provide communications capability:** Learners are notified of the assignment of each course and the 90-day time frame in which they must complete it. The notification is made through an automated e-mail directing them to their personalized University of Minnesota portal pages. When learners authenticate to the portal, they see links to each of the training courses that have been assigned to them. Countdown information for the 90-day completion window is available for each course. If an individual exceeds the 90-day window on mandatory courses, the system sends a series of automated reminder e-mails. Sanctions (suspension of network authentication privileges) may be applied if the training is not completed after the third reminder is delivered.

- **Provide pre- and post-training survey for evaluative information:** To evaluate the effectiveness of the training program, the project team worked with the university's Office of Measurement to develop a pre-training survey that asked learners what their confidence level was in performing certain data management-related tasks. The survey is an online questionnaire that rates the individual's confidence level on a scale of 1 to 5.

After the completion of the final primary course, the learner is presented with the same online questionnaire asking the same questions. The results are compared to the responses to the first questionnaire to see if learners are more confident in identifying security incidents and managing private data more securely.

- **Reports:** The database developed to automatically track the completion of each course also provides various reports about progress with training for each individual, for the groups they belong to, and for larger associated groups (such as each campus). The reports are accessible to the local coordinators. Summary reports are automatically sent to unit leaders as well.
- **Reusability:** In the process of developing the tracking system, care was taken to create a reusable, scalable application. The tracking database has been duplicated for several other projects and compliance programs that require the system interfaces and interactive functionality we have developed.
- **Link management:** Each course of the training program is loaded into the campus-wide course management system. For system performance purposes, we limit enrollment in each course to approximately 250 learners. When a course fills up, we "clone" the course and enroll students in the newly cloned course. As a result, we have many clones of each course. The training program was specifically designed to incorporate the use of links where appropriate to take learners directly to policies and procedures, information on data security, and university resources available to users. These web pages change frequently, and the links in each of the course clones get broken. We developed a program that allows us to test links and to correct them when we find broken links. The program allows the correction to flow through course clones and to maintain active links.

Perhaps the most significant outcomes are increased knowledge, confidence, and skill among those trained, as indicated by responses to post-training surveys. Other notable successes include improvements in incident reporting across the institution, as measured by the integration of police, security, and risk-management office reports, as well as by an increase in the use of encryption on mobile devices and more formalized policies on data security.

What It Means to Higher Education

It is the ethical responsibility of higher education institutions, regardless of laws and regulations, to protect private and sensitive data they collect and maintain. Each institution's employees play a critical role in securing data that resides in the care of that institution. Some institutions, however, might not have taken the steps necessary to ensure that their employees understand their responsibilities in protecting data; safeguards they can implement to increase data security; procedures that must be followed in accessing, transporting, or sharing data; and the consequences that result from data breaches.

Like the experiences of many institutions needing to address data security training compliance, the project described here resulted from the need to find an expedient, effective, cost-effective, and manageable training solution. The solution used a systematic process to leverage existing technologies and content, involve key resources from both inside and outside the institution, add new content and techniques, and employ a new strategy for staging the release of training modules. The practices detailed here may be of value to others considering similar training needs.

Key Questions to Ask

- What regulations govern our storage and use of private data?
- How is our institution exposed to risks and penalties by data breaches?
- Does our institution have policies on data protection that comply with all relevant laws and regulations?
- How do we communicate policies and practices to employees?
- What assistance do we provide to build employees' skills and comfort levels for dealing with private data in the workplace?
- Does our institution have existing training or communication resources that will help us improve our employee training?
- Does our institution need to reexamine our approach to employee training around the protection of private or sensitive data?

Where to Learn More

- Horton, William. *Designing Web-Based Training: How to Teach Anyone Anything Anywhere Anytime*. Hoboken, NJ: John Wiley & Sons, 1993.
- Janssen, Ross T., and John Jensen. "Leveraging IT Infrastructure for HIPAA Training" (Research Bulletin, Issue 14). Boulder, CO: EDUCAUSE Center for Applied Research, 2004, available from <http://www.educause.edu/ecar>.

- Sales, Greg C. *A Quick Guide to e-Learning*. Andover, MN: Expert Publishing Inc., 2002.
- University of Georgia Office of Information Security, “State Security Breach Notification Laws,” <http://www.infosec.uga.edu/policymanagement/breachnotificationlaws.php>. This chart provides information regarding security breach notification legislation that has been enacted in U.S. jurisdictions.
- Sitko, Toby D., Norma K. S. Kenigsberg, Marilyn A. McMillan, and Pietrina Scaraglino. “Life with HIPAA: A Primer for Higher Education” (Research Bulletin, Issue 7). Boulder, CO: EDUCAUSE Center for Applied Research, 2003, available from <http://www.educause.edu/ecar>.

Endnotes

1. Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub. L. No. 104-191, August 1996, <http://www.cms.hhs.gov/HIPAAgenInfo/Downloads/HIPAALaw.pdf>; 45 CFR parts 160 and 162; 65 Fed. Reg. 50311 (Aug. 17, 2000); 65 Fed. Reg. 70507 (Nov. 24, 2000) (correcting certain minor errors); 68 Fed. Reg. 8381 (Feb. 20, 2003) (modifications); Sarbanes-Oxley Act of 2002, Pub. L. No. 107-204, 116 Stat. 745, July 30, 2002, <http://fl1.findlaw.com/news.findlaw.com/hdocs/docs/qwbush/sarbanesoxley072302.pdf>.
2. University of Georgia Office of Information Security, “State Security Breach Notification Laws,” <http://www.infosec.uga.edu/policymanagement/breachnotificationlaws.php>.
3. Criteria for IRB approval of research, 45 CFR § 46.111 (DHHS regulations).
4. Criteria for IRB approval of research, 45 CFR § 46.111(a)(7).
5. Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub. L. No. 104-191, § 264, 110 Stat. 1936, 2033 (codified at 42 USC § 132d-2(note)); Standards for Privacy of Individually Identifiable Health Information, 67 Fed. Reg. 53, 182 (Aug. 14, 2002).
6. David Austin, “Security Breach Upends College,” *The Oregonian*, September 28, 2007, <http://www.oregonlive.com/news/oregonian/index.ssf?base/news/119094815196650.xml&coll=7>.
7. The U.S. Department of Energy fined the University of California \$3 million for violations related to a security breach at Los Alamos National Laboratory. See www.nature.com/news/2007/071010/full/449649a.html.
8. Steven Musil, “FBI Probes Network Breach at Stanford,” *CNET News.com*, May 25, 2005, http://www.news.com/FBI-probes-network-breach-at-Stanford/2100-7349_3-5720754.html.
9. Minnesota Data Practices Act, Section 21. Effective August 2005, state agencies and the University of Minnesota now have a new responsibility that requires notification of individuals if there is a breach of security of certain private or sensitive data.
10. A “covered entity” is defined as a health plan, a health care clearinghouse, or a health care provider that transmits any health information in electronic form in connection with a covered transaction. Standards for Privacy of Individually Identifiable Health Information, 45 CFR § 160.103. For an explanation of how this HIPAA designation relates to higher education institutions, see Toby D. Sitko, Norma K. S. Kenigsberg, Marilyn A. McMillan, and Pietrina Scaraglino, “Life with HIPAA: A Primer for Higher Education” (Research

Bulletin, Issue 7) (Boulder, CO: EDUCAUSE Center for Applied Research, 2003), 4, available from <http://www.educause.edu/ecar>.

11. Walter O. Dick, Lou Carey, James O. Carey, *The Systematic Design of Instruction* (Boston: Allyn & Bacon, 2004).
12. Greg C. Sales, "Improving Return on Investment (ROI) Through Increased Attention to the Product Lifecycle," *Journal of Interactive Instruction Development* 15, no. 1 (2003): 27–30.
13. Greg C. Sales, "Developing Online Faculty Competencies," in *Encyclopedia of Distance Learning: Distance Learning Technologies and Applications*, ed. Patricia L. Rogers (Hershey, PA: Information Science Publishing, 2005).
14. All 30,000 members of the University of Minnesota workforce were required to take general data security training; 17,000 people who work with PHI were also required to take specialized HIPAA privacy training.

About the Authors

Ross T. Janssen (janss006@umn.edu) is Director of the University Privacy and Security Office and the Office of Occupational Health and Safety at the University of Minnesota.

Greg C. Sales (gsales@sewardinc.com) is President and CEO of Seward Incorporated.

Copyright

Copyright 2008 EDUCAUSE and Ross T. Janssen and Greg C. Sales. All rights reserved. This ECAR research bulletin is proprietary and intended for use only by subscribers. Reproduction, or distribution of ECAR research bulletins to those not formally affiliated with the subscribing organization, is strictly prohibited unless prior permission is granted by EDUCAUSE and the author.

Citation for This Work

Janssen, Ross T, and Greg C. Sales. "Regulatory Compliance Training: Public Jobs, Private Data" (Research Bulletin, Issue 8). Boulder, CO: EDUCAUSE Center for Applied Research, 2008, available from <http://www.educause.edu/ecar>.