

# Three Steps to Increasing Employee Information Security Awareness

Save to myBoK

by Karen Czirr, MS, RHIA

---

Driven by current and potential privacy regulations and legislation, the Children's Hospital of Philadelphia (CHOP) decided to address employee understanding of information security. In 1999, CHOP, comprised of a hospital, rehabilitation facility, physician offices, satellites, and ambulatory programs, began to build a comprehensive employee awareness program on confidentiality and security of patient and hospital information.

With the Joint Commission on Accreditation of Healthcare Organizations and the Health Insurance Portability and Accountability Act in mind, our first step was to define our operational goals. These included:

- improve understanding of privacy, confidentiality, and security issues
- increase awareness of behavior and practices
- implement and manage appropriate information security practices
- assist individuals in taking responsibility for their actions
- assess, develop, and maintain competence to meet CHOP expectation
- serve all users, including vendors, volunteers, contractors, researchers, students, clinical staff, and others

We realized that there were two distinct groups of employees we needed to reach—new and experienced. New employees need general information about the CHOP network. But historically, new employee orientation programs are exercises in information overload. We wanted to communicate confidentiality and security guidelines so that employees would remember the critical elements at the appropriate times.

Our experienced employees have more insight into the operations of the CHOP network as well as a working knowledge of our clinical, financial, and communications infrastructure. They needed an annual education program to refresh their knowledge. Finally, we wanted to develop a users' guide to confidentiality and security of patient and institutional information. As a result, we decided to develop a three-phase awareness program.

## Phase I: Initiating the Newcomers

Our first awareness program is designed to be used at new employee orientation. General orientation is held at the hospital and is mandatory for all new employees regardless of their final work location. The 30-minute confidentiality and security presentation, "Information Security Awareness," includes computer slides and a brief video.<sup>1</sup> The video reinforces the information covered in the slide presentation. The language of the presentation is simple and easy to understand. Topics include the importance of the security awareness program, definitions of confidentiality and information security, legal and federal mandates, and an assessment of employee behavior. Also covered are the proper use of e-mail, cellular phones, voice mail, copy machines, fax machines, and computers. At the conclusion of the orientation program, each employee signs a statement attesting that they have attended orientation and are aware of all the topics presented. This document is kept on file in the human resources department.

## Phase II: Reviews for Current Employees

Phase II of the awareness program is designed for all other employees and is part of our annual mandatory education program. The 60-minute presentation, "Confidentiality of Patient and Institutional Information," consists of computer slides and a short video.<sup>2</sup> Again, the language of the program is basic and easily understood. Topics include all of those discussed in Phase I but in a greater level of detail. For example, in Phase I we explain that e-mail is to be used for hospital business and messages should not contain confidential patient or institutional information. In Phase II, we add that e-mail is not secure when used to exchange information across the Internet, that the e-mail system is the property of the hospital, and that the hospital reserves the right to monitor all e-mail messages. This presentation focuses on patient trust, the hospital's legal obligation to maintain the confidentiality of all hospital and patient-identifiable information, and breaches in confidentiality. Also included are reminders of the disciplinary process should policy violations occur.

At the conclusion of the presentation, there is a question-and-answer period and a test. Each employee is asked to sign a confidentiality agreement that is kept on file by his or her department supervisor. This agreement reinforces understanding of the material presented and serves as a reminder of each person's responsibility to protect and maintain the confidentiality of hospital and patient information.

The program is undergoing testing in hospital departments and in satellite locations in the form of in-service education. Feedback on relevance, the need to communicate this information with employees, and the slide presentation technique is consistently positive.

### **Taking It to the Intranet**

A computer-based version of the awareness program is currently in development for use on the CHOP intranet (CHOPnet). Annual mandatory education on fire safety, infection control, and hazardous chemical safety is already on the CHOPnet and computer-based instruction has proven to be cost-effective and efficient. The fact that it is self-paced and flexible and actively engages the employee in the educational process increases employee satisfaction. The immediate feedback enables the employee and manager to assess the progress of the employee and offers clues about program deficiencies.

Further, 24-hour access to the education program saves time and space and reduces or eliminates travel requirements for those working in satellite facilities. Overall, annual mandatory education can be monitored more closely and status reports to managers are provided in a more timely manner, so that 100 percent compliance is assured.

In order to migrate to an online version, the material in our present slide presentation will need to be abridged without sacrificing content, while also including a test and confidentiality agreement. Once the program is up and running, the employee will sign on using his or her unique ID and password and select the security awareness program. After reading the instructions and completing the slide show, the employee will take a brief true/false quiz so that new knowledge can be verified right away. When a passing score is achieved, the confidentiality agreement appears for review. By answering "yes" to the statement "*I have reviewed the confidentiality agreement and agree with directives as stated,*" the employee is prompted to submit results to human resources for file maintenance. He or she is also able to print the score and submit it to the supervisor as confirmation that the mandatory education for security awareness has been completed.

### **Phase III: Writing the Book**

Phase III of the security awareness program will be an employee handbook, which is currently in development. It will address all the topics mentioned in Phase I and II and reference relevant hospital policies, provide links to other resources on security and confidentiality, address frequently asked questions and list telephone numbers and contact names for specific issues. The handbook will be available initially in hard copy, but as CHOP becomes more wired, it will be available online to everyone who has access to the CHOPnet.

### **Notes**

1. *Confidentially Speaking*. 14 min. Oregon Health Information Management Association, 1992. Available at [www.orhima.org/products/products.html](http://www.orhima.org/products/products.html). Videocassette.
2. *Keeping It Confidential*. 18 min. Oregon Health Information Management Association, 1998. Available at [www.orhima.org/products/products.html](http://www.orhima.org/products/products.html). Videocassette.

**Karen Czirr** is information security manager of the Children's Hospital of Philadelphia. She can be reached at [czirr@email.chop.edu](mailto:czirr@email.chop.edu).

---

**Article citation:**

Czirr, Karen. "Three Steps to Increasing Employee Information Security Awareness." *Journal of AHIMA* 71, no.7 (2000): 30-31.

---

Driving the Power of Knowledge

Copyright 2022 by The American Health Information Management Association. All Rights Reserved.