Team Approach to Managing an Information Security Program

by Cindy Zakoworotny, MS, RRA, Cheryl Rutz, MA, MT (ASCP), and Cheryl Zwingman-Bagley, MSN, RN, CNAAA

In 1994, Hartford Hospital began to prepare for a 1995 survey by the Joint Commission on Accreditation of Healthcare Organizations. In reviewing the hospital's policies, it was clear that they addressed the assignment of user IDs and passwords for a mainframe environment rather than a network environment connecting geographically distant campuses. The installation of sophisticated, state-of-the-art systems, proliferation of personal computers, and roll-out of the hospital's clinical repository-Open Architecture Clinical Information System (OACIS) required updated policies addressing the current environment and associated privacy and confidentiality issues.

Background

Hartford Hospital is an 879-bed, private, tertiary care, teaching hospital. It is one of the largest hospitals in New England, specializing in organ transplantation. Hartford Hospital houses Connecticut's two air-ambulance helicopters/flying intensive care units, and it serves as a level 1 trauma center. The medical staff includes 808 physicians.

Residents, fellows, and medical students in 16 clinical disciplines receive training at Hartford Hospital. Connecticut Health System is Hartford Hospital's parent corporation. Connecticut Health System has affiliations and partnerships with other healthcare organizations throughout the state, such as Connecticut Children's Medical Center, Veteran's Memorial Medical Center, Immediate Medical Care Centers, Hartford Physician's Hospital Organization, Office of Professional Services, and the Institute of Living.

Hartford Hospital was a mainframe shop until 1990. Computer connections were hard wired and a mainframe package with audit trails controlled access. The hospital's programming and technical staff designed, coded, and maintained the hospital's systems. Job description defined levels of access to all systems. Information Services managed users' IDs and passwords. The drawback to this idyllic world of security was the lack of computerization in most departments at Hartford Hospital.

Funding for personal computers was not available for Hartford Hospital until 1989. At that time an Executive Information Committee (EIC) was formed-the formal planning and policymaking body for the hospitalwide Information Systems Strategic Plan. With EIC approval, the hospital hired a consultant to develop information security policies, standards, and guidelines. The project began with interviews with Connecticut Health System members. Based on interview findings, policies were developed and eventually approved by the Hartford Hospital EIC in December 1995. Connecticut Health System approved the policies, systemwide, in June 1996.

The Medical Record Department historically had served as the designated gatekeeper of medical record information in the paper environment, but with the electronic medical record based in Information Services, the role of the Medical Record Department was unclear. The new policies did establish that Information Services was responsible for physical system security and the Medical Record Department was the arbitrator of confidentiality issues.

In 1990, Hartford Hospital began a program called Patient-Centered Redesign with a grant from the Pew Charitable Trusts and the Robert Wood Johnson Foundation. This program brought about a shift in the hospital's culture toward collaborative, interdisciplinary, systems-oriented team concepts. Within the Patient-Centered Redesign framework, a multidisciplinary team for managing information security was proposed.

Overview of the Information Security Coordination Team

The Information Security Coordination Team at Hartford Hospital is a three-member team with representation from the Medical Record and Information Services departments and the clinical services. The Medical Record Department director is the team leader. The Information Services representative is the data administrator who participated in the hospital policy development process. The clinical representative is a registered nurse who is currently accountable for redesign and implementation of the Patient-Centered Care Delivery Model, the result of Patient-Centered Redesign. A clinical representative was recommended because the majority of business information within a healthcare organization is clinical. All team members must demonstrate a visionary view of the organization and healthcare.

The role of the Security Coordination Team is to:

- Coordinate all activities related to privacy, security, and confidentiality of information
- Develop and implement the principles, structure, and tools to assure protection of information while balancing access needs
- Partner with all users and share accountability for compliance

The team's overall responsibility is to ensure that the organization takes the appropriate steps to protect confidentiality, integrity, and availability of patient, employee, administrative, financial, marketing, and business information.

The team initiated the security process with the following tasks:

1. Develop standards and procedures
2. Create partnerships with other members of Connecticut Health Systems that use Hartford Hospital's information systems
3. Hire an information security coordinator to serve as staff to the Information Security Coordination Team
4. Serve as a resource to the OACIS Team for questions on balancing access with security
5. Develop an access audit process
6. Develop customer-specific education programs
7. Evaluate paper disposal options

The Medical Record Department's Role

Based on feedback from the hospitalwide interviews, the Medical Record Department was perceived as the patient's hospital-based agent for protecting confidentiality. In addition, from the director's perspective, it was important for the Medical Record Department to assume leadership to clearly establish its role in an electronic medical record environment.

The information security policies at Hartford Hospital designate the director of the Medical Record Department as the "owner/agent" of patient-identifiable information. The hospital's security standards define an information owner as "the manager of the organizational unit that has the primary responsibility for the information to perform its business function." As "owner/agent" the designee has custodial responsibility for that information. As owner/agent of patient-identifiable information, the Medical Record Department's responsibilities include:

- Determine the classification of information-public, internal, confidential, and registered confidential
- Authorize access to the information
- Implement controls to protect the information

Team members perform high-level planning, organizing, directing, communicating, and reporting functions. Daily security activities require staff support. Because of its historical position as patient information security manager, the Medical Record Department reallocated funds to create a staff position that would provide support to the Information Security Coordination Team. By establishing a formal security position, the Medical Record Department heightened the visibility of its information management role at Hartford Hospital.

The Information Security Coordinator

Role and Responsibilities

The information security coordinator is the process owner of the security function at Hartford Hospital. The coordinator's primary role is to create information security savoir faire among hospital staff, volunteers, students, medical staff, and

residents. The information security coordinator also serves as an internal consultant to health care teams and managers. In this capacity, the security coordinator identifies exposure and risks to confidentiality, integrity, and availability of patient, caregiver, and business information.

The information security coordinator implements standards developed by the Information Security Coordination Team. Functionally, this translates to

1. Providing hospitalwide awareness and direction to staff members through education and individual meetings and consultations

2. Understanding hospitalwide department-based automated applications in order to assist managers in the development of information security procedures that meet the hospital standards

3. Assisting Information Services in the development of audit trails and computer-based applications that provide the controls in the computerized patient record that will assure that patient-identifiable information is accessible only to authorized individuals on a need-to-know basis

   The team wanted the information security coordinator to be perceived by collaborative management teams and managers as a facilitator, liaison, consultant, and resource. Thus, the coordinator acts as an ambassador for the Information Security Coordination Team, which has the goal of developing customer/client relationships. Exhibit 1 provides a detailed description of the role of the information security coordinator at Hartford Hospital.

Exhibit 1

Hartford Hospital Medical Record Department
Role Description: Information Security Coordinator

Position Summary

The information security coordinator serves as support staff to the hospital's Information Security Coordination Team. In this capacity, the information security coordinator coordinates ongoing activities to protect the confidentiality and integrity of computer-based patient, physician, and employee information in compliance with the hospital's Information Security Program. The information security coordinator serves as a major stakeholder in creating information security awareness within the Hartford Hospital culture.

Key Accountabilities

Major Responsibility 1
Provide information security awareness training to all levels of management and to all employees and staff members

Supporting Actions:

- Develop new employee orientation program highlighting key information security policies and standards
- Provide education sessions to health care teams, managers, owners/agents of information, and application managers
- Develop and present ongoing information security awareness programs

Major Responsibility 2
Serve as a resource to the Information Security Coordination Team in managing the business functions of the Security Program

Supporting Actions:

- Document policies and procedures developed by the Information Security Coordination Team
- Record minutes of Information Security Coordination Team meetings
- Develop and implement format for ongoing review and revision of Hartford Hospital Information security policies, standards, and guidelines

- Prepare quarterly status report for Information Security Coordination Team reflecting Joint Commission compliance, training, audit issues, risk assessments, and other pertinent programs

Major Responsibility 3
Serve as a hospital-based information security consultant to health care teams and managers

Supporting Actions:

- Provide guidance to managers and health care teams when information security questions and concerns arise
- Assist managers in defining appropriate access levels for staff
- Assist managers with the design of department-specific information security procedures
- Serve as security resource for staff throughout the hospital relating to access to patient, employee, and physician information
- Assist OACIS Team with the development of audit trails and computer-based applications to administer security
- Serve as principal representative for information security on various teams, task forces, and committees
- Work with internal Audit Department to develop monitoring and reporting structures

Major Responsibility 4
Provide day-to-day management of the hospital's Information Security Program

Supporting Actions:

- Provide support on demand to Information Services staff responsible for processing access requests
- Monitor and evaluate audit trails for possible security exposures
- Handle phone calls from individuals reporting breach of confidentiality and/or security
- Investigate and report threats to confidentiality and security

Qualifications

Education:

- Bachelor's degree from an accredited health information program

Credentials:

- Registered Record Administrator

Experience/Training:

- Four or more years of health information management experience
- In-depth understanding of the patient care environment, information systems and networks, information needs, and information handling procedures of the hospital
- Strong computer/PC skills essential

Job Skills:

- Knowledgeable about the unique issues related to the culture of healthcare organizations and networks
- Knowledgeable about state and federal laws, licensing regulations, Joint Commission standards, and similar regulatory requirements related to information security and patient confidentiality
- Knowledgeable in the design and presentation of educational programs

Qualifications

The ideal candidate for this position possesses thorough knowledge of the patient care environment, all forms of information in use throughout a healthcare organization, and information systems and networks. Since a major component of Hartford

Hospital's security program is a culture change accomplished through hospitalwide training, adult teaching experience is a desirable skill. Additionally, the coordinator must have a strong understanding of Joint Commission information management standards and federal and state release of information regulations. At Hartford Hospital, the coordinator is not responsible for the technical aspects of security but does work closely with Information Services in the development of the appropriate system controls. Given these qualifications, a health information management professional possesses the ideal skill set for this position.

Information Security Coordination Team Philosophy

The Information Security Coordination Team at Hartford Hospital has established itself as a self-managed team. As such, the team is empowered to execute policies approved by the executive board of Hartford Hospital through procedures and support structures. This self-managed team philosophy allows creativity in implementing and managing the security process. It lays the foundation for employee empowerment and ownership of security responsibilities rather than placing the Information Security Coordination Team or information security coordinator in a policing role. For example, an educational campaign for the 6000 employees at Hartford Hospital is intended to create hospitalwide awareness of the security policies, standards, and guidelines (see Exhibit 2). More importantly, during the education process, employees sign a mandatory confidentiality agreement, thereby taking ownership of their individual responsibilities relating to information security.

Exhibit 2

Hartford Hospital Information Security Education Plan

Three levels of training are presented based on access level and use of information.

Basic: Presented to employees with limited access to patient information (no computer sign-on, i.e., environmental service workers, nurse aides, diet aides, security guards)

Education Content:

- Security video
- Review confidentiality agreement
- Define and role play examples of privacy, security, and confidentiality

Intermediate: Presented to employees with high access (computer sign-on to network) and limited supervision, i.e., nurses, physicians, unit secretaries, medical record staff

Education Content:

- Basic program
- Faxing protocols
- E-mail etiquette
- Voice mail etiquette
- Liability issues for self and organization
- Audit processes
- Disposal of paper
- Password security
- Electronic signature
- Virus detection

Management: Presented to collaborative management teams, department heads, and above

Education Content:

- Basic and intermediate education programs
- Management role accountabilities

- Granting access levels
- Identifying high-risk situations
- Performing a risk assessment
- Staff accountability
- Role modeling
- Unit/department-based data management, manipulation, and distribution issues
- Implementing new technologies

Similar teams are in place at Veteran's Memorial Medical Center and Connecticut Children's Medical Center, partner organizations in the Connecticut Health Systems. Hartford Hospital's Information Security Coordination Team meets monthly with the Information Security Coordination Teams of those two facilities to assure consistency and to eliminate duplication of effort. As a group, we have built a great deal of consensus on philosophy, concepts, and approaches. We believe the blend of professional disciplines, together with our unique perspectives, strengthens our results.

Acknowledgment

The authors acknowledge Dale W. Miller, Irongate Inc., San Rafael, CA, for his consultation in developing the original security policies, standards, and guidelines and implementation for Connecticut Health System, Inc.

Cindy Zakoworotny *is director of the Medical Record Department, Hartford Hospital, Hartford, CT, and Veteran's Memorial Medical Center in Meriden, CT. She is a member of AHIMA's Information Security Task Force.* ***Cheryl Rutz*** *is director of data administration for the Information Services Department at Hartford Hospital.* ***Cheryl Zwingman-Bagley*** *is transition leader, Hartford Hospital.*

Article citation:
Zakoworotny, Cindy, et al. "A Team Approach to Managing an Information Security Program." *Journal of AHIMA* 68, no.5 (1997): 26-30.
