CONSIDERING THE CREATION OF AN INFORMATION SECURITY OFFICER POSITION AT A REGIONAL MEDICAL CENTER: A CASE STUDY

by

Aaron C. Redalen

A Master’s paper submitted to the faculty of the School of Information and Library Science of the University of North Carolina at Chapel Hill in partial fulfillment of the requirements for the degree of Master of Science in Library Science.

Chapel Hill, North Carolina

April, 1999

Approved by:

____________________
Advisor

This case study examines the process used at a regional medical center to assess the need for an information security officer, and to determine the duties and responsibilities of the position, if it were created. Thirteen administrators from ten different departments or divisions were interviewed to assess the need and support for the creation of an information security officer position, and to inventory the responsibilities that administrators would expect such an officer to fulfill.

After the interviews, responses were reorganized, transcribed and tabulated. The recommendations offered and requirements expressed by interview respondents were then compared with recommendations found in the literature on information security officers. Recommendations were made for the creation of an information security officer position, the duties and responsibilities of such a position, and further directions for action and study.

Headings:

Right of privacy

Information policy

Records management

Information systems – Special subjects – Medicine
Introduction

The confidentiality and security of patient information are among the oldest and most central values in the practice of medicine and provision of healthcare. Trust and confidence are essential to the open communication and honest disclosure necessary for good physician-patient relationships. The medical profession has recognized and expressed these values in the Hippocratic Oath from antiquity, and in modern times they are enacted through state and federal legislation and regulations, industry standards promulgated by such agencies as the Joint Commission on Accreditation of Healthcare Organizations (JCAHO) (1998), and professional ethics promoted by organizations such as the American Medical Association (1997), which holds that “information disclosed to a physician during the course of the relationship between physician and patient is confidential to the greatest possible degree” (p. 94). More fundamentally, some contend that patient privacy and confidentiality proceeds not only from professional ethics, but are members of the constellation of basic human rights promoted by the United Nations and other humanitarian organizations (Chapman, 1997). Although patient information confidentiality and security have long been recognized as vitally important in healthcare regulation and policy, ensuring these conditions has become an increasingly complex challenge as new information technologies and trends in healthcare administration and finance reshape the collection and use of patient information and place new burdens on its owners and guardians.

The emergence of electronic medical records has had a tremendous impact on the management of patient information and has raised serious concerns about confidentiality and security. Confidentiality is here defined as “a form of informational privacy characterized by a special relationship, such as the physician-patient relationship,” and security as “technical and administrative procedures designed to protect data systems against unwarranted disclosure, modification, or destruction, and to safeguard the system itself” (Gostin, et. al., 1993, p. 2487). Electronic patient records offer numerous opportunities for improvement of clinical diagnosis and
therapy, and can become rich, vast sources of data in biomedical and health services research. Electronic medical records are also believed to hold potential for greater efficiency and reduced waste in healthcare administration and finance. Furthermore, Barrows and Clayton (1996) argue that “With appropriate safeguards…computer-based medical records may actually offer more security than traditional paper-record systems” (p. 139). However, the protection of the confidentiality and security of electronic patient records is the subject of serious discussion and debate among consumer advocacy groups, researchers, regulatory agencies and legislators, as well as physicians and healthcare administrators. As Cassidy and Sepulveda (1995) write, “current legal protections are neither uniform nor responsive to the issues associated with an electronic health data environment” (p. 606).

The transition from paper-based to electronic patient records is rarely smooth and never simple. Healthcare facilities attempting this transition must (at least temporarily) use various combinations of paper-based and electronic patient records, and often continue to maintain and use paper-based records for some services and tasks even after electronic record systems have been implemented. The existence of both paper and electronic records engenders duplication and overlap of patient medical data across record systems, thereby increasing the potential for inconsistencies between systems and multiplying the vulnerabilities of patient information systems. The use of multiple record systems also places additional burdens on the medical records and information systems personnel who must audit and control access to patient information to safeguard its confidentiality and security. Policies must either be applicable to all patient record systems, or multiple policies must be developed to govern the different forms of patient information. Policy development, education, evaluation and enforcement therefore become more difficult to plan and coordinate, and such efforts may be unnecessarily duplicated. Furthermore, the more numerous and complex the policies governing the collection and use of patient information, the greater the risk of confusion and frustration among staff, increasing resistance to
the adoption of new information technologies and their attendant confidentiality and security policies.

The increasingly competitive business environment of healthcare provision has precipitated sweeping reorganizations of healthcare facilities. Regional medical centers, community hospitals, clinics, and a wide variety of specialties and private practices are entering into alliances and banding together under common administration to form integrated delivery systems (IDS). However, the component organizations and facilities of such systems come into the IDS with unique patient information systems and environments, all with their own policies and procedures. The task of harmonizing these policies and procedures to ensure common standards of service and a consistent level of confidentiality and security across an IDS can be difficult, if not daunting. The Council on Competitiveness (1996) contends that “The extent to which [IDS] can achieve [the integration of health information systems] will pace their ability to deliver higher-quality, more cost-effective, patient-centered care and, hence, their long-term competitiveness” (p. 40). The coordination of multiple overlapping patient information policy efforts across a variety of healthcare environments also places increased administrative burdens on medical records, risk management and legal departments, as well as other administrative personnel within the member facilities.

Integrated delivery systems must maintain common standards of care across their component facilities, which requires reliable and efficient access to accurate, complete and appropriate patient information. Tang and Hammond (1997) assert that “To manage the delivery of care in an [integrated delivery system], a health system must have efficient and accurate ways of capturing, managing and analyzing clinical data collected at all the different sites where care is provided” (p. 3). To this end, IDS’s have been developing and implementing integrated networked information systems to provide broader and more efficient access to patient information, from medical history and clinical data to demographic and financial information. However, the
distribution of access to patient information across physical and organizational boundaries greatly multiplies potential vulnerabilities and requires concerted efforts to ensure the accurate, reliable and secure flow of confidential patient information.

One promising approach to the task of integrating diverse information systems and environments has been the use of open or modular information systems architectures in which component systems appropriate to specific information needs and settings can be removed, upgraded or added as necessary without upgrading or replacing the entire system. However, although such systems are designed to facilitate efficient distributed access to patient information, they are dependent on relatively new network technologies that have not been in use long enough to fully research the confidentiality and security of the patient information that they store and transmit. Furthermore, the companies that develop the hardware and software of such modular systems are primarily concerned with rapidly exploiting the newest techniques and technologies to offer powerful and competitive functionality; confidentiality and security concerns are rarely the highest priority. Broccolo, Fulton and Waller (1993) recommend that in acquisition of information systems “The request for proposal [from information system vendors] should address the desired security features and functions in as much detail as other desired features and functions, and be made part of the relevant vendor agreement” (p. 46). Healthcare facilities must diligently review, monitor and audit their information systems on a continuous basis to ensure the confidentiality and security of patient information.

Within the healthcare industry there are many competing, sometimes conflicting demands for patient information, and the distribution of access to this information has significantly increased cause for concern. Healthcare workers have access to a great deal of patient information and may be tempted, often by curiosity or concern, to inappropriately access the records of family, acquaintances, neighbors or prominent individuals. Many physicians view their own or their families’ medical records, frequently without the presence of the attending physician and without
the official consent that may be required by law. Insurance companies, employers and managed care organizations may seek information about patients that could potentially be used to refuse or withdraw coverage, or to deny employment. Lawrence (1994) offers an example of such damage: “Disclosure of medical information can…damage one’s career or profession, as when Senator Thomas Eagleton ended his campaign for U.S. vice president in 1972, after it became known that he had been treated for mental illness” (p. 640). Competing demands for patient information have become a particularly thorny problem as managed care organizations and insurance providers become part of IDS’s as well. Patient information confidentiality and security policies must be carefully crafted to address different demands for patient information and to assign appropriate levels of and procedures for access to sensitive medical data.

New standards, regulations and legislation regarding patient information are still emerging, and the administrative and regulatory landscape of patient information confidentiality and security is far from stable. Information technology and healthcare industry groups, as well as national and international standards organizations are developing a variety of health data encoding and communication standards, which the administrators of medical information systems must be prepared to comply with as they are completed and adopted by health data organizations and regulatory agencies. The Food and Drug Administration which oversees approval of medical devices as well as foods and drugs, is still considering its role in the testing and approval of healthcare information technology and medical records systems and software. The Health Insurance Portability and Accountability Act (HIPAA) of 1996 contains administrative simplification provisions requiring Congress to pass legislation governing the use of electronic patient information, including measures to protect confidentiality and security and sanctions for failure to do so. Congress is currently slated to pass the required legislation by August 21 of 1999, and HIPAA requires that the Secretary of Health and Human Services pass appropriate regulations to meet these requirements should Congress miss its deadline. Healthcare facilities must closely
monitor these regulatory and legislative developments to anticipate and prepare for any changes required for compliance with new Federal legislation or regulations. Facilities that fail to adequately prepare for these changes may be obligated to hastily alter their policies and practices to avoid fines for failure to comply, potentially at great cost in time and effort.

These developments have required a high degree of coordination within institutions to develop policies to protect the confidentiality and security of patient information. Many healthcare facilities have responded to this challenge by instituting a position that has become known as an information security officer, whose responsibility it is to plan, organize and undertake the necessary actions to ensure the confidentiality and security of patient information. The specific tasks and duties of information security officers can vary widely from one institution to another, and each individual officer typically focuses on either the technical aspects or on the administrative aspects of patient information confidentiality and security, though they must necessarily be involved in both. The information security officer works in coordination with administrators and managers from all departments to ensure patient information confidentiality and security. The Computer-Based Patient Record Institute (1996) defines the information security officer as “the central focal point for the overall coordination of security policies and procedures for the organization.” (p. 3).

Case Study

This case study investigates the process used at a regional medical center to assess the need for an information security officer, and to determine the duties and responsibilities of the position, if it were created. This medical center (which shall be from this point referred to as the Healthcare Institution), like many of its peers has grown from its beginnings as a hospital to incorporate a wide variety of clinics, specialties, and private practices, and has become an integrated delivery system. The Healthcare Institution currently uses both paper-based and
electronic patient records, the combinations and configurations of which vary from one clinical or administrative setting to another. The Institution is also expanding the capabilities of its existing information systems and incorporating new technologies to meet its growing patient information needs. Patient information confidentiality and security have long been recognized as very important issues within the Healthcare Institution. Currently, confidentiality and security are addressed through the concerted efforts of the Medical Records, Risk Management and Information Systems departments, and Medical Records and Confidentiality and Security Committees comprised of representatives from most departments within the Institution. However, the possibility is being considered that the coordination of efforts required for the protection of patient information confidentiality and security might be more appropriately and effectively provided by a dedicated information security officer who could focus solely on these functions, rather than performing them in addition to other duties.

Methods

The Healthcare Institution operates in an extremely competitive environment, and diligently guards proprietary information about its practices, its organization and its strategic plans. This concern was amplified by the prospect of an independent researcher examining the Healthcare Institution’s confidentiality and security policies and procedures. Consequently, the identity of the Healthcare Institution or those of its personnel are not disclosed. Also, since it would be problematic to risk a security breach through publication of specific vulnerabilities and risks to patient information, portions of this report discuss risks and vulnerabilities confronting healthcare facilities in general, and not necessarily the Healthcare Institution specifically.

This research project was conducted through close collaboration with the Director and several administrative personnel of the Medical Records department and with a member of the Medical Records and Confidentiality and Security Committees, all of whom shared their
experience in working with confidentiality and security issues at the Healthcare Institution. The Medical Records department provided minutes of previous meetings of the Medical Records and Confidentiality and Security Committees, in which patient information policies and procedures had been discussed, developed and approved, and in which the possible need for an information security officer was first voiced. Analysis of these minutes provided valuable insight into the Healthcare Institution’s work on patient information confidentiality and security, and highlighted additional areas of concern for confidentiality and security within the Healthcare Institution. A discussion of the work of these committees appears in the results portion of this publication.

Interviews were conducted with thirteen administrators from ten of the Healthcare Institution’s departments to discuss the need for an information security officer and to identify the duties and responsibilities of the position. The participants represent a variety of departments and divisions within the Healthcare Institution, including Medical Records, Radiology, Nursing, Information Systems, Psychiatry, Surgery, and Patient Services, as well as a physician’s advisory group on clinical information technology, the administrative body overseeing the Institution’s specialty clinics, a clinical research administration organization, and a community and family medicine clinic. These personnel serve in different departments and in different capacities within the Healthcare Institution, but all share a common involvement with and responsibility for patient information confidentiality and security. The interview method was chosen for its flexibility, openness and potential for greater and more selective detail than other methods such as surveys or questionnaires. Furthermore, the qualitative nature of interview responses was expected to be of greater value than quantitative information for a situational case study.

Interview candidates were selected through consultation with the Director of the Medical Records Department and a member of the Medical Records and Confidentiality and Security Committees. The candidates were chosen for their past and current participation in the development of confidentiality and security policies and procedures, as well as for their official
responsibilities for the protection of patient information confidentiality and security. Interview participants were then selected on the basis of availability and willingness to participate in the research project. All participants were provided informed consent for participation in the interview and in the research project. Almost all of the participants are either members of the Medical Records or Confidentiality and Security Committees, or have employees within their departments who serve as representatives to one or both of these committees. The participants were provided with the interview questions in advance of their interviews, to allow them time to think about the issues being studied and to consider their responses.

The interview questions (Appendix A) were developed through review of the available literature on information security officers in healthcare environments, and through subsequent consultation with the Director and administrative staff of the Medical Records department and a member of the Medical Records Committee. Questions were then further refined in response to the recommendations of these personnel. The interview procedure was designed to evaluate the need for an information security officer by inquiring whether the services and functions that could be provided by an information security officer are currently being performed, and if so, how these functions are being performed, and by whom. The interview was also meant to provide participants an opportunity to share opinions on the need for an information security officer, and to discuss any other administrative support needs or requirements that they or their departments would expect an information security officer to satisfy. Since the interview was intended to be an open and dynamic conversation about patient information confidentiality and security, the questions were crafted as points for discussion and as conceptual cues rather than simple queries eliciting explicit answers. The questions were organized in a series of functional groups corresponding to possible responsibilities and duties of an information security officer. These functional groups were identified through review of available literature on information security officers and programs, and are described in greater detail below.
The first group of questions, “Background,” was intended to initiate the conversation by asking interview participants to describe their duties and the roles of their departments within the Healthcare Institution. The first question was also intended to start the participants thinking about the possible impacts that changes in the way confidentiality and security issues are addressed could have on their work and the work of their departments. The next two questions opened the topics of management of patient information and awareness of confidentiality and security issues for further discussion, and inquired about the ways that interview participants have heretofore learned about confidentiality and security issues in patient information.

Perhaps the most central responsibility of an information security officer is to actively work to identify potential risks to the confidentiality and security of patient information. As confidentiality and security risks are identified, the information security officer must take the necessary steps to address and guard against these risks. The first question of the second group, “Risk and Policy Needs Analysis,” was intended to determine the extent to which interview participants are involved in searching for possible risks to patient information confidentiality and security, and to establish whether any formal procedures or techniques are used to identify such risks. The second question of this group asked whether any person within the participant’s department has been officially assigned responsibility for identifying and addressing confidentiality and security risks, or whether this function is included in anyone’s job description or official duties. The third question inquired about the means by which identified risks to information confidentiality and security inform the development and adoption of patient information policies and procedures. This question also asked whether any formal procedures are used to initiate the development of patient information policies and procedures in response to identified risks.

The first question of the third group of interview questions, “Policy Development,” was intended to determine whether anyone in the department bears official responsibility for initiating the development of policies and procedures to protect the confidentiality and security of patient
information. The second question of this group assessed participants’ awareness of how confidentiality and security policies are developed, and attempted to determine the level to which they and their departments are involved in such policy development. If confidentiality and security policies are to be accepted by the administrators and personnel that they affect, the information security officer must work closely with these administrators, and provide them with the opportunity to review and suggest revisions to confidentiality and security policies prior to approval. The last questions in this group asked whether participants and their departments are provided opportunities to review confidentiality and security policies prior to adoption.

The effectiveness of confidentiality and security policies is substantially reduced if front line personnel do not understand and adhere to these policies. Information security officers play an important role in determining needs of departments for education of staff on patient information confidentiality and security. The first question in the fourth group of interview questions, “Education,” asked participants how needs for policy education are determined, and the extent to which departments are involved in assessing these needs. Information security officers should take responsibility for planning and implementing programs and initiatives to educate employees about confidentiality and security policies and procedures. The second question in this group asked participants how confidentiality and security programs are developed, and the extent to which they and their departments are involved in the development of such programs. The third question asked whether anyone in the participants’ departments has been assigned responsibility for conducting confidentiality and security education, or ensuring that such education is provided. The fourth question in this group asked whether the effectiveness of confidentiality and security education and training is evaluated, whether the responsibility for evaluation has been assigned to anyone within the department, and whether any formal methods or schedules are used in conducting such evaluations.
Once confidentiality and security policies have been established and employees have received appropriate education and training, the policies must themselves be monitored and evaluated. The first question in the fifth group, “Policy Evaluation,” asked whether anyone in the participants’ departments has been assigned responsibility for monitoring the effectiveness of confidentiality and security policies, and for ensuring departmental compliance with established policies and procedures. The second question asked whether participants’ departments use any formal procedures for monitoring the effectiveness of confidentiality and security policies and the departments’ compliance with these policies. The final question of this group asked participants whether confidentiality and security policies are actively enforced, how such enforcement is conducted, and whether anyone in their departments has been assigned formal responsibility for policy enforcement.

Finally, if healthcare facilities are to be adequately prepared for future requirements for protection of confidentiality and security, legislative and regulatory developments affecting the management of patient information must be closely monitored. The first question of the last group, “Future Developments,” asked participants whether anyone in their departments monitors regulatory and legislative actions affecting management of patient information, and whether this is a formally assigned responsibility. In protecting patient information, healthcare facilities should also study the methods and strategies used by other facilities in protecting confidentiality and security, including organizational changes (such as the hiring of information security personnel), revisions of job descriptions, and development and revision of information policies. The second question of this group of interview questions asked participants whether anyone in their departments attempts to study the activities of other facilities in protecting the confidentiality and security of patient information, or to compare relevant policies and practices of the Healthcare Institution with those of similar institutions.
Each of the interviews lasted approximately thirty to forty-five minutes and was allowed to change course to suit the flow of the conversation. The interview questions described above were used as topics for discussion and as cues for guiding this flow. The interviews were also intended to be open-ended and to allow participants to add or volunteer additional information about the protection of patient information confidentiality and security. Therefore, the last group of interview questions also included questions meant to provide interviewees an opportunity to provide such additional information, and to offer any other thoughts on the creation of an information security officer. Eleven of the interviews were conducted in the participants’ offices, and two were conducted by telephone. To provide participants a greater degree of confidentiality, none of the interviews were taped; rather, written notes were taken by the interviewer. After each interview, the notes were reviewed and reorganized to consolidate topics that had arisen at different times during the interview.

Once the interviews were completed, all interview notes were transcribed and reviewed, and participants’ responses reorganized by question group and individual question. Once all of the responses had been functionally organized, participants’ responses to questions or thoughts on confidentiality and security issues were examined and compared. The responses then were organized by most commonly expressed opinion, thought or concern. Once these reorganizations were completed, responses were tabulated for more efficient review. Finally, participants’ interview responses were compared with recommendations from the available literature for the creation of information security officers or information security programs.
Results

Previous Efforts in Protecting Confidentiality and Security

Although the Healthcare Institution does not currently employ an information security officer, it has given diligent consideration to issues of patient information confidentiality and security, and has undertaken many efforts to protect patient information. Most of these measures have originated from the activities of the Medical Records Committee and its Confidentiality and Security subcommittee. The Medical Records Committee bears responsibility for advising the Medical Records Department, drafting policies governing Medical Records for approval by the Executive Committee of the Healthcare Institution, monitoring the quality of medical records and enforcing record completion, reviewing forms for inclusion in the medical record, and reviewing requests for research use of medical records. The Medical Records Committee is a standing committee, and includes representatives from most medical departments of the Healthcare Institution, as well as the Medical Records, Risk Management, and Information Systems Departments. The confidentiality and security portions of the work of the Medical Records Committee are addressed in its Confidentiality and Security Committee, for presentation to and discussion by the full Medical Records Committee.

The Confidentiality and Security Committee is responsible for identifying patient information confidentiality and security issues, making recommendations to heighten awareness of and improve patient information confidentiality and security, developing strategies to ensure continued awareness, and developing confidentiality and security policies for the Healthcare Institution. The Confidentiality and Security Committee also includes representatives from many medical departments, as well as from such administrative departments as Medical Records, Risk Management, Administration, Managed Care, Internal Audit, Information Systems, Human Resources, Education, and the Ethics Committee. The Healthcare Institution’s confidentiality and
security policies were developed by this committee, and it was in this committee that the need for an information security officer was first discussed.

Several confidentiality and security policies currently under consideration or in use at the Healthcare Institution were developed by the Confidentiality and Security Committee, including policies on proper disposal of confidential information, use of passwords and log-in procedures for electronic information systems, e-mail communication, telemedicine technologies, and internet/intranet usage, to name a few. The Confidentiality and Security Committee also developed a standard confidentiality agreement that is to be signed by all employees upon hire and renewed on an annual basis. This confidentiality agreement is intended to raise awareness among employees of the importance of patient information confidentiality and security, and to familiarize employees with the Healthcare Institution’s relevant policies. Requiring employees to sign the agreement also serves as an additional assurance that employees have been informed of confidentiality and security policies, hopefully preventing claims of ignorance in the event of a confidentiality or security breach. One policy currently in the final stages of development is a policy on breach of patient confidentiality; this policy is intended to define levels of confidentiality breaches and to ensure that disciplinary actions required by such breaches are consistently applied. The proposed policy was drafted by administrative personnel of the Medical Records Department, and has been developed through consultation with Risk Management, Human Resources and the Institution’s Legal Counsel.

The Confidentiality and Security Committee provides a forum for discussion of patient information confidentiality and security issues. Such issues have included the appropriateness of allowing individuals to access their own medical records, the need for additional security features in the Institution’s medical information systems, and the risks of making highly sensitive information available in patient information systems. The Confidentiality and Security Committee also considers requests for access to patient information systems from various departments,
divisions and personnel within the Institution, reviews proposals for use of new patient information systems, and considers requests for exceptions to confidentiality and security policies.

The Confidentiality and Security Committee has also discussed, developed and undertaken initiatives to raise awareness of confidentiality and security issues throughout the Institution. The Medical Records department has for two years conducted an Institution-wide program to heighten awareness of patient confidentiality. This program includes signs, a variety of promotional materials, flyers that explain confidentiality issues and present patient confidentiality and security scenarios, screensavers that remind employees about patient confidentiality, a Powerpoint presentation that administrators and managers can use with their employees, and recommendations to administrators for raising awareness of patient confidentiality and security issues.

Although the Medical Records and Confidentiality and Security Committees, and the Medical Records and Risk Management departments have done substantial work to protect patient information confidentiality and security, there has been a growing consensus within the Healthcare Institution, and particularly within these committees that the need has arisen for an information security officer. This need was first formally raised as a result of a project undertaken one year ago to determine the usefulness of a standard patient record access auditing procedure. Auditors reviewed accesses to the hospital information system record of a prominent patient whose admission had been highly publicized by local media. Managers and administrators throughout the Institution were sent lists of employees who had accessed this patient’s record, and were asked to determine whether each access had been appropriate and to take disciplinary action for those that weren’t. Recommendations following the audit included a reassessment of confidentiality and security policy educational efforts, and the development of an office to perform ongoing audit functions to be directed by an information security officer. Since that time, the Confidentiality and Security Committee has repeatedly discussed the need for an information security officer, which
has culminated in a formal recommendation to the Medical Records Committee that the Institution consider creating an information security office/officer.

Need for an Information Security Officer: Interview Results

As explained in the methods section above, the first question in the “Background” group (see Appendix A for the interview questions) was used to gather some basic information about the roles and duties of the interview participants and their departments within the Healthcare Institution. The next question asked participants to describe some of the ways that different types of patient information are used by their departments, as well as the range of patient information used, and served to open the subject of patient information for broader discussion. Once a baseline of background information had been established through discussion of the first two questions, the third question guided the conversation to discussion of the protection of confidentiality and security by asking participants how they are informed about patient information confidentiality and security issues. The participants responded with a variety of sources: three had attended conferences on confidentiality and security or had employees who had attended such events; two stated that they frequently discuss these issues through academic and professional involvement in medical informatics; one participant’s division has its own information technology staff, one of the responsibilities of which it is to ensure compliance with research regulations. Most, but not all participants identified the Medical Records and Confidentiality and Security Committees, and the Medical Records department as sources for information on confidentiality and security. This was expected, as most of the interviewees either serve as or employ representatives to one or both of these committees. However, not all departments are represented on these committees, and one participant stated that the participant’s department had very little communication with these committees. Although these committees and the Medical Records department were the most
commonly cited sources for information on confidentiality and security, no single department or group was uniformly identified as an authoritative source for this information.

The next group of interview questions addressed the identification of risks to patient information confidentiality and security, and the way that these risks inform the development of information policy. Only one participant’s department regularly audits its information systems for confidentiality and security risks. The most common response was that the participants’ departments only identify risks to confidentiality and security as they appear, on an ad hoc and informal basis, and a few responded that this was not done at all. Nearly all participants stated that no formal procedures or methods were used within their departments to identify risks to patient information confidentiality and security. The assignment of responsibility for identifying and responding to confidentiality and security risks varies from one department to the next. Some participants responded that although responsibility had not been formally assigned, ultimate responsibility for confidentiality and security risks rested with department heads. In other departments, the participants themselves bear responsibility (again, informally) through the course of their work with information systems or through their representation to the Medical Records or Confidentiality and Security Committees. One participant responded that this responsibility would default to the participant’s clinic’s quality improvement committee. In other departments, the participants did not think that this responsibility had been assigned in any meaningful way. In nearly all cases, responsibility for identifying risks to confidentiality and security was only informally assigned, if at all. Several interview participants indicated that the most common way risks to confidentiality and security inform policy development is through representation to and communication with the Confidentiality and Security Committee. Finally, some departments develop their own internal policies or standard operating procedures to address these issues, independently of the Medical Records Committee. All interviewees indicated that no formal
methods have been established for identified risks to confidentiality and security to inform information policy development.

Nearly all participants, with the exception of those whose departments develop internal policies and procedures, stated that patient information policies are passed down from the Medical Records Committee and its Confidentiality and Security Committee. Departmental involvement in the development and drafting of policy was agreed to be dependent on departmental representation to one or both of these committees. When asked whether departments were involved in the review and approval of forthcoming information policies, most participants responded that policies pending approval were sometimes discussed at departmental meetings or circulated within departments via e-mail. Some stated further that the personnel or departments that would be directly affected by new policies or policy revisions would probably be given the opportunity to make comments on policies under consideration. However, most participants conceded that review and discussion of forthcoming information policies with affected personnel or within departments happened on an ad hoc basis, and that no formal procedures were used in such discussion or review. Furthermore, several participants indicated that no formal procedures or mechanisms are used to distribute policies once they have been submitted for approval by the Medical Records Committee or approved by the Executive Committee, and asserted that this function requires improvement.

The greatest divergence of responses appeared in the portion of the interview addressing patient information confidentiality and security education and training. The education and training used in departments varies greatly depending on the departments’ functions, and needs for education and training are determined primarily within departments. However, it is worth noting that none of the participants responded that needs for confidentiality and security policy education were formally assessed in any way. Although some participants’ departments provide internal education and training on patient information confidentiality and security, most participants
indicated that such education was conducted mainly through the orientation provided to new employees upon hire. During part of this orientation, new employees watch a videotape that discusses various aspects of hospital safety, and which ends with a short presentation on patient information confidentiality and security. New employees also sign a confidentiality agreement which details what employees must do and must not do to protect the confidentiality and security of patient information, and in which employees indicate that they have been informed of and understand their responsibilities in this effort. Most participants indicated that continuing education on confidentiality and security is provided primarily through mandated renewals of this confidentiality agreement, though there was some disagreement between respondents about whether these renewals were annual or biannual, and several interviewees questioned whether the completion of agreement renewals was being monitored in any way. Several interviewees felt that the confidentiality and security awareness initiatives undertaken by the Medical Records department had significantly raised consciousness of confidentiality and security issues. Finally, although a variety of education and training efforts were described, only two participants indicated that their departments performed any evaluation of the effectiveness of such training.

The most evident gap in the protection of patient information confidentiality and security that arose in the interviews is absence of evaluation of information policy effectiveness and monitoring of departmental compliance with these policies. Only two participants were able to identify anyone responsible for evaluating policy effectiveness and for monitoring their departments’ compliance with information policies. The remaining participants conceded that no person had been formally designated as responsible for these tasks. Most participants also stated that no formal evaluation of policy effectiveness or monitoring of compliance is performed, and that if such evaluation and monitoring were to be performed, it would only be in the event of a request for internal audit or a breach of patient confidentiality or security. Participants were, however, able to describe the enforcement of information policy, though the variation between
interview responses indicates that policy enforcement procedures may not be well-established either. In all cases, policy enforcement was described as a collaborative effort between departments, Risk Management, Medical Records, and Information Systems. In the event of a breach of confidentiality, the employee’s supervisors or managers (depending on the chains of command involved), Information Systems and Risk Management would carry out an investigation at the direction of Counsel’s Office. Then, Human Resources works with the department to take necessary and appropriate disciplinary action. (It should be noted, however, that participants from Information Systems indicated that the department has been careful to avoid assuming a role of policing information system users).

When asked whether anyone in their departments monitored legislative and regulatory developments that could affect the management of patient information, participants returned a variety of responses. A few departments have employees who monitor legislative and regulatory developments, and two of the departments have internal units responsible for monitoring compliance with applicable legislation and regulations. In most departments however, if legislation and regulation were being monitored at all, it was in the course of an employee’s other duties, or as the result of research interests or professional communications. Finally, few departments have personnel who are involved in benchmarking patient information policies and procedures, and several participants stated that the financial and human resources were not available within their departments to conduct such efforts. Several interviewees, however, noted that the Medical Records department has performed substantial and valuable benchmarking of information policies and procedures for the Medical Records and Confidentiality and Security Committees.

All of the participants appeared to agree that the Healthcare Institution needs an information security officer, and all but two explicitly stated this in their interviews. Some participants complained that many of the patient information confidentiality and security efforts described in the interviews simply could not be addressed within their departments due to lack of
necessary resources and administrative support. Several participants suggested that this problem
could be ameliorated through the creation of an information security officer who could work
between departments. Although nearly all of the participants recognized the valuable work that the
Medical Records department has done by taking the initiative to ensure that necessary measures are
taken and policies drafted to adequately protect confidentiality and security, several questioned
whether such tasks were appropriately part of the department’s functions, and whether an
information security officer might more appropriately be assigned such responsibilities.

Another common concern among participants was that a lack of formalized procedures and
official responsibilities for the confidentiality and security tasks and efforts described in the
interviews presents the risk of inconsistency and discontinuity in protecting confidentiality and
security. Although informal practices and assumptions of responsibility have so far appeared
adequate, the transfer or turnover of key personnel could result in important confidentiality and
security practices being dropped or forgotten. The formal definition of confidentiality and security
procedures and responsibilities in the job description of an information security officer would do
much to ensure consistency and continuity of confidentiality and security protection. Some
participants also suggested that an information security officer could perform the valuable function
of building consensus between departments with different needs and priorities in protecting patient
information confidentiality and security.

One participant, stating that there is a serious need for an information security officer,
thought that the Healthcare Institution had experienced an explosion of information and
connectivity, but that the Institution has not yet caught up with this explosion and its implications
for patient information and the protection of its confidentiality and security. One participant felt
that the creation of an information security officer who could take a leadership role in protecting
confidentiality and security would serve as an enabling step in the development and adoption of
new information technologies. Finally, although in support of the creation of an information
security officer position, several interviewees expressed concern that an information security officer be a team player, and that the officer understand the technical and organizational limitations of the Healthcare Institution and not be a “loose cannon,” with insufficient oversight and accountability.

Conclusions

This project’s interviews with Healthcare Institution personnel highlighted a number of tasks currently being performed on an ad hoc or informal basis that could be better performed by a dedicated information security officer. The interviews also identified some services not currently being provided in a systematic or consistent fashion that could be more consistently performed by an information security officer. One of the primary duties of an information security officer is to serve as an information resource on confidentiality and security issues for their coworkers and administrative constituencies:

The information security manager promotes information security awareness throughout the organization to all levels of management and to all employees and professional staff members. The information security manager provides a central source of information on state-of-the-art security techniques and products and acts as the principal representative for information security on various teams, task forces and commissions. (CPRI, 1996, p. 7).

Interview participants identified Medical Records, Risk Management and the Medical Records and Confidentiality and Security Committees as primary sources for such information. However, not all of these sources are equally available to all personnel or departments (as in the case of departments not represented on these committees). Additionally, many departments lack the resources necessary to send personnel to external confidentiality and security conferences and workshops. The information security officer should serve as the Healthcare Institution’s official contact person and designated expert on confidentiality and security issues. Furthermore, the information security officer’s duties should include planning and implementing strategies to
publicize the most current and pertinent information available on patient information confidentiality and security.

The information security officer should also be responsible for working with Risk Management and the various departments of the Healthcare Institution to proactively identify potential risks to patient information confidentiality and security. Job descriptions for information security officers frequently includes such responsibilities as “reviewing changes to security systems; assisting in all new systems development, purchasing and strategic planning to ensure that appropriate controls are implemented in new systems; monitoring audit trail records to identify security violations” (Miaoulis, 1997, p. 92). Most departments cannot afford to dedicate resources to the development and use of formal procedures to search for such risks. Most respondents indicated that an information security officer however, should bear responsibility for developing and implementing such formal procedures to conduct regular audits of departmental practices and information systems for confidentiality and security risks. One respondent pointed out that substantial audit logs of access to patient records were constantly being recorded and stored in a database but were not currently being used to their fullest potential.

Another compelling reason for employing an information security officer is to designate a person to be formally responsible for the confidentiality and security of patient information. “The information security officer is accountable for successful implementation of the information security program” (CPRI, 1996, p. 5). Most respondents agreed that the information security officer should bear official responsibility for this task and have support from Healthcare Institution administration to eliminate any confusion, doubt or indecision. An information security officer would be able to systematically assess confidentiality and security risks, gather and analyze the resulting findings, and take necessary actions, including the application of this knowledge to the development and refinement of patient information systems, policies and procedures through close work with relevant departments and committees.
Another key function of an information security officer is to plan and coordinate the consultation and joint efforts from diverse departments necessary to develop and support new information policies and procedures. “The information security manager identifies the resources needed to maintain the effectiveness of the [security] program and works with senior management to assign responsibilities throughout the organization” (CPRI, 1996, p. 6). The Healthcare Institution’s information confidentiality and security policy development should be initiated and coordinated by the information security officer, whose close work with departments to identify risks to confidentiality and security would provide valuable insight about the unique needs and concerns of each department.

An information security officer is responsible for researching and drafting confidentiality and security policies, and serves as a bridge between the different departments affected, by consulting with the administrators and other personnel whose support will be needed to ensure to success of these policies. Miaoulis (1997) contends that “Regardless of to whom he or she reports, it’s essential that the information security officer receive the support and authority to implement information security controls” (p. 93). The information security officer should serve as a clearinghouse in confidentiality and security policy development by regularly discussing proposed policies and policy revisions with all departments that would be affected by them. Providing departments a regular and formal opportunity to review proposed policies and make comments could greatly increase support for these policies upon approval, leading to an increased sense of cooperation and joint responsibility for protecting confidentiality and security. Also, as two respondents agreed, the information security officer should institute methods to systematically distribute and explain new and revised policies to ensure awareness of changes among the departments and personnel of the Healthcare Institution.

One of the most important tasks of the information security officer should be to plan, develop, support and execute training and education programs on confidentiality and security
issues, policies and procedures. Miaoulis (1997) asserts that “an information security officer has to use every mechanism at her or his disposal to educate employees about their responsibility to keep patient information confidential” (p. 94). The information security officer should collaborate with departments to assess each department’s specific and unique needs and to develop appropriate educational programs. Additionally, the information security officer should coordinate the support required for these programs from such departments as Education, Human Resources, Medical Records, and Information Systems. The lack of agreement between interview responses on current policy education and training indicates a need to standardize and formalize this function. Finally, “Evaluation studies should be conducted to determine the value of each individual information security education program or offering, as well as the effectiveness of the overall information security program” (CPRI, 1995, p. 10). This is a task that should be part of the educational responsibilities of an information security officer. The information security officer should systematically assess the effectiveness of confidentiality and security education and training, and strive to continuously improve these programs based on formal evaluation of educational effectiveness.

Information security officers are responsible for monitoring and evaluating the effectiveness of confidentiality and security policies and procedures. “The information security manager monitors overall organization compliance with the information security program” (CPRI, 1996, p. 6). The Healthcare Institution’s information security officer must be responsible for monitoring the effectiveness of patient information policies in protecting confidentiality and security. This should include the development of formal audit or review procedures used to systematically monitor departmental compliance with relevant policies. Additionally, several respondents indicated that an information security officer should be responsible for developing a procedure for review of audit logs for suspicious or inappropriate accesses to patient records. This recommendation is also one of the recommended “Organizational approaches” for protecting
electronic health information recommended by the National Research Council (1997, p. 97-99).

Such systematic reviews would provide the information security officer with valuable information for the continuous improvement of information policies and procedures, as well as confidentiality and security education.

Confidentiality and security policies are of little use if these policies are not actively and consistently enforced through established disciplinary actions or sanctions. “Breaches of confidentiality and violations or suspected violations of policy should be reported to the information security manager. Procedures for reporting potential exposures should be established” (CPRI, 1996, p. 7). Another key function of the information security officer should be the coordination and support of patient information policy enforcement, including deterrents to breach of confidentiality and security, such as systematic and (internally) publicized audits for appropriateness of accesses to random patient records, as well as to those of prominent individuals. The information security officer should also facilitate the development and adoption of standard procedures to be followed in the investigation of a possible confidentiality or security breach and participate in such investigations. If a breach is discovered, the information security officer must systematically and thoroughly document all investigative findings as well as disciplinary actions taken by departments or by Human Resources. The information security officer should also ensure that employee transfers and terminations result in appropriate and immediate changes to or denials of access to patient information.

The Healthcare Institution’s information security officer should continuously monitor legislative and regulatory developments that could impact the management of patient information confidentiality and security. The Healthcare Institution must be able to adequately anticipate and prepare for the requirements of new legislation and regulations to avoid costly mistakes and minimize the need to drastically alter policies or procedures. Lastly, the information security officer should keep abreast of the most current practices and techniques in the protection of patient
information confidentiality and security. This should include benchmarking the Healthcare Institution’s confidentiality and security policies and practices with those of similar institutions, attending relevant seminars, workshops, conferences and conventions, creating support networks of other information security officers, and seeking opportunities for continuing improvement of professional knowledge, skills and abilities. Miaoulis (1997) writes, “One of my first efforts [as information security officer] was to try to build a network of individuals who shared my concerns about health care information security” (p. 93).

Finally, although the issue was not addressed in the interviews, the Director of Risk Management pointed out “the need to protect…the security officer’s works via peer review and quality assurance.” The information security officer should conscientiously strive for the continuous improvement of information confidentiality and security policies and procedures, and should undertake and submit regular self-evaluations of his or her work as information security officer. Furthermore, the information security officer should regularly report on this work and submit to review by his or her peers within the Healthcare Institution.

The Healthcare Institution would benefit immensely from the creation of the position of information security officer to oversee the protection of patient information confidentiality and security. Broad support already exists among prominent members the Institution’s administration for such a position, the need for which has now been discussed by the Medical Records and Confidentiality and Security Committees for over a year. The above recommendations represent functions that should be included in the duties and responsibilities of the Healthcare Institution’s information security officer, and do not constitute a complete or official job description. The Medical Records department has already initiated benchmarking of information confidentiality and security management practices among similar institutions, and additional benchmarking is planned for the development of a formal job description.
References


Appendix A

General Framework for Interviews

This is a general framework for interviews. These questions represent areas of inquiry and will be used to guide conversations rather than to rigidly structure them. “Policy” in these questions can be assumed to mean policy regarding or affecting patient information.

Background

- What is your role and the role of your department in the Healthcare Facility?
- How is medical information used by your department?
- How are you and your department informed about confidentiality and security issues with regard to patient information?

Risk and policy needs analysis

- Does the department participate in identifying risks to the confidentiality and security of patient information? If so, how are these risks identified? Is there any audit or review procedure used to identify such risks?
- Who bears responsibility for identifying such risks and taking appropriate action?
- How do these risks inform policy development? Is there an established or formal procedure for taking action on identified risks to patient information?

Policy development (departmental or hospital)

- Who is/would be responsible for the initiation of patient information policy development?
- How is policy drafted? Is the department involved in policy development? What other departments or personnel are consulted/involved in drafting policy?
- What departments and/or personnel must review new policies? Is the department involved in reviewing new policies?
- How are new policies approved? Is the department involved in policy approval?

Education

- How are needs for education on policies regarding confidentiality and security of patient information determined? Does the department determine these needs, are these needs determined outside the department, or is this a collaborative process?
- How are the department’s policy education plans or programs developed? Is the department involved in developing policy education?
- Who is responsible for conducting the department’s policy education?
- Is the effectiveness of confidentiality and security policy education evaluated? If so, who is responsible for such evaluation, and how is evaluation conducted? How often is the effectiveness of policy education techniques or programs reviewed?
Policy evaluation

- Who is responsible for monitoring policy effectiveness and department’s compliance with policy?
- How is policy effectiveness and the department’s compliance with policy evaluated?
- How are policies enforced? Who is responsible for enforcement?

Future developments, other issues

- Does anyone in the department monitor legislative and regulatory developments that could affect electronic patient information and policies concerning it?
- Is anyone in the department involved in benchmarking electronic patient information policies and procedures with other departments or health care facilities?
- At any time during the last year have you heard about confidentiality and security policies and/or initiatives? If so, do you have any thoughts as to their effectiveness and usefulness? Do you have any other ideas that you think might be effective in raising awareness of confidentiality and security issues?
- Do you or your department have any other administrative support or policy development needs with regard to confidentiality and security of patient information that we have not discussed?
- Is there anything else you would like to discuss regarding patient information confidentiality and security?
Appendix B

Consent Form

Introduction

- I am inviting you to participate in a study on the protection of the confidentiality and security of patient information at The Healthcare Facility.
- Aaron Redalen of the School of Information and Library Science at the University of North Carolina at Chapel Hill will be conducting this study.

Purpose

- The purpose of this project is to study the need for the creation of an information security officer position at The Healthcare Facility and to determine the duties and responsibilities of such a position, were it created.
- It is hoped that this study will assess the information security needs and requirements of The Healthcare Facility’s personnel and departments. The findings of this study will be presented in a white paper for the Confidentiality and Security Committee, and portions of this study will be used in a master’s paper at the School of Information and Library Science at UNC-Chapel Hill.

Procedures

- I will ask you to participate in one interview which should take no longer than 45-60 minutes.
- I may request a brief (10-20 minute) follow-up interview (for clarifications, elucidations, etc.)
- If you have any questions about participating in this study, you should call Aaron Redalen at (919) 572-0980 (home), (888) 838-5273 (pager), or e-mail redaa@ils.unc.edu.

Risks and Discomforts

- I do not know of any personal risk or discomfort you will experience from participating in this study.

Your Privacy

- For the purposes of the internal white paper, you will not be directly identified, and none of your interview responses will be quoted in any way that would specifically identify you.
- In any external publications, your identity will be known only to me, and none of your interview responses will be quoted in any way that would identify you. Furthermore, any external publications will be reviewed by the Confidentiality and Security Committee to assure that no sensitive information is inadvertently released.
Your Rights

- You decide on your own whether or not to participate in this study.
- You will not be punished or treated any differently if you decide not to participate in the study.
- If you agree to participate, you reserve the right to stop participating at any time.

Institutional Review Board Approval

- The Academic Affairs Institutional Review Board (AA-IRB) of the University of North Carolina at Chapel Hill has approved this study.
- If you have any concerns about your rights in this study, you may contact the Chair of the AA-IRB, David A. Eckerman at CB #4100, 201 Bynum Hall, UNC-CH, Chapel Hill, NC 27599-4100, (919) 962-7761, e-mail: aa-irb@unc.edu.

Summary

- I understand that this is a study to assess the need for the creation of an information security officer position at The Healthcare Facility and to determine the duties and responsibilities of such a position.
- If I agree to participate in this study, I will be asked to participate in one (45-60 minute) interview, and may be asked to participate in a brief (10-20 minute) follow-up interview.

I have had an opportunity to ask any questions I have about this study, and they have been answered for me.

I have read the information in this consent form, and I agree to participate in the study. I understand that I will receive a copy of this consent form after I sign it.

__________________________  
(Name of Participant)

__________________________  
(Signature of Participant)

__________________________  
(Date)