Leveraging IT Infrastructure for HIPAA Training

Ross T. Janssen, University of Minnesota

John Jensen, University of Minnesota
In the fall of 2002, the University of Minnesota (UM), like all higher education institutions across the country that provide health care services, health plans, or health care clearinghouses, was faced with a daunting task. It needed to train almost its entire workforce (in varying degrees, no less) about their responsibilities and university policies and practices related to the privacy and security of health care information. And this needed to be accomplished by April 14, 2003—a timeframe of only six months. The training was mandated by the federal Health Insurance Portability and Accountability Act of 1996, or HIPAA. HIPAA is comprised of four sets of regulations that promulgate standards for: transactions and code sets; privacy; security; and unique identifiers for individuals, employers, health plans, and health care providers. The purpose of the regulations is to ensure health insurance portability, to require security for health information, to reduce fraud and abuse, and to enforce privacy standards for health information.

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 raised significant challenges for the enterprise. HIPAA forced institutions to carefully examine the many complex relationships within the university, including those among 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 that interact, in some way, with protected health information (PHI). At the University of Minnesota, nearly 17,000 workforce members (including approximately 5,700 health professions students) across 252 university departments in more than 50 schools, colleges, and programs (including six health professional schools and colleges) spread across four campuses in five cities would need to be educated about HIPAA and the university’s newly written policies and procedures for the protection of health information. And each person’s training had to be tailored to the specific role of that individual in the institution.

Privacy and security project managers at the university weighed the options. Should they try to schedule in-person training with everyone, and how would that be done? How could they accommodate work schedules and avoid loss of clinic time for health care workers? Would they have to arrange a training venue as large as a sports arena?

For the answers, they turned to the university’s vast network of resources—specifically, its enterprise business systems—to see if they could develop customized, online training courses with maximum flexibility for trainees. The result was the creation of a scaleable, password-protected system that not only tracked completed training modules but also alerted employees to training sessions yet to be completed. To date, the system has delivered more than 20,000 personalized HIPAA training programs that can be accessed at the individual’s convenience and can be completed at the individual’s own pace. By April 14, 2003—the deadline for compliance with the privacy standards—the university, within eight weeks, had assigned and delivered 46,851 HIPAA courses in individualized,
role-based sets to its 17,000 workforce members. Of the courses assigned and delivered, 45,766 were completed, yielding a completion rate of 97.7 percent.

The university’s solution was based on creatively determining which existing resources could be used or repurposed to meet the HIPAA training challenge. The required system was developed by “borrowing functionality” from various business systems used by the university. The system that was developed for HIPAA training proved so useful that it is being used for other applications at the university: it now tracks the delivery of online orientation to online courses for School of Nursing students, manages workflow for the creation and distribution of employee identification badges, and tracks compliance with required immunizations for health professions students. Other uses for the tool are planned for the near future.

**Highlights of HIPAA Training**

The HIPAA training project team established requirements for selecting training and developing a system to deliver, track, and report training results for more than 17,000 workforce members in a compressed timeframe. In addition to these requirements the team established the following requirements for the program.

- The training needed to be online, available 24 x 7, and able to be completed at the learner’s own pace—so busy people could start the training, stop if necessary, and pick up where they left off when they returned to the training.

- Workforce members needed to be presented with the appropriate combination of courses based on their role at the institution and their individual access to PHI.

- Workforce members needed to be notified about their status with respect to each course—which courses were completed, and which ones were outstanding.

- The privacy officer and 70+ privacy coordinators needed a mechanism to track real-time progress of workforce members for whom they were assigned responsibility. They also needed functionality that would allow them to “reach out and touch” workforce members who were not making adequate progress against their training deadlines.

- The courses themselves needed to be interactive and designed so that people taking the training could test how well they learned the competencies identified by the Education and Training Task Force. University leadership requested measurements developed to assess effectiveness through behavioral change. University leadership also requested that learners be given an opportunity to evaluate each of the courses.

- The courses had to incorporate links to newly written university policies and procedures and other resources available to learners.
The university project also needed to deliver and track customized HIPAA privacy training for a separate faculty physician corporation with more than 700 employees.

The university’s Privacy and Security Project took a collaborative approach that included hundreds of project team members across the system to develop an online multimedia training program that leveraged internal subject matter expertise and existing technology resources. The HIPAA privacy training program consists of an introductory video and three courses: Safeguarding PHI on Computers, Privacy and Confidentiality in Clinical Settings, and Privacy and Confidentiality in Research. Workforce members were required to complete the awareness video and possibly one or more of the three courses, depending on their role at the university and their access to protected information (see Figure 1).

**Figure 1. HIPAA Privacy Training Program**

Two large, institution-wide task forces were assembled and charged with HIPAA training—the Education and Training Task Force and the Technology Task Force. While the project employed a consulting instructional design team, the curriculum and course content were developed around competencies identified by the task forces and subject matter experts, including lawyers, technologists, clinicians, researchers, support staff, and educational professionals.
The technical components of the training and tracking system were created as a result of a collaborative effort among the university’s workforce members who would be taking the training and using the tracking system, Office of Information Technology personnel, Web development groups, course management system (WebCT) experts, Web designers, usability experts, database architects and administrators, project management professionals, and educational technology professionals.

In order to incorporate all of the functionality required for the HIPAA privacy training program, functionality in many existing systems was leveraged. A comprehensive model was developed to allow the university to meet its training objectives for the initial HIPAA training deadlines and for ongoing training of new workforce members and students. Figure 2 illustrates how various systems were integrated to provide a seamless training and tracking program. Each of the systems used is identified below with a description of the functionality leveraged and an explanation of its purpose within the training model.

**Figure 2. Integrating UM Systems for HIPAA Training**
Portal Application

To meet the needs and time constraints for the HIPAA compliance training program, the project needed to identify and use an existing online environment from which individuals could be linked to their personalized HIPAA training programs based on their role in the institution. The new university portal provided the solution. Not only is the portal a convenient address from which trainees can link to the enterprise learning management system, it also allowed developers to push personalized information to trainees about their training progress. Portal channels (RSS news feeds hooked up to the Academic Health Center’s content management system) also provided the opportunity for trainees to subscribe to updates about the project. All of this was accomplished by using the X.500 authentication system to establish portal accounts for each trainee. Once identified through authentication, trainees could view their personalized training programs through their portal accounts. The portal and authentication systems work together to allow trainees to pull information they want from various sources, including information about HIPAA training requirements and progress.

Authentication Application

The University of Minnesota had the good fortune of making some key technology decisions early on that allowed the project to hit the ground running. The decision to provide e-mail for everyone in 1991 led to the development of the X.500 directory, which allowed the university to authenticate users with a single sign-on to all enterprise systems. The university maintained the integrity of this system as it added new enterprise systems—it has made the authentication process using the directory available for the university’s wireless network and for local developers to authenticate to their system(s) with the single sign-on. The successful evolution of this system made it possible to provide HIPAA trainees with seamless access, functionality, and content from a variety of other enterprise systems.

HIPAA Tracking Tool

An Oracle database was developed to act as a sort of middleware between the university’s enterprise human resources and student systems (both PeopleSoft) and the portal. While much of the functionality that exists in the tracking tool could be delivered in the university enterprise systems, development of the tracking tool database became necessary under the severe time constraints faced by the project team. Decisions to modify or enhance enterprise systems and the programming and training required did not happen quickly or cheaply. By using a simple Oracle database with a Web-based interface, the team was able to quickly and inexpensively manage and direct information to produce necessary key functionalities required by the training program:

- **Organize and maintain groups of workforce members and students.**
  Because the university is a “covered entity” under the HIPAA Privacy Standards, it was required to identify workforce members across the institution that have access to PHI. To manage the HIPAA training task and to ensure compliance with the regulations, the institution looked at existing enterprise systems to find a way to sort the workforce into manageable groups. We found
the correct structure in the financial systems and keyed the trainee groups on department IDs. For the most part, the trainee database was populated by copying necessary information for each workforce member associated with a particular department ID into the database.

- **Map privacy coordinators to their groups.** To assign appropriate courses to individuals based on their role in the institution, we assigned privacy coordinators to groups. The coordinators were given access to the tracking tool, where they assigned appropriate courses for each individual in their group(s) and where they could monitor progress of the individuals in their group(s).

- **Assign HIPAA training courses.** The process for managing the assignment of coordinators to groups and individuals to groups was modeled after a university enterprise system called the Electronic Grants Management System. By delegating authority to coordinators, we leveraged departmental knowledge and put the authority for role-based course assignment close to the workforce members.

- **Allow coordinators to assign up to four alternates.** To make the larger groups more manageable for coordinators, we borrowed functionality from another university enterprise system called Financial FormsNirvana. This functionality allowed coordinators to assign alternates who in turn were granted access to assign training and communicate with groups they needed to monitor.

- **Provide communications capability.** The university e-mail system was also leveraged for the HIPAA training program. Coordinators use the tracking tool to "round up" individuals who have not completed a certain course and send them an e-mail reminding them that they need to continue training.

- **Provide reports.** Coordinators and other authorized individuals can log into the tracking system and view progress reports aggregated to various organizational levels (by department, by coordinator, by college, etc.).

- **Ensure reusability.** In the process of developing the tracking system, care was taken to create a reusable, scaleable application. By using general terminology, existing taxonomies, and functionality from other systems, the tracking tool can be duplicated and easily modified to track other activities, data, or events.

### What It Means to Higher Education

Higher education is faced with an expanding gauntlet of regulations that are making institutions more accountable for the privacy and security of data. Institutions are responding by developing compliance programs that include education, policies, and procedures intended to reduce institutional risk. Institutions may be able to reduce the cost of compliance and consolidate training and tracking efforts by leveraging existing IT infrastructure.

By strategically integrating back-end functionality of existing systems, it is possible to develop a general tracking tool with delegated authority that is flexible enough to track
any number and type of data—not just HIPAA-related information. The university has found other uses for such a tracking tool:

- The Academic Health Center Office of Education has partnered with the university student health services provider to create a slightly modified version of the HIPAA tracking tool called AHC-Utrack for the purpose of monitoring health professions students’ immunization requirements.

- The university School of Nursing is using a slightly modified version of the tracking tool to track the completion of a required online orientation to online courses.

- The Academic Health Center is using a modified version of the tracking tool to track information about security badges for employees.

- A private corporation is using the HIPAA tracking tool to coordinate and track HIPAA training for its employees.

In addition to these purposes, a project charter has been approved that provides for the employment of the HIPAA tracking tool to coordinate and track HIPAA training specific to certain affiliated Twin Cities hospitals and their residents. Other planned uses for the tracking system include managing subscriptions to e-newsletters, tracking auditing and monitoring efforts, tracking and reporting information about university affiliation agreements, providing functionality as an educational technology project clearinghouse, and tracking and reporting HIPAA security training.

The HIPAA training and tracking model developed by the university can easily be transferred to other enterprises and institutions. The university model integrates functionality from various systems for the purposes described in Table 1 below.

<table>
<thead>
<tr>
<th>System</th>
<th>General Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Financial and HR enterprise systems</td>
<td>Identify and sort users and provide relevant information</td>
</tr>
<tr>
<td></td>
<td>Identify new employees and those who have separated from the institution</td>
</tr>
<tr>
<td>Portal</td>
<td>Link trainees to HIPAA courses</td>
</tr>
<tr>
<td></td>
<td>Communicate training progress</td>
</tr>
<tr>
<td>Authentication system</td>
<td>Identify trainees and match them with appropriate courses and progress information</td>
</tr>
<tr>
<td>Learning management system (WebCT, Blackboard, or other)</td>
<td>Deliver training content and quizzes</td>
</tr>
<tr>
<td></td>
<td>“Bookmark” location within course modules</td>
</tr>
<tr>
<td></td>
<td>Track module and course completion</td>
</tr>
<tr>
<td>Oracle database</td>
<td>Receive data from the data warehouse to create and manage lists of required employee and student trainees</td>
</tr>
<tr>
<td></td>
<td>Receive data from payroll system to sort trainees into groups and to assign groups to coordinators</td>
</tr>
<tr>
<td></td>
<td>Track assigned courses</td>
</tr>
<tr>
<td></td>
<td>Track course completion dates</td>
</tr>
<tr>
<td></td>
<td>Record comments about trainees</td>
</tr>
<tr>
<td></td>
<td>Generate automated e-mails to trainees</td>
</tr>
<tr>
<td>Reporting system (Cognos)</td>
<td>Generate reports</td>
</tr>
<tr>
<td>Web mail</td>
<td>Deliver reminder and thank-you e-mails</td>
</tr>
</tbody>
</table>
Not all institutions have precisely the systems identified in Table 1, but many have other institutional applications that can provide data to accomplish the same purpose. The university model is based on the use of a simple database set up to receive data from the various systems automatically and to be refreshed at least daily with new data. Depending on the size of the institution, some components of the model could be addressed by manually entering data. The university model was designed to be as automated as reasonably possible to help bring the institution into compliance with HIPAA within a very compressed time frame and also to maximize opportunities to enhance productivity and reduce project costs.

The university model addresses productivity issues in two major ways. It minimizes soft and real costs associated with employees taking time from their work to be trained by making the training available online 24 x 7 and by saving trainees’ places in a given module and allowing them to pick up where they left off. It also addresses productivity by automating some of the communications process and by giving the Privacy Coordinators a tracking tool that allows them to manage their group’s training progress from one site. The tracking tool is enhancing productivity in other areas that are using the tool by automating business processes. A conscious effort was made to create a tracking tool that leverages and enhances existing infrastructure by interfacing the tool with systems and functionality needed for the training program. Some “bridges” needed to be built between systems, but little technical invention was required.

While every institution must take an approach to HIPAA compliance that is reasonable for that institution, many have an information technology infrastructure that can be leveraged for compliance purposes. One approach to challenges like the ones confronted by the university is a collaborative approach that taps internal expertise necessary for the project. The university also used work groups to identify the key competencies for the training program, the issues that needed to be addressed, and the technology solutions for them.

**Implementation Challenges**

Some of the issues encountered with the deployment of this massive required online training program are described below.

- **Determining the scope and size of the workforce.** To discover how much of the workforce would require training, questionnaires were sent to departmental leaders. In cases where departmental responses indicated access to PHI, follow-up interviews were conducted to determine to what extent employees in that department needed training.

- **Developing a communications plan.** A major implementation challenge centered on the communications aspect of getting more than 17,000 people who were geographically separated to take the training at roughly the same time. The project took direction from internal communications professionals. A very effective and comprehensive communications plan was developed and implemented. The key components of the plan included urgent messages from top leadership and using existing communications vehicles to remind people about their responsibility for the privacy and security of data and for taking their
HIPAA training. By the time training was ready, people understood what was expected of them.

- **Supplying and supporting the required technology.** To make the training courses interactive, some of the course content was designed in Flash. Streaming video technology was used to deliver the introductory video online. The Flash content and the QuickTime video required certain plug-ins to be installed on trainees’ computers. For those with older computers, this required downloading the plug-ins from the Internet. Given the number of workforce members, this became a constant challenge. Help was available online, by phone, by e-mail, and in person.

- **Providing help and assistance to a large workforce.** In addition to the technical challenges people faced with the online HIPAA training, they had questions about the HIPAA regulations and what they meant. To manage the inquiries, central university help desk staff members were trained on HIPAA and the technology used for the online training so they could triage the questions. When people started really learning about the new HIPAA-driven institutional policies and procedures through the training program, the help desk was receiving hundreds of e-mails and phone calls daily.

### Key Questions to Ask

- Which parts of your campus IT infrastructure can be leveraged to provide enterprise-wide training?
- To what degree can online training methodologies used for HIPAA be adapted for other training efforts?
- How can the information technology infrastructure be architected to facilitate both academic and administrative learning?
- Can the tracking system be repurposed for other tasks?

### Where to Learn More


### Endnotes


6. Protected health information (PHI) is individually identifiable information, including demographic information, related to the past, present, or future physical or mental health or condition, the provision of health to an individual, or the past, present, or future payment for such health care, that is created or received by a covered entity. The form of the PHI is irrelevant and may be oral or recorded in any medium, including electronic data, paper records, or any other form. C.F.R. §§ 160.103.

7. The University of Minnesota has campuses in Crookston, Duluth, Morris, and the Twin Cities. The Twin Cities campus is in both St. Paul and Minneapolis.

8. The university-wide Education and Training Task Force included 34 faculty, staff, and student members who were charged with the development of a curriculum plan that would address the HIPAA competencies required of health professional students, staff, and faculty. Included are information technology competencies and knowledge required of other health data laws, policies, and best practices. View the task force membership at <http://www.ahc.umn.edu/ahc_content/about/privacy/> by selecting Privacy and Security at the U of M link, followed by Education and Training Task Force.
9. The university-wide Technology Task Force had 28 faculty, staff, and student members who were charged with the development of a technical infrastructure plan that would address access to clinical data for education, research, and clinical care. View the task force membership at <http://www.ahc.umn.edu/ahc_content/about/privacy/> by selecting Privacy and Security at the U of M, followed by Technology Task Force.


About the Authors

At the University of Minnesota Ross T. Janssen (janss006@umn.edu) is Director of Educational Technology and HIPAA Privacy and Security Officer and John Jensen (jense100@umn.edu) is a Program Associate in the Academic Health Center Office of the Senior Vice President for Health Sciences and Coordinator of the University Privacy and Security Project.