IDENTIFYING COMPETENCIES FOR HOSPITAL PERSONNEL INVOLVED WITH SECURITY, PRIVACY, AND INFORMATION SYSTEMS

Donna M. Schaeffer
Marymount University, 2807 N. Glebe Road, Arlington, VA 22207
Donna.schaeffer@marymount.edu
703-284-5718

Cynthia Knott
Marymount University, 2807 N. Glebe Road, Arlington, VA 22207
Cynthia.knott@marymount.edu

ABSTRACT

Implementation of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) has created a need for hospitals to adopt an organizational structure that pays attention to privacy, security, and the role of information systems. Partial adherence to HIPAA includes sustaining and maintaining privacy rights of individuals, the institution, and documents. There are three key positions whose job responsibilities could include maintaining privacy and security: Chief Information Officer (CIO), Chief Privacy Officer (CPO), and Chief Information Security Officer (CISO). The nature of these positions require different competencies.

The purpose of this proposed research is to learn the competencies required for success in the positions of CIO, CPO, and CISO in a hospital setting. This learning will include understanding the professional and educational backgrounds of persons assigned to the CIO, CPO, and CISO positions, and identifying the position responsibilities in organizations employing such persons.

The expected outcome is to identify the competencies that are needed to be a successful CIO, CPO, and CISO in a hospital setting and to provide performance appraisal measures for administrators who oversee these new positions.

Keywords: HIPAA, security, privacy, chief information officer, performance appraisal.

The Health Insurance Portability and Accountability Act of 1996 (HIPAA). In 1996, the United States Congress passed The Health Insurance Portability and Accountability Act (HIPAA). Through its various titles, HIPAA protects health insurance coverage for workers and their families when they change or lose their jobs, calls for the establishment of national standards for electronic health care transactions and national identifiers for providers, health insurance plans, and employers, and provides for the security and privacy of health data.
As part of HIPAA, The Final Rule on Security Standards (aka "The Security Rule") took effect in 2003. This rule requires that covered entities (entities that must comply with HIPAA requirements) must adopt a written set of privacy procedures and designate a privacy officer to be responsible for developing and implementing all required policies and procedures.

Hospital Organizational Structures. Prior to the HIPAA regulations, many hospitals have had a role for Chief Information Officer (CIO) or Director of Information Technology. This role heads up the information technology (IT) group. In business, the CIO typically reports to the Chief Executive Officer (CEO); however in healthcare, most CIOs report to the Chief Financial Officer (CFO). A content analysis of hospitals for which organizational charts were available to the public reveal that almost two-thirds (6.25%) of the CIOs report to the CFO, 12.5% report to the Chief Operating Officer, and 25% report to the Chief Executive Officer of the hospital. Implementing HIPAA has elevated the visibility of, or caused the creation of, the related roles of Chief Privacy Officer (CPO) and Chief Information Security Officer (CISO). Some hospitals have designed new job positions, while others have added the duties affiliated with these positions to existing personnel. The CIO may be the overseer of security and privacy, with these roles reporting to him or her. In some cases, argument can be made for these roles to report to someone other than the CIO, which puts them in more of a watchdog role.

Sample Job Descriptions. The CIO is a job title commonly given to the person in the organization who is responsible for information and communications technology (ICT). Major responsibilities include identifying the information technology needed to achieve goals and working within a budget to implement the plan. Since the CIO is involved with analyzing and reworking existing business processes, with identifying and developing the capability to use new tools, with shaping the physical infrastructure and network access, and with identifying and exploiting the enterprise's knowledge resources, it is important that the CIO have a background in healthcare (Biohealthmatics.com) or learns about that industry as quickly as possible. One competency that is desirable is the ability to work with others, both as a manager and as part of the management team. According to Biohealthmatics.com, hospitals typically require a minimum of a Bachelors degree in Business Administration, Computer Science or a related field and some may require a Masters level in the one of the above fields or Public Health, Hospital Administration or related field.

Due to external regulations such as HIPAA, in a hospital, emphasis may be placed on structuring data analysis and entry and developing protocols and procedures for working with data. This is where the role of CPO comes in. The CPO oversees the development and implementation of organization-wide privacy principles, policies, and practices (Association of American Medical Colleges). In the healthcare setting, priority placed on advocating and protecting patient privacy.

Protecting privacy requires secure systems. This brings in the role of CISO, whose major function is protecting and monitoring any and all information from being removed, accessed or manipulated from those outside of the organization (Biohealthmatics.com) or by those inside the organization, who do not have the legal right to access this information. In hospitals, this includes all patient files, medical notes, research based information, billing information, employee files and any and all other potentially sensitive information. There are technical aspects to the position, such as deciding upon and implementing encryption protocols. According to Biohealthmatics.com, most hospitals require personnel in these positions to have at least a four year Bachelors degree in computing science or business management or other related field. Some hospitals may also require certifications such as the Certified Information Systems Security Personnel (CISSP), Certified Cisco Network Associate (CCNA) or Computer and Network Security Awareness (CNSA).

Appendix One includes sample job descriptions that are compiled from a variety of sources, including the Association of American Medical Colleges and position announcements.

Competencies and Performance Appraisal. Implementing and overseeing the federal regulations are the job of the three professional level staff described above, i.e., the CIO, CPO, and CISO. Each of these jobs require in-depth and technical knowledge of patient interaction as well as understanding of how information is being stored and there is much overlap between the three job functions of CIO, CPO, and CISO. (McGarry, Schaeffer, and Knott, 2006). Responsibilities in the position, especially the CIO position, may require managerial competencies as well. This blend of technical, managerial, and health care-specific knowledge creates specific competencies that should be addressed in performance appraisal.

Competency is generally defined as a measurable pattern of knowledge, skills, abilities, behaviors, and other characteristics that an individual needs to perform work roles or occupational functions successfully. The competencies may be identified along technical and managerial lines and those that are health-care specific:

Technical:

- Proficiency with specific hardware
- Proficiency with specific software
- Proficiency with specific operating systems
- Ability to manage data
- Ability to document systems

Managerial:

- Demonstrate effective interpersonal relationships in the workplace
- Ability to solve problems
- Ability to deal with internal customers
- Ability to make decisions
- Good oral and written communication
- Ability to plan and evaluate
- Ability to provide leadership
- Skilled in negotiations
- Demonstrate sensitivity to the needs of others

Health-care Specific:

- Knowledge about organizational culture
- Knowledge about federal regulations
- Ability to deal with change and ambiguity
- Identify laws/regulations that relate/effect security and privacy in health care
- Explain the legal and ethical ramifications of recording/ reporting client/patient information

Performance Appraisal. Because of the nature of these positions, and the competencies required to perform the jobs well, it may be desirable to implement 360 degree feedback. In this type of performance appraisal, the holder of the position receives feedback from people whose views are considered helpful and relevant. The feedback is typically provided on a form showing job skills/abilities/attitudinal/behavioral criteria with a standardized scoring. People who provide

feedback can include peers, managers, top-level executives, subordinates, or customers. Basically, feedback is sought from anyone who has contact with the employee. The employee also assesses himself or herself using the same feedback instrument or form.

360 degree feedback is appropriate for these positions for three major reasons. First, the performance of these positions impact many people throughout the hospital, including the medical staff (MDs, RNs, and other professionals), the patients, and other employees. Receiving feedback from these people will provide a well-rounded look at how the person carrying out the position works with others and if the mission of the position fits within the hospital setting. This provides input for the job functions that are deigned so important, such as teamwork and communication skills.

Second, receiving feedback from a diverse group will reinforce the idea that these positions exist to serve the employees and patients of the hospital. If the security policy, for example, is so rigid that the persons providing patient care are unable to access or share the data and knowledge they need to perform their jobs, it is quite possible that employees will find ways to circumvent policies and procedures and create informal means. It is important to identify, through 360 degree feedback, how well the person and the policies he or she has designed and implemented work for the system.

Third, the pool of people providing feedback is broadened so that the recipient of the feedback is ensured that persons with varying amounts and types of expertise will be providing input. This is an especially important consideration where reporting lines are unclear or non-traditional. For example, in many hospitals, the Chief Information Officer reports to the Chief Financial Officer (CFO). In a traditional performance appraisal, the CFO might be the only person evaluating the CIO. The CFO may not have a background in technology. In 360 degree feedback, staff from the IT department may provide input on the CIO's technical expertise. The CPO may report to the Director of Patient Care, since much of the responsibilities deal with patients'privacy. The Director of Patient Care may not have the technical expertise to evaluate how well the CPO handles access to the database, for example, but in the case of 360 degree feedback, the CIO may provide input on the technical performance even if he or she is not the direct supervisor of the CPO.

REFERENCES

American Association of Medical Colleges. *Supplement to the Guidelines for Academic Medical Centers on Security and Privacy.* Available via http://www.aamc.org/members/gir/gasp/jobdescriptions.pdf.

"Chief Information Officer." Available via: http://searchcio.techtarget.com/sDefinition/0,,sid19_gci213620,00.html

"Chief Information Officer." Available via: http://www.biohealthmatics.com/careers/PID00310.aspx

"Chief Information Security Officer." Available via: http://www.biohealthmatics.com/careers/PID00313.aspx

"Chief Security Officer." Available via:
http://searchsecurity.techtarget.com/sDefinition/0,290660,sid14_gci858563,00.html

McGarry, Nina, Cynthia Knott, and Donna M. Schaeffer. "Issues Concerning Operationalizing Efficiency and Effectiveness When Operations are Dispersed Among Three Executives." *Proceedings of the Hawaii International Conference on Business,* May, 2006.

APPENDIX. Sample Job Descriptions

Position	**Chief Security Officer**: This position is a senior level manager responsible for championing institutional security awareness, security policy and procedure development, and working to ensure compliance with internal and external standards related to information security. The CSO would report to the ORGANIZATION Deputy Corporate Compliance Officer. The Information Security Officer designs, develops and implements security changes and enhancements to the Information Technology (IT) computing environments. The Information Security Officer is responsible for determining appropriate security measures and creating policies and procedures that monitor and control access to system resources and data. The Information Security Officer will update security standards as necessary and is responsible for the prevention, detection, containment and correction of security breaches.
Organizational Relationships	The position reports to [administrator, CIO, vice president, etc.]
Position Overview	• Implements and supports information security initiatives throughout the organization. • Acts as a focus and resource for information security matters. • Works with those in corresponding roles at other organizational entities. • Takes direction from the oversight committee and organization administration. • Investigates and recommends secure solutions that implement information security policy and standards. • Coordinates Office of Information Security activities and manages staff. • Oversees, implements and monitors any special security requirements levied by government agencies in the performance of funded research, clinical trials and other activities. • Provide project management and operational responsibility for the administration, coordination, and implementation of information security policies and procedures across the Health System including the hospitals and health centers, Medical School. • Perform periodic information security risk assessments including disaster recovery and contingency planning, and coordinate internal audits to ensure that appropriate access to ORGANIZATION information assets is maintained. • Serve as a central repository for information security-related issues and performance indicators. Develop, implement, and administer a coordinated process for response to such issues. • Function when necessary as an approval authority for platform and/or application security and coordinate efforts to educate the ORGANIZATION community in good information security practices. • Maintain a broad understanding of federal and state laws relating to information security and privacy, security policies, industry best practices, exposures, and their application to the ORGANIZATION information technology environment. • Make recommendations for short and long-range security planning in response to future systems, new technology, and new organizational challenges. • Act as an advocate for security and privacy on internal and external committees as necessary. • Develop, maintain and administer the security budget required to fulfill ORGANIZATION information security

	expectations • Oversees the establishment, implementation and adherence to policies and procedures that guide and support the provision of information security services • Conducts risk assessments and risk analysis to help the organization develop security standards and procedures that support strategic, tactical and operational objectives on a cost-effective basis • Makes recommendations on appropriate personnel, physical and technical security controls • Manages the Information Security Incident Reporting program to ensure the prevention, detection, containment and correction of security breaches • Participates in resolving problems with security violations • Responsible for the content (and in some cases the delivery) of information security seminars and training classes • Coordinates the communication of information security awareness to all members of the organization • Certifies that IT systems meet predetermined security requirements • Strives to maintain high system availability • Works with vendors, IT associates, and user departments to enhance information security
Education/Experience/Job Specifications	• A four-year college degree is required. • A Certified Information Systems Security Professional rating is desired. • At least ten years of information security work experience is required with both public and private sector experience preferred. • The ability to work effectively in a collegiate, consensus driven organization is required, as are demonstrated personnel and information security program management skills. • A working knowledge of all aspects of information security is essential, as is the ability to apply this knowledge in an open network environment. • In-depth understanding of network and system security technology and practices across all major-computing areas (mainframe, client/server, PC/LAN, telephony) with a special emphasis on Internet related technology • Good verbal and written communication skills • A high level of integrity and trust • Knowledge and understanding of technology-related and health-related state and federal regulations
Preferred Qualifications	• Specific experiences in the health care industry. • Extensive familiarity with health care relevant legislation and standards for the protection of health information and patient privacy. • Demonstrated successful project management expertise. • Professional certification, e.g. CISSP, CISA.
Position	**Privacy Officer**: The Privacy Officer oversees the development and implementation of corporate-wide privacy principles, policies and practices. The Privacy Officer is responsible for coordinating all corporate activities with privacy implications, as well as monitoring all of the organization's services and systems to assure meaningful privacy practices. The Privacy Officer also advocates and protects patient privacy by serving as a key privacy advisor for patients, handling disputes and managing patient

	requests regarding their medical record.
Requirements	• Coordinates corporate privacy activities which include overseeing the establishment, implementation and adherence to corporate policies on patient privacy, confidentiality and release of patient information • Reviews new or revised government healthcare laws and regulations pertaining to privacy determine if new policies or modifications of current policies are needed • Conducts privacy risk assessments and internal privacy audits. • Manages patient privacy-disputes and requests for changes to their medical record • Increases the public's awareness of the organization's efforts to preserve patient privacy • Oversees the development and delivery of privacy training and awareness. • Works closely with Health Information Management, Information Technology and Marketing departments • Ensures that record custodians correctly protect and archive patient information • Ensures that the organization's privacy protections keep pace with technological advances • Participates in outside healthcare organizations for keeping updated on privacy developments and "best practices" for patient privacy • Reports to the organization's executive officers on emerging legislation/regulations and how the company is currently dealing with privacy issues
General Skills	• Good verbal and written communication skills • A high level of integrity and trust • Knowledge and understanding of technology-related law and public policy experience, clinical • Research and related issues
Professional Certifications or Experience	Registered Health Information Administrator (RHIA)