AN EVALUATION OF THE SKILLS REQUIREMENTS OF HEALTH INFORMATION SECURITY AND PRIVACY EXECUTIVES

by

Justin B. Fletcher, PhD

Presented to the Department of Medical Informatics & Clinical Epidemiology
and the Oregon Health & Science University School of Medicine

in partial fulfillment of
the requirements for the degree of

Master of Biomedical Informatics
June 2012

School of Medicine

Oregon Health & Science University

CERTIFICATE OF APPROVAL

This is to certify that the Master's Capstone Project of

Justin B. Fletcher, PhD

AN EVALUATION OF THE SKILLS REQUIREMENTS OF HEALTH INFORMATION SECURITY AND PRIVACY EXECUTIVES

Has been approved

Judith R. Logan, MD, MS
Capstone Advisor

Table of Contents

Acknowledgements

I would like to thank Dr. Joan Ash for providing me with the foundation to perform a qualitative study that delves beyond the basics, and to Dr. Ronald Marcum for his expertise in the aspects of clinical privacy. I would also like to thank Dr. William Hersh, who provided the opportunity and impetus to pursue this study while serving in his department as the healthcare information privacy and security workforce role lead.

I also wish to thank Dr. Barbara Swore Fletcher for her support and assistance during the writing of this document, and special thanks are reserved for Dr. Judith Logan for her patience, understanding and mentorship during this long process.

Abstract

Existing federal and state legislation provides for strong security and privacy requirements for health information. While these strong requirements exist, there is limited research on the actual responsibilities of and skills required by the information security professionals responsible for protecting patient healthcare information. In this research, a qualitative study is performed to compare the expectations of responsibilities and skills for healthcare information security and privacy officers to the perception of the actual responsibilities and skills required by current security and privacy officers. While the perceived actual responsibilities correspond to the anticipated responsibilities, the required skills are significantly different, with an emphasis on soft people skills over technical capabilities.

Introduction

Health information in the United States is considered to be private to the individual and is strongly protected by federal and state laws and regulations. Federal law requires every health care organization to have privacy and security officers [1, 2] but although there are definitions of some of the tasks that must be performed by healthcare organizations, there is no standard definition of the responsibilities of security and privacy officers.

Professional organizations have also looked at the requirements for security and privacy. The American Medical Informatics Association (AMIA) identifies security and privacy as a core competency [3] in healthcare and technology and in ethical, legal, and social issues, but does not identify the responsibilities and skills required for these competencies. The American Health Information Management Association (AHIMA) has provided job descriptions for privacy and security officers, including requirements and qualifications. This research will examine the background and responsibilities of the executives who currently hold senior positions in the protection of healthcare information and help identify the critical skills necessary to ensure that the privacy and security of healthcare information is maintained.

Background

Health information in the United States is afforded significant levels of protection. In 1995, a study was performed at the request of the National Library of Medicine, resulting in the publication of “For the Record: Protecting Electronic Health Information” [4]. In that report, the committee examined the issues of threats to health care information, the adequacy of existing privacy and security measures, future mechanisms and best practices, and barriers to adoption. The report provides recommendations for technical and organizational approaches to protect health information, including the appointment of an information security officer “who is authorized to implement and monitor compliance with security policies and practices and to maintain contact with national organizations that promulgate and enforce guidelines and standards regarding system security.” This study contributed to the primary law defining these rights, the Health Insurance Portability and Accountability Act of 1996 (HIPPA) [5]. Basic protections afforded include “procedures to assure that the privacy of individuals receiving health care services is appropriately protected” and section 1173 specifically calls for security standards that

> ‘‘(A) take into account—
>
> ‘‘(i) the technical capabilities of record systems used to maintain health information;
>
> ‘‘(ii) the costs of security measures;

‘‘(iii) the need for training persons who have access to health information;

‘‘(iv) the value of audit trails in computerized record systems; and

‘‘(v) the needs and capabilities of small health care providers and rural health care providers (as such providers are defined by the Secretary); and

‘‘(B) ensure that a health care clearinghouse, if it is part of a larger organization, has policies and security procedures which isolate the activities of the health care clearinghouse with respect to processing information in a manner that prevents unauthorized access to such information by such larger organization.”

as well as safeguards to

‘‘(A) to ensure the integrity and confidentiality of the information;

‘‘(B) to protect against any reasonably anticipated—

‘‘(i) threats or hazards to the security or integrity of the information; and

‘‘(ii) unauthorized uses or disclosures of the information; and

‘‘(C) otherwise to ensure compliance with this part by the officers and employees of such person.

In addition, section 264 calls for the recommendations for the protection of health information, including an individual’s rights, procedures for the establishment of those rights, and the requirements for the use and disclosure of that information. The responsibility to make those recommendations fell to the Secretary of Health and Human Services as there was no following legislative action. The Privacy and Security Rules [1, 2] were created by the Department of Health and Human Services (HHS) to detail the requirements for the protection of health information following significant public discussion and review. In those regulations, a healthcare organization is required to identify the security and privacy officials who are responsible for development and implementation of the required policies and procedures.

HIPAA was updated by Title XIII, the ‘Health Information Technology for Economic and Clinical Health Act” (HITECH) [6] of the American Recovery and Reinvestment Act of 2009 (ARRA) [7]. Major extensions include notifications to individuals of potential breaches of confidential information by either the health organization or a business associate where the organization must “notify each individual whose unsecured protected health information has been, or is reasonably believed by the covered entity to have been, accessed, acquired, or disclosed as a result of such breach.”[1] In addition, the organization must publicly report significant potential breaches if more than 500 individuals are involved as detailed in the Breach Notification Rule [8].

HIPAA and HITECH are just two of the federal laws affecting health information. The Office of the National Coordinator for Health Information Technology (ONCHIT or

[1] Section 13402.

ONC), a division of HHS established in 2004 through executive order, has identified nearly 50 federal laws and regulations that affect health information requirements [9]. In addition, the laws for each state must be considered on a state-by-state basis. In a report for the ONC, White et al [10] found that virtually every state allows individuals to access the medical records maintained by their healthcare providers. While some states allow access to many types of providers, others restrict access to specific types of providers, and may have different standards that apply to physicians, osteopaths, hospitals and clinics, among others.

The report also noted that few states have privacy protections as extensive as those identified in the Privacy Rule, but most have legislation that covers access to the records held by physicians and hospitals, including a patient's right to access their information, the amount of time that the provider has to respond to a request for information, and limits on the fees charged to furnish the information.

The significance of the field of healthcare security and privacy is emphasized by the identification of security and privacy as one of the twelve workforce roles identified by the ONC. These roles were created as part of Section 3016 of the HITECH Act [6] to "establish or expand medical health informatics education programs, including certification, undergraduate, and masters degree programs, for both health care and information technology students to ensure the rapid and effective utilization and development of health information technologies (in the United States health care infrastructure)." The Funding Opportunity Announcement for the Program of Assistance for University-Based Training identified security and privacy as one of six key roles to be taught at the university level, and defined the role of Health Information Privacy and Security Specialist as one with the responsibility of

> “Maintaining trust by ensuring the privacy and security of health information is an essential component of any successful health IT deployment. Individuals in this role would be qualified to serve as institutional/organizational information privacy or security officers.” [11, p. 10]

There was also an expectation of specialized education for this position:

> “We anticipate that training appropriate to this role would require specialization within baccalaureate-level studies or a certificate of advanced studies or post-baccalaureate-level training in health information management, health informatics, or related fields, leading to a university-issued certificate or master’s degree.” [11, p. 10]

Given the expectations for both staff and executive positions, it is surprising that there is limited research available on the requirements for individuals who support these rules and regulations. A PubMed search for "privacy officer" OR "security officer" returns only 54 publications, with no articles identified that described skills requirements or that addressed potential updates required by the HITECH act or responsibilities.

We see some of the general responsibilities and requirements for privacy and security officers in the legislation and subsequent rules, but need to examine these responsibilities in greater detail. One way to identify them is to examine a job description for each of these roles; two such job descriptions have been proposed in American Health Information Management Association (AHIMA) publications. AHIMA recommends that the chief privacy officer be the individual who “oversees all ongoing activities related to the development, implementation, maintenance of, and adherence to the organization’s policies and procedures covering the privacy of, and access to, patient health information in compliance with federal and state laws and the healthcare organization’s information privacy practices.” [12] The responsibilities associated with the role are significant, and nineteen specific tasks are identified. These may be summarized as serving in a leadership role, defining and implementing policies and procedures, conducting risk assessments and compliance monitoring, working with appropriate internal and external organizations, maintaining knowledge of laws and regulations, and overseeing appropriate educational activities.

The proposed *qualifications* for the role include certification as an Registered Health Information Administrator (RHIA) or Technician (RHIT) [13, 14] with appropriate education and experience, knowledge of and experience in privacy laws, knowledge of and ability to apply the principles of health information management, project management, change management, and skills in organization, facilitation, communication, and presentation.

Responsibilities identified by AHIMA are similarly demanding for the information security officer. As proposed, the security officer is “primarily responsible for all ongoing activities related to the availability, integrity and confidentiality of patient, provider, employee, and business information in compliance with the healthcare organization's security policies and procedures, regulations and law.” [15] Here fourteen responsibilities were identified, summarized as defining and implementing policies and procedures and ensuring compliance, providing security training, monitoring systems and perform risk analyses, ensuring disaster recovery and business continuity plans are in place, monitoring changes in technology, legislation and accreditation standards, serving as an internal security consultant and organizational liaison and defining security awareness activities.

The expected *qualifications* include at least a baccalaureate in a related technical field, information security certification such as a Certified Information Systems Security Professional (CISSP) [16], health information certification such as a Registered Health Information Administrator (RHIA) [14], project management skills, knowledge of computer networks and database applications, and good presentation and communication skills.

Review of the responsibilities and qualifications proposed for privacy and security officers shows a potential requirement for organizational, educational, policy, management, political, legal and technical skills with expert training, and to be a skilled technical writer and communicator. This is a daunting list of skills, and raises several questions. Which skills are perceived as important by the professionals who hold these positions? What training do individuals currently serving in these positions have? How do the training and skills required to perform these roles in practice compare with the training and skills proposed by AHIMA and AMIA? The research described here uses a qualitative methodology to begin to answer these questions.

Material and Methods

To start to answer these questions, a qualitative research study using phenomenology was performed. When performing a phenomenological study, the researcher has the objective of understanding the essence of the subject's experience [17]. The interview process continues until no additional information is obtained by further interviews, a point known as *saturation*. In this study, selected subjects were interviewed to determine their professional experiences and perceptions, and the resulting interviews were analyzed for patterns and themes.

Interviews of privacy and security officers at Pacific Northwest health institutions were conducted in order to identify the backgrounds, responsibilities and of the skills required by privacy and security professionals, as perceived by these officers. The interview questions were semi-structured and open-ended allowing the individual full explanation and exploration of the topic. The primary questions were:

- What is your title and role inside your organization?
- Would you describe your background and how it led to this role?
- What are your day-to-day responsibilities?
- Would you describe the organizational structure of your security and privacy departments?
- What skills do you see as required by a privacy officer? Which of these do you consider as critical?

- What skills do you see as required by a security officer? Which of these do you consider as critical?
- Could you describe example incidents where these skills were exercised?
- What skills do you see as becoming critical in the near future?
- What skills do would you like to see in a potential staff member?
- What skills would you like to acquire?

The questions and follow-on probe questions varied with the organizational role of the interviewee.

Candidate subjects were a convenience sample identified by their roles inside healthcare institutions in this area. These candidates were identified by examination of the corporate web sites to identify senior privacy and security officers, and by contacting the organizations directly through either e-mail or telephone. Additional candidates were identified through recommendations of other security and privacy officers by interview subjects. Once candidate subjects were identified, a recruitment letter and information sheet (Appendix A) was sent by e-mail. If the subject agreed to participate in the study, the interview was arranged at the subject’s location. All interviews were conducted in person to ensure full communication and were recorded for transcription. Interviews were conducted until saturation was reached.

The recorded interviews were than transcribed, and the resulting transcriptions were coded and analyzed line by line for thematic content using the qualitative research software MAXQDA [18].

This study was approved by the Institutional Review Board at Oregon Health & Science University.

Results

Five interviews were conducted with privacy and security officers, each associated with a different healthcare institution in western Oregon. While each privacy or security officer had individual experience and perspectives, enough commonality was expressed in their viewpoints to believe that a reasonable level of saturation was achieved by the fifth interview. The interviews are included in Appendix B, redacted to protect the privacy of the interview subjects and their respective organizations. Analysis of these interviews led to insight into the backgrounds, responsibilities and skills required of privacy and security officers. The emphasis was on the executive skills required by a security or privacy officer, and the primary interview questions do not differentiate significantly skills required of privacy officer or of a security officer.

Backgrounds

The subjects came from highly varied backgrounds. One had a clinical healthcare background prior to entering the field, while another had a basic science education. Three subjects had education and experience in information technology, and two had military experience. While three of the subjects had had limited formal education in the field, two of the subjects received training and specialized certification, one as a CISSP and one with certification in healthcare compliance. One subject observed that “it’s my feeling that most of the people who got here, it was not a planned career move. It was more or less something that’s assigned to somebody who has had experience in the hospital and other type of … responsibilities and somehow you're more or less given this responsibility, even though you never planned to be here in the first place."

Responsibilities

An analysis of the coded interviews shows responsibilities similar to those indicated by the previously identified job descriptions. Highest on the subjects' list of responsibilities are policies and procedures, management of patient record access, education and committee activities, both internal and external to the organization. Other responsibilities include compliance management, risk analysis, maintaining knowledge of regulatory updates, and acting as a subject matter expert.

Policies and procedures. The responsibility of developing and managing policies and procedures was the task most frequently referenced by the subjects. One subject entered the field as a result of wanting to address issues that required procedural management.

> "But I was the one that was pestering everybody on: How come we-, we don't have the things written down on how we, you know, passwords, any of the other procedures and . . . the backup rotations and things like that. So ITS had created a position of an Information Security Analyst and put me in that position, you know, to -, to keep me quiet. If I didn't like the answers then I could go and fix it."

This is not just a single task; it's an on-going responsibility, as noted by another subject.

> "I'm involved in regular review and revisions of our – the various policies around privacy and security as well."

Patient record access. There are two primary responsibilities when considering patient record access. One is the investigation of potential access violations; the other is providing access to and reviewing requests to amend patient records. Monitoring potential violations is a significant role.

> "I have responsibility for any type of breach investigation and also subsequent notification to patients and Department of Health and Human Services."

A significant portion of this responsibility is to determine whether a report constitutes an actual case of invalid access to patient records.

> "You might have a complaint where let's say a staff member is accused of, you know, getting into a chart where they shouldn't have and I've got to investigate that whole thing."

While there may be numerous reports of potentially invalid access, most are not considered actionable.

> "So the percentage of valid complaints, there's relatively *low*. But if we do *have* one, there's a fair amount of time that goes into that."

However, the subject observed that a significant amount of time may be consumed by a valid issue.

> "But if we *do* get a valid *complaint*, then a fair amount of time goes into it . . . I'd say maybe eight to ten hours with regard to the investigation. Possibly longer if we have to start writing reports to the Office for Civil Rights. That could double the time."

In addition to the investigation of potentially invalid access to patient records, the executives have the role of reviewing and determining if a patient record should be amended.

> “If there are requests to amend records, I review those requests and address the issue with the . . . clinical provider to determine whether we’ll allow an amendment or not.”

The process may be challenging.

> “… patients have certain rights and in two of them kind of work together. One of them is the right to have access or obtain copies of their own health information, and kind of along with that one is the right to request an amendment to your health information. So, you know, the assumption is you review your records and you see something that you think is incorrect or incomplete or just plain wrong. And so, you go back to your healthcare provider and request an amendment. Those are not very straightforward ...”

Education. Education is an on-going responsibility for the surveyed executives.

> “… we're constantly updating our … training offers. We have internal training for privacy and security in other things.”

> “I provide education to staff regarding HIPAA Privacy requirements”

> “… the final piece of that is … making sure that we provide a sufficient amount of education for folks regarding compliance.”

Educational aspects may include in-person activities as well as preparation of educational material.

> "I do spend a portion of my day on education as well …[E]very Monday we have new employee orientation and I staff a portion of those where I actually go and present myself."

Committee activities. A significant portion of time is spent working in meetings and working with committees, both internal and external.

> "I also work with about probably a half a dozen different committees that are specific to compliance, just kind of different flavors of compliance, if you will, or different aspects."

> "And then the other chunk of my time is spent going to or participating in a lot of meetings and initial discovery meetings on a topic that we're gonna need to do risk analysis on, and figuring out who the right analyst is to assign to that."

> "… there are a couple different organizations HIMSS, AHIMA, OrHIMA in Oregon, the Association of Hospitals and Health Systems. They all have different security and privacy working groups that are valuable in different ways."

Compliance. Ensuring compliance with legislation, regulation and policies and procedures is a significant role of the privacy and security officers:

> "Day-to-day responsibilities include ongoing maintenance and updates of our various online resources for compliance and for HIPAA compliance as well. We have quite a

> wide variety of online resources to support … our caregivers, our employees in the field.”

> “I’m involved in regular review and revisions of … the various policies around privacy and security as well. I also work with about probably a half a dozen different committees that are specific to compliance, just kind of different flavors of compliance, if you will, or different aspects.”

Risk analysis. One subject considered this to be the primary responsibility of the position.

> “And my primary job is to oversee our security risk assessment and risk analysis program. So everything from the way we do it … what we evaluate from a security risk perspective, how we document that, how we communicate it, where we prioritize work and where we don’t prioritize work. So that we make sure … we’re doing a reasonable and appropriate job of managing security risks rather than focusing on things we shouldn’t be focusing on.”

Regulatory updates. The subjects noted that the regulatory landscape is evolving in the healthcare industry, and it’s the responsibility of security and privacy individuals to remain informed on the current requirements.

> “I would say also keeping an eye on … in the privacy world on national discussions on privacy and so forth, and seeing whether we need to adjust our own policies.”

Subject matter expert. The subjects also noted that they are expected to be the subject matter expert in their fields.

> "I need to understand the law that I represent so I need to understand HIPAA privacy in and out so the skill that I need there is the ability to read the laws and to read the updates and to understand how they apply to us."

> "I am the, more or less, subject matter expert for people with regard to HIPAA questions with regarding privacy."

Skills

The interview phase and a thematic analysis of the coded interviews indicated that rather than emphasizing expert professional skills, importance was consistently placed on the non-technical skills: communication, judgment and collaboration.

Communication. Communication was considered the most critical skill for these roles.

> "Communication is … *the* number one."

The proper application of communication skills can also help to resolve issues and prevent unnecessary escalation.

> "I think it's the communication skills. That's incredibly important. As an example, … I've dealt maybe three or four times with Office for Civil Rights complaints, and I think, being able to communicate well over the telephone really precluded some negative interactions from them, and really precluded some … intense follow-up that might have been required if we didn't have a good communication initially over the phone."

A security or privacy officer needs to be able to communicate with individuals both inside and outside the organization, and may also include education on communication skills as described by one subject.

> "I definitely need the skill to work with people … and not just internal people but external people. It could be as simple as educating a line person on how to appropriately talk about patient information, you know, don't do it in the elevator, don't do it in the cafeteria. You know, make sure you are definitely not doing anything on Facebook or anything like that … some of the obvious stuff. But it could be as elevated as … talking to a very irritate patient and then even more so, there is this delicate balance on how to communicate with regulators."

Communication skills need to written as well as oral.

> "You have to have good communication skills, and not only with staff *within* the hospital, but also dealing, at times, with irate patients who have a real complaint … about privacy issues. You have to have good *written* skills. There have been times where I've had to respond to inquiries from the Office for Civil Rights because … they've gotten a patient complaint about privacy. And therefore, written reports have to be submitted to the Office for Civil Rights to address that particular complaint."

Judgment. A second major theme was the ability to apply good judgment. Perhaps this is best summarized by the comments of one subject:

> "The … people that I've worked with in security and compliance who probably have the most challenges are the ones who just aren't effective at *general* interpersonal

> communication, and then communication, making communications relevant to the organization that they're at. You know, beating the fear, uncertainty and doubt drum, and saying … 'The bad Romanian hackers are comin' to get us. We have to do *absolutely* everything. We're totally insecure.' Well, no - … every organization is dealing with scarce resources. You've got to apply them at the best place, so you gotta be able to communicate that you *understand* the constraints, and *why* the specific risks that you want to address are the ones that should be addressed because they are significant and real to the organization."

Another subject reminds us that we need to consider the care of the patient, beyond the strict requirements of our regulatory framework:

> "Yes, and … I also find that there are times … when staff member are overly concerned about … confidentiality to the point where it's impeding … not necessarily *clinical* care, but let's say involvement of family members with the patient. And based upon corporate policy and my other readings, you know, I can counsel staff, saying that if in your professional judgment, that family member is part of the care of the patient, you can certainly share information with that family member with regard to that care. At least for in those situations where, let's say, the patient can't really communicate at all. So … you can make a professional judgment there, to *share* information if you *do* think that it is something that will facilitate the care of the patient."

This theme was expressed by another subject in a different manner.

> "So, … you look at how people are interpreting a given say rule and – and the critical thinking comes in well, how does that really apply to us in this situation in our organization. And … if we don't comply, what's the risk; what's the risk to us as an organization; what's the risk to the patient, and really, the patient comes first; what's best for the patient. So, in my critical thinking, I'm always considering what's in the best interest of the patient and what's in the best interest of the organization as I am attempting to apply the rules. And so, that ends up perhaps being some inconsistent application from time to time."

Judgment is also necessary when considering impacts of system changes on patient care.

> "Well, … if our banking system or our wire transfer system is down for an hour, their question would be: What's the revenue impact to the organization? Which is very important to them, and it's important, you know, to us, as well, but more important would be … the question of … well, we don't wanna cause a death or an adverse outcome."

Collaboration. The ability to work positively with other individuals and organizations was viewed as a critical component of the skills required by a privacy or security officer. One subject expressed the perspective in this manner:

> "You will find the law enforcer which is really … all about coming in and telling you what you are doing wrong and trying to scare the bejesus out of you and so they use more of a fear tactic to get their way or you will find the collaborator and they are … the technical expertise but … they also have an inability to build a relationship in the

> operations world so that when people do have things going wrong, they are more inclined to call you and ask for your assistance, um instead of being afraid to tell you because they are worried about getting in trouble. My motto is you catch more flies with honey and so I totally embrace a more collaborative model and I am highly critical of my peers who use the law enforcement model and quite frankly I don't hire staff that use the law enforcement model. It is all about what value we can add when we come to the table."

However, though collaboration is a necessary skill, it can be difficult to accomplish in the role.

> "There is the ability to work collaboratively. … I think … a privacy officer is most successful if they are able to integrate themselves into the day-to-day operations of the organization. That's a very tough challenge. Certainly, in my experience and in talking with other privacy officers that I know, we're often seen as the police, as outsiders, and not necessarily welcome. And I've been doing this work, you know, since the – from the beginning before, you know, the HIPAA privacy regulations were final. And it's really only within the last two or three years that I feel like I'm really starting to make inroads with our operations folks."

Additional skills. Numerous other skills were suggested as elements of the skills needed by healthcare privacy and security officers. These included attention to detail,

> "You have to be a little bit OCD [laughs]. You know you really have to pick up on details and make sure you're keeping track of all type of things."

management skills,

> “Sometimes if you feel like you’re herding cats, but I’m sure I’m not the only one that feels that way in their position …”

and ethics:

> “I think the skills that I am always looking for is analytical skills and an attention to detail. Um, obviously honesty and integrity, I think that is just absolutely paramount …”

Technical skills were also viewed as an important capability:

> “I think you … really do have to have a knowledge about the technology involved. Electronic communication, you know, involves the electronic medical record, just all types of electronic type of *issues* … and you really need to be aware of what that technology is and how it works and the consequences of those technologies.

These skills were considered to be significant for both privacy and security officers:

> “Well, obviously skills with regard to technology. You know, it’s interesting. The Privacy Official deals primarily with written and verbal communication. Security Official has to deal with all the electronic information … that comes under HIPAA, and more and more information is going to be in that realm. And … so an awareness of all the technology that potentially could impact confidentiality is really important.”

Analytical and political skills were also considered a useful skill:

> “I actually enjoy investigating or researching laws and regulations, and – and making sure that we are doing the right thing. There are the political aspects and I’m not talking about national … or state … or … political kinds of things but there are, you know, internal political aspects that are – are less enjoyable.”

While additional skills were mentioned by the interview subjects, it’s also important to observe that while not a significant theme, professional capability is expected of the individuals in these positions:

> “The most crucial skills, if you are going to hit the ground running then you know, being a subject matter expert on whatever law you are going to be representing so for a privacy or security official, you know, an in and out understanding of the HIPAA privacy and security rules.”

> “I’m kind of leaving unsaid … to me there’s an implied - they have to … be *experts* in that field. They have to have a full understanding of the security control requirements and compliance requirements, regulations, corporate culture and policy, and how that influences what is OK and what’s not OK.”

Discussion

> "I do think there is a difference between what someone in the *healthcare* does for information privacy and security as opposed to some of the other industries. 'Cuz we are a little bit *different."*

We have seen significant requirements for the protection of health information in federal and state laws and regulations, from the Health Insurance Portability and Accountability Act of 1996 to the Health Information Technology for Economic and Clinical Health Act [5, 6] with the resultant Privacy Rule, Security Rule and Breach Notification Rules [1, 2, 8]. The requirements include controlling access to a patient's health information, ensuring that patient records are properly protected and that unintended disclosure is identified and reported. These federal laws also define the requirement for healthcare organizations to identify privacy and security officers who are responsible for the development and implementation of the policies and procedures to meet the requirements to appropriately protect patient health information.

Both the Office of the National Coordinator (ONC) and the American Health Information Management Association (AHIMA) identify specialized education or certification as part of the background expected for privacy and security officers. AHIMA specifically lists certification as a Registered Health Information Administrator (RHIA) or Registered Health Information Technician (RHIT) for a chief privacy officer and certification as Certified Information Systems Security Professional (CISSP) or RHIA for a security officer. However, only two of the interviewed privacy and security officers selfidentified as being certified. This may be because that the interview subjects can be considered a first generation of privacy and security officers and obtained the necessary skills under operational circumstances, or it may be that these privacy and security officers do not consider certification to be critical to their background.

The expected responsibilities for the position of a chief privacy and security officers were identified from job descriptions published by AHIMA. These responsibilities were significant, including leadership, policy definition, risk assessment, organizational involvement, maintaining knowledge of laws and regulations, disaster recovery planning, knowledge of technology and serving as a subject matter expert. The analysis of the interviews showed the subjects currently serving as privacy and security officers perceive that their responsibilities are similar to the identified list of professional responsibilities.

The expected skills for chief privacy and security officers were also identified from the AHIMA job descriptions. These skills include knowledge of privacy laws, health information management, project management, change management, organization, specialized technology, communication and presentation.

The interviewed privacy and security officers placed an unexpected emphasis on the required skills for these positions. A preconception of these skills required for individuals in these positions from laws, regulations and job descriptions might expect the critical skills to be the ability to interpret rules and regulations, to craft policies and procedures and to perform a risk analysis. However, while these skills are still considered necessary, the subjects placed an strong emphasis on skills such as the ability to successfully communicate at many levels and with many different internal and external organizations, to apply judgment to determine the actual risks to the organization and the patients and know when to be flexible in interpretation, and to be able to collaborate with many individuals, groups and organizations. While technical capabilities are still required, there is agreement that the emphasis is on the soft, or people skills.

It’s worth observing that these professionals enjoyed their roles in their organizations. As one subject said, “It’s a great . . . fun, most of the time.”

While this study is limited in that interview subjects are from a single region, it is believed that this study should be generalizable across a broader population. The interview subjects were from independent healthcare organizations and there was a strong sense of agreement on the responsibilities and skills for privacy and security officers which are based on national, not regional, requirements.

Further research is warranted into the exploration of security and privacy positions at healthcare organizations. It is possible that at a more junior position the emphasis is on the more technical skills rather than the communication, collaboration and judgment required of a senior individual. An additional research area would be to examine and compare the necessary skills for senior executives in other area, such as in the financial and industrial sectors, to determine if there is a similar emphasis on people skills at the executive level.

Conclusions

The healthcare setting in the United States places a high premium on the protection of healthcare information, as is evident from the legal and regulatory requirements at federal and state levels, and from the inclusion of the knowledge and training requirements in federal legislation and national organizations such as AMIA and AHIMA.

Limited previous research exists on the actual background, responsibilities and skills of the individuals who protect that information in the role of an organization's privacy or security officer. This research, by examining the perceptions of healthcare security and privacy officers, is an initial examination of these backgrounds, responsibilities and skills. We learned that backgrounds are extremely varied, that the responsibilities are as broad and significant as anticipated, and, most important, that while technical expertise is expected, the most important skills perceived as the most important for the role of a chief privacy or security officer are the “soft” skills of communication, judgment and collaboration.

References

1. U.S. Department of Health & Human Services, *The Privacy Rule*, 2008. Retrieved from http://www.hhs.gov/ocr/privacy/hipaa/administrative/privacyrule/index.html.

2. U.S. Department of Health & Human Services, *The Security Rule*, 2009. Retrieved from http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/index.html.

3. Kulikowski, C.A., et al., *AMIA Board white paper: definition of biomedical informatics and specification of core competencies for graduate education in the discipline.* J Am Med Inform Assoc.

4. National Research Council, *For the Record: Protecting Electronic Health Information*. 1997: The National Academies Press.

5. *Health Insurance Portability and Accountability Act of 1996*. Public Law 104–191. 110 Stat. 1936. 1996.

6. *Health Information Technology for Economic and Clinical Health Act*. Public Law 111–5. 123 Stat. 226. 2009.

7. *American Recovery and Reinvestment Act of 2009*. Public Law 111–5. 123 Stat. 115. 2009.

8. Department of Health and Human Services, *Breach Notification for Unsecured Protected Health Information.* Federal Register, 2009. 74(162).

9. The Office of the National Coordinator for Health Information Technology, *Summary of Selected Federal Laws and Regulations Addressing Confidentiality, Privacy and Security*, 2010. Retrieved from http://healthit.hhs.gov/portal/server.pt/gateway/PTARGS_0_11113_911059_0_0_18/Federal%20Privacy%20Laws%20Table%202%2026%2010%20Final.pdf.

10. White, J., J. Daniel, and S. Posnack, *Privacy and Security Solutions for Interoperable Health Information Exchange: Report on State Law Requirements for Patient Permission to Disclose Health Information*, 2009. Retrieved from http://healthit.hhs.gov/portal/server.pt?open=18&objID=910326&parentname=CommunityPage&parentid=6&mode=2&in_hi_userid=11113&cached=true.

11. Office of the National Coordinator, *American Recovery and Reinvestment Act of 2009: Information Technology Professionals in Health Care: Program of*

Assistance for University-Based Training Funding Opportunity Announcement. 2009, U.S. Department of Health and Human Services,.

12. American Health Information Management Association, *Sample Position Description: (Chief) privacy officer.* Journal of AHIMA, 2001. 72(6): p. 37-38.

13. American Health Information Management Association, *Registered Health Information Technician*, 2012. Retrieved from http://www.ahima.org/certification/rhit.aspx.

14. American Health Information Management Association, *Registered Health Information Administrator*, 2012. Retrieved from http://www.ahima.org/certification/rhia.aspx.

15. American Health Information Management Association, *Sample Security Officer Position Description*, 2003. Retrieved from http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_019915.hcsp?dDocName=bok1_019915.

16. International Information Systems Security Certification Consortium, I., *Certified Information Systems Security Professional*, 2012. Retrieved from https://www.isc2.org/CISSP/Default.aspx.

17. Crabtree, B.F. and W.L. Miller, *Doing qualitative research*. 2nd ed. 1999, Thousand Oaks, Calif.: Sage Publications.

18. VERBI GmbH, *MAXQDA*. 2012.

Appendix A: Study Information Sheet

eIRB# IRB00007644

OREGON HEALTH & SCIENCE UNIVERSITY

Study Information Sheet

TITLE: Skills Requirements for Health Information Privacy and Security Officers

PRINCIPAL INVESTIGATOR: Justin Fletcher, PhD (503) 494-4494

CO-INVESTIGATOR(S): Judith R. Logan, MD (503) 494-5902

PURPOSE:

You have been invited to participate in this research study because you are a health information privacy or security officer, have supervisory responsibilities for privacy or security officers, or are a key member of the health information privacy or security organization. The purpose of this study is to determine the skills and background of existing information security officers and to determine the requirements for such a position.

A total of 24 subjects will be enrolled for the entire study.

PROCEDURES:

For this study, you will participate in a recorded interview on your background and on the skills that you believe are appropriate for health information security and privacy executives.

<u>RISKS AND DISCOMFORTS</u>:

There are no known risks and discomforts.

<u>BENEFITS</u>:

You will not personally benefit from participating in this study. However, by serving as a subject, you may contribute new information which may benefit others in the future.

<u>ALTERNATIVES</u>:

You may choose not to participate in this study.

<u>CONFIDENTIALITY</u>:

Neither your name nor your identity will be used for publication or publicity purposes.

<u>COSTS</u>:

There is no cost to participate in this study.

Appendix B: Redacted interviews

Interview 1

JF: Today is February 2nd, 2012. Ground Hog-, Ground Hog Day.

Subj: And it's sunny outside.

JF: Yes, so maybe that-, maybe that means six weeks of win-, winter will start.

Subj: Yeah, ha ha.

JF: I'm Justin Fletcher with Oregon Health and Science at the University and we are interviewing at [redacted], and if you could give me your name and role?

Subj: Yeah, it's [redacted]. I'm the HIPAA Privacy [redacted] at the hospital. And that's one responsibility I have, amongst others. Would you like to know what the others are?

JF: Please.

Subj: [redacted]

JF: And obviously, I'd like to confirm that you're willing to participate in these interviews. The results will be anonymous, hopefully for-, for publication but any information will be anonymous.

Subj: Yeah, I'm willing.

JF: OK. And I have the in-, have the tape recorders going. Is that OK?

Subj: That's fine with me.

JF: Great, thank you very much. So tell me, a little more formally or informally perhaps what-, what your role within the organization is.

Subj: Well, with regard to HIPAA Privacy, I provide education to staff regarding HIPAA Privacy requirements. I am the, more or less, subject matter expert for people with regard to HIPAA questions with regarding privacy. I have responsibility for any type of breach investigation and also subsequent notification to patients and Department of Health and Human Services.

With regard to the processes we have here, we have a HIPAA Privacy Committee. The Chairman is our [redacted], but I'm the one who pretty much does all the support. Developing agendas and writing up the minutes and presenting the various reports that are necessary to track where we're going.

JF: And do you have a separate Security Officer? Or is that also part of your role?

Subj: No, we do have a separate Security Officer. [redacted]

JF: What would you describe your background and how it led to this role?

Subj: [redacted]

[redacted] HIPAA Privacy Official being one of those additional responsibilities that was given to me.

JF: It may sound like an odd-ish question, but do you enjoy it?

Subj: Yeah, it is really quite interesting. It's interesting to interact with the various *people* who have HIPAA concerns. It's also one of the few opportunities I have to-, to be involved with a-, a committee outside of the hospital. The Hospital Association has a Compliance Committee, which initially started as a HIPAA Compliance Committee so I interact with a lot of colleagues there. And it's kind of interesting, keeping up on the various revisions to HIPAA, you know, HITECH came out not too long ago. So there's-, there's always something new going on.

JF: What would you say are your day-to-day responsibilities?

Subj: With regard to HIPAA? Actually, it's-, it's more or less hit and miss. If there is a . . . a breach of privacy, I get involved in that particular investigation. If there are requests to amend records, I review those requests and address the issue with the . . . clinical provider to determine whether we'll allow an amendment or not. And then I-, I get involved in various other requests from-, from patients. So on a day-to-day basis, there are times maybe nothing happens with regard to HIPAA.

Other times, you know, you've got a full-scale investigation. You might have a complaint where let's say a staff member is accused of, you know, getting into a chart where they shouldn't have and I've got to investigate that whole thing.

JF: How often would you say that you're performing the investigative role?

Subj: Well . . . we had [redacted] reportable breaches last year. There are . . . I would say, maybe [redacted] impermissible disclosures which . . . because they did not pose a *risk*, never elevated to become a reportable breach. But I have to do a minor investigations with regard to that. So . . . it's possible I might have to do some minor type of investigation maybe once a week or so.

JF: With regard to patients, how often do they come to you with an issue?

Subj: Just looking back on the last year, I'd say . . . maybe once a month. You know, maybe 20 times a year we have some kind of patient complaint with regard to privacy issues.

JF: I know we're getting slightly off topic, but how often are those, from-, in your personal viewpoint, how often are those complete, those complaints . . . *reasonable?*

Subj: Well, valid? Yeah, let's say we had 20 last year, and only three were determined to be reportable breaches. So I'd say, you know, 3 out of 20 were actually valid complaints. Many of-, most of the rest of them were not-, not substantiated as really being a valid complaint.

JF: OK. Beyond you and the [redacted], what is the remainder of the organizational structure of your security and privacy departments?

Subj: Well, with regard to privacy, we do have our HIPAA [redacted] Committee that meets on a monthly basis. We have the hospital security official, [redacted]. We have nursing representation. We have rep-, representation from our medical records Department, so they're-, they all get involved with regard to that committee.

With regard to security, quite frankly, I don't know not that much about what happens there. It's the [redacted] responsibility and a lot of the [clears throat] direction there comes from our corporate office in [redacted] because it's very much involving I.T. and Corporate initiatives.

JF: So as a Privacy Officer, what skills do you see as really being required by a Privacy Officer?

Subj: OK. You have to be a little bit OCD [laughs]. You know you really have to pick up on details and make sure you're keeping track of all type of things. One, you know, you have to be able to educate. I think it's very important that you provide the appropriate education to all staff members. Secondly, you have to be able to keep up on the particular regulations so that you can serve as the subject matter expert. You have to have good communication skills, and not only with staff *within* the hospital, but also dealing, at times, with irate patients who have a real complaint about-, about privacy issues. You have to have good *written* skills.

There have been times where I’ve had to respond to inquiries from the Office for Civil Rights because they’re-, they’ve gotten a patient complaint about privacy. And therefore, written reports have to be submitted to the Office for Civil Rights to address that particular complaint. So I think, you know, more of the standard skills that a really good manager would have are the type of things you need with regard to HIPAA.

JF: Of these skills, what would you view as the most critical?

Subj: I think it’s the communication skills. That’s incredibly important. As an example, you know, I’ve dealt maybe three or four times with Office for Civil Rights complaints, and I think, being able to communicate well over the telephone really precluded some negative interactions from them, and really precluded some, you know, intense follow-up that might have been required if we didn’t have a good communication initially over the phone.

JF: Let’s take your catterport-, your counterpart. What skills do you see as required for a Security Officer?

Subj: Again, that’s not an area where I have a lot of knowledge but . . . I think you-, you really do have to have a knowledge about the technology involved. Electronic communication, you know, involves the electronic medical record, just all types of electronic type of *issues* and . . . and you really need to be aware of what that technology is and how it works and the consequences of those technologies.

JF: OK. And would it be possible for you to take-, and consider or two, that you've had to deal with and describe them in a bit more detail?

Subj: OK. Again, I won't use any patient identifiers.

JF: Of course.

Subj: No-, no names or any-, anything to identify a patient. But last year an issue came up. We had a young patient in the hospital who was comatose and the parents had been visiting, and they started-, they contacted me and indicated that there was a . . . a caregiver here at the hospital who was also known to them socially, who approached them, indicating that they had information about the patient's son, that nobody would know about unless they actually *looked* at the medical record. And so the parents were very concerned that the confidentiality of their son had been breached. We did an investigation and we do have software here that will identify all people who have accessed the electronic medical record. We determined that the employee who that they had a concern about indeed, accessed the son's medical record, even though that employee, at no time, was in-, involved in the care of the *son*. This was a breach of confidentiality. After discussion with the department head and our [redacted] we decided to terminate that employee. So . . .

Other type of investigations: We had a complaint . . . [redacted] we had a complaint from woman that there was . . . Her husband was the patient in the agency and yet she felt that people were looking into *her* medical record and discussing it in the physician's office. After extensive investigations and everything, we found that *that* complaint was not founded, at *all*, and we provided the appropriate information to the Office for Civil Rights, and they agreed with us, that that complaint was-, was not a valid complaint.

So we've-, we've had both kinds – valid and invalid complaints.

JF: How often do you think that a-, a complaint is-, is justified? How much of your time are you-, are you spending on issues that people are complaining about but really-, that they really shouldn't be?

Subj: Yeah, like I mentioned, I think last year maybe 3 out of 20 complaints were actually *valid*. But if we *do* get a valid *complaint*, then a fair amount of time goes into it. I . . . I'd say maybe eight to ten hours with regard to the investigation. Possibly longer if we have to start writing reports to the Office for Civil Rights. That could double the time. So the percentage of valid complaints, there's relatively *low*. But if we do *have* one, there's a fair amount of time that goes into that.

JF: What skills do you see as really becoming critical in the near future?

Subj: Well, obviously skills with regard to technology. You know, it's interesting. The Privacy [redacted] deals primarily with written and verbal communication. Security Official has to deal with all the electronic information that-, that comes under HIPAA, and more and more information is going to be in that realm. And . . .

and so an awareness of all the technology that potentially could impact confidentiality is really important.

You know, an example, and I think it's something that all the organizations are dealing with now, is the at-, is the . . . enormous use of cell phones with cameras, staff potentially discussing issues on Facebook. All of that technology, it could potentially be a real risk to patient confidentiality. So I think that's an area that really, everybody needs to be aware of.

JF: If you were having a-, a new staff member join your organization, what skills would you like to see them coming in with?

Subj: Joining the organization in what-, in what capacity I-, I guess I'm . . .

JF: Joining you to work, to work on HIPAA Privacy.

Subj: Oh, on HIPAA Privacy? I think they would have to have a-, a good background regarding how healthcare is provided within a hospital. I think they would have to have a good background with regard to the electronic medical record, and also the processes that take place in a medical records department. I think, you know, they need the skills that I mentioned to you before, in terms of communication. But they would have to be aware of the various technologies that could impact patient confidentiality.

JF: What skills would *you* like to acquire?

Subj: What skills would *I* like to acquire?

JF: Yeah.

Subj: I'm not even on Facebook [laughs] so . . . You know, I think I really do have to beef up some of the things I do with regard to social media. I need to-, yeah, I need to probably learn more about *that.* And-, and *again*, you know, I'm really kinda concerned. We've heard so much about, you know, staff members getting things onto social media that, you know, impacts the organization and potentially could breach confidentiality. And you know, that's just an area I-, I don't know that much about.

JF: Have you seen cases of that?

Subj: I am not aware of any cases *here*, but at our [redacted] meetings, there's certainly been a-, a lot of discussion about those type of issues.

JF: What questions didn't I ask?

Subj: Let's see . . . Yeah, I-, I-, I think it's this whole question about how do you-, how did you get into your present position? And . . . it's *my* feeling that most of the people who *got* here, it was not a *planned* career move. It was more or less something that's *assigned* to somebody who has had experience in-, in the hospital and other type of . . . responsibilities and somehow you're more or less *given* this new responsibility, even though you never planned to be here in the first place. So it's really interesting, you know, how-, how do you *get* to where you *are* with regard to being a HIPAA Privacy [redacted].

JF: I have to ask, considering all of that: How do you manage to keep up on all the laws and regulations that affect privacy?

Subj: Yeah, that-, that's a-, that's a concern I have. There are a few ways. Certainly meeting with the Compliance officials through the Hospital Association is very helpful. There's a lot of information that's shared there. Secondly, we're part of a-, a [redacted] system so there's a [redacted] office down in [redacted] [redacted]. We have a [redacted] HIPAA Privacy [redacted] who does provide information to *us*. And there are various list serves and email services that I-, I participate in where I do get new information as it comes out.

RECORDING PAUSED

RECORDING RESUMED

JF: We're continuing our discussion on judgment and what's we're used to . . .

Subj: Right, and-, and I have to say that there are times I get questions from staff members and I'm not absolutely sure I have the correct answer, but I make a judgment call. And part of that judgment has to take into account what's a reasonable accommodation, with regard to protecting confidentiality?

As an example, we have a clinic where they're storing medical records, and I received a call from the manager, indicating that there is-, they're undergoing a remodel of the clinic and what type of safety windows should they be installing in this clinic now, to really protect the records? And I indicated that we shouldn't really go beyond what we normally do in a clinic. If things are *locked*, that's a reasonable accommodation. We don't have to put bars on the windows and really spend an enormous amount of money to protect those medical records, beyond what we would normally do in a clinic setting.

And there were other times where you get a call, people need an immediate answer. You're pretty sure about what you're doing but you can't quote the regulations or requirements, and you do make judgment calls. Sometimes they might not be *correct*, but you're doing what you think is the best at that particular moment.

JF: Do you sometimes find people that seem to be *overly* concerned with the fine points of security.

Subj: Yes, and I-, and I also find that there are times when . . . when staff member are overly concerned about . . . about confidentially-, confidentiality to the point where it's impeding . . . not necessarily *clinical* care, but let's say involvement of family members with the patient. And based upon corporate policy and my other readings, you know, I can counsel staff, saying that if in your professional judgment, that family member is part of the care of the patient, you can certainly share information with that family member with regard to that care. At least for in those situations where, let's say, the patient can't really communicate at all. So you know, you can make a professional judgment there, to *share* information if you *do* think that it is something that will facilitate the care of the patient.

JF: Thank you very much.

Subj: You’re welcome.

END OF RECORDING

Interview 2

JF: Turn on record, I think. Today is Friday, February 3rd, the post Ground Hog Day on-, in 2012. I'm Justin Fletcher from Oregon Health and Science University. And today I am-, I am talking with . . .

Subj: [redacted].

JF: And your-, your title is?

Subj: I'm the Information [redacted].

JF: Thank you. Now, first of all, it is-, are you willing to participate in this-, in this study?

Subj: Yes, I am.

JF: Thank you. And is it all right if-, if we keep the recorders running?

Subj: Certainly.

JF: And the in-, the interview is at the [redacted]

Subj: [redacted]

JF: All right, thank you. So can tell-, can you tell me your title and role inside both [redacted]

Subj: Well, there's a separation from how each hospital conducts its own business. I'm at the-, [redacted], so my *primary* duty is the-, the HIPAA person [redacted].

JF: And when you say, 'HIPAA Person,' what do you mean by that?

Subj: Well, I did the implementation of our-, our HIPAA processes and procedures and continued to answer questions and run audits, and keep track of things like that. I do a lot of policies and procedures.

JF: OK.

Subj: To back those up. I do the HIPAA, security risk assessments.

JF: OK. How would you describe your-, your background and how you ended up in this position?

Subj: [redacted] So I have an I.T. background for many, many years. But I was the one that was pestering everybody on: How come we-, we don't have the things written down on how we, you know, passwords, any of the other procedures and . . . the backup rotations and things like that. So [redacted] and put me in that position, you know, to-, to keep me quiet. If I didn't like the answers then I could go and fix it. So that's what I did and I-, I rolled out HIPAA in that role [redacted] And then when we had our HIPAA Security assessment, it was felt that we should have a corporate level [redacted]

JF: Do you enjoy what you're doing?

Subj: It's a great . . . fun, most of the time. Sometimes if you feel like you're herding cats, but I'm sure I'm not the only one that feels that way in their position so . . .

JF: OK. When you say you're developing policies, where do you get the information to base the-, to base the policies upon?

Subj: It depends on what the policy's *for*. So I do a lot of keeping track of any state or federal regulations that are coming down that are going to impact either the HIPAA Privacy, security or anything that we're doing, and so our-, we had . . . I'll give you an example. The red flags rule for the-, the . . . from that particular piece and we had to roll somethin' out to track down potential patient identity thieves and the organization, and so I put together the group that wrote the policy and how we're gonna do it, and how we keep track of those. When we call the police, when we don't, that type of stuff.

JF: Do you have to do that often?

Subj: More often than I would *like*. We very rarely find them while they're still *here*, which is the only time we call the police. If we have somebody that we think is using someone else's I.D. and they're still in house, then we'll call. Otherwise, we usually don't find out about it until the wrong patient was billed.

JF: You commented, and this is on the state and federal regulations. There are a huge number of change in regulations. How do you keep that information current? Where do you find your most current information?

Subj: Actually, since this is healthcare, we work a lot with the [redacted], and they keep, as far as the-, the sta-, the federal . . . Well, not so much the federal but the state regulations, and then it's just goin' out there and make sure you're on all the appropriate list serves so that you get notification when new things are coming up. And doing lots of reading.

JF: What would you describe as your day-to-day responsibilities?

Subj: My day-to-day responsibilities are patient requested audits, lots of policies and a little bit of information security sprinkled in.

JF: OK. How often do you need to-, to do a patient-requested audit?

Subj: They seem to go in waves. But I'd say, on an average, about once a week.

JF: OK. And . . . how many-, how many of those requests would you view as valid?

Subj: Well, they're all *valid*. They may not all turn out the way that the patient *expects* them to turn out, but they're all-, all . . . I like them from the sense that it gives us a chance to practice our procedures and how we-, we handle incidents, and how those things get reported to me, and how they go on down the-, the chain so to speak. So it's good from that standpoint. We have to audit our systems. This gives us an opportunity to *do* that. I'm not-, I'd say about half of the time whatever the patient suspected was happening with their record is-, is correct.

JF: Mm-hmm. OK. And on a day-to-day basis, and what do you really do? What's-, what's your most critical function?

Subj: Critical from whose point of view?

JF: From *your* point of view.

Subj: From *my* point of view? The audits and the policies and fielding questions.

JF: Can you describe the organizational structure . . . of your org-, well, redundant. Can you des-, describe the structure of your organization?

Subj: Structure, as in the . . .

JF: Well, for the . . .

Subj: . . . organizational chart? Or . . .

JF: . . . for the security and privacy departments. Effectively, organizational chart.

Subj: [redacted] We have a process that we call [redacted], so if we have a policy that says you're screen saver is supposed to come on every 20 minutes, and we have areas, for example, the O.R., where that's not gonna work. They need a longer time. We've got a process to-, to keep track of those and approve those, and . . . and that committee does that, as well.

JF: And as a Privacy Officer, what skills do you see are really required to perform that role?

Subj: Well, I'm the [redacted]. So for my role, and the CISSP, if you're gonna be at the management level, you have to have an I.T. background to do this. You don't have to have a certificate, but if you've got the-, the I.T. background and the-, and the willingness to read the regulations, and to push those out, I think anybody could do it. I think right now there's not as many . . . degrees, though I see that are some coming out now, as far as college degrees for this type of a-, a role. And so most of the folks that I talk to when I go to conference and stuff have been, basically they've just been doing it. They've come up through the-, the I.T. ranks more or less.

JF: OK. And . . . what do you think is the most critical skill?

Subj: You have to *like* it. I mean, it's . . . you can have people who-, you just have to like the security. You have to be a bit of a-, a geek. People who like to . . . to know *why* things are-, are set that way and-, and question things. You know, why do we have to do it that way? And why can't we do it *this* way?

JF: OK.

Subj: People willing to-, to open those cans of worms.

JF: OK. It seems as if you've got multiple roles then. From the-, from the policy side, you've got the privacy side; from the technology side you have the security piece. Do you see differences in skills between those two?

Subj: Not for a role at this level. At least for an organization of our size. I mean, there's basically me, and the [redacted]. Some larger organizations, they have some of that stuff, carpent-, compartmentalized a little bit better or *differently* so that you have more of a security person who primarily just does the-, the I.T. piece of security. And we don't have that so it's more of a-, a catch-all.

JF: And do you . . . do you find yourself being stretched a little thin?

Subj: It gets a bit chaotic, at times, yeah. A lot of, you know, runnin' around and . . . difficult to-, to stay ahead of things.

JF: And do you have some incidents that you're willing to describe that exercise some of these skills?

Subj: That exercise the *skills*? [pause] Well, I'm not quite sure what you're after there as far as skills or what I'm doin' or . . .

JF: Well . . . well, one example is . . . how you would-, how you caught the people who are . . . have the potential for identity theft. Do you have-, do you have others like that?

Subj: We have the identity theft issue and I hear about those. We get calls from Patient Registration, or somebody who's up on the floor and they saw somebody who is in today, saying they're patient Smith, but the remember treating them several weeks ago as patient Jones. And so at *that* point, I get a call and we'll go through some records and see if we can confirm that we *think* it's an issue, and if they're in-house, we'll call the police.

JF: Are there other incidents that you can talk about?

Subj: Well, we have the . . . the audits that I run when patients call. They are concerned that somebody's been in their record, and they wanna know if that's true, so we have to coordinate our-, coordinate with our top 16 systems. Then we have audits run and call and talk the patients back and forth through that. And that is a bit of a challenge at times, as we have a long list of people who are in records and trying to determine who is the *correct* person to be in the record and not.

JF: And do you often-, often find examples of inappropriate access?

Subj: My concern with inappropriate *access* is we usually don't find about-, out about them until after the fact. You know, the computer systems, the applications are not at the point where they can say, 'Dr. Fletcher can't be in this record because he doesn't *treat* patients like this.' So we wouldn't find out about any type of inappropriate access until somebody either *saw* somebody doin' somethin' that they *shouldn't* be doin', or we hear from the patient, or somebody, they think somebody was in their record because their neighbor was tellin' 'em about it. So it's-, it's a challenge from that standpoint. I don't *like* it that we have to wait 'til after the fact because then the damage, if there's any damage, it's already been done. It's already happened.

JF: What skills do you see as becoming critical in the near future?

Subj: Boy, I don't see anything different or than there's a lot more stuff – regulations, the issues around Meaningful Use, and electronic medical records. Right now we're a hybrid *here*, with a lot of paper records still. We have a paper chart that's up on the floors. With electronic medical records you just have a whole much more issue from an access standpoint, and there's just so much more that people can *get to* easily. Where with the *paper* record, it's a little bit . . . a *slightly* more controlled. They can't get it out of Medical Records without checking it out and passing certain things. But if they have the electronic access they can get to it and then depending on how quickly the audits can locate that stuff, or we hear about it from patients, it's-, it's done.

JF: What skills would you like to see of a potential staff member?

Subj: I would like to see somebody who really knew their computer systems . . . understood the *laws*, and how to really-, a way of explaining those types of issues to management and the folks who have to-, to follow the policies that they may or may not agree with. They don't *like* to have to change their password. They'd like to keep their current password they've used for the *last* ten years. They *know* it. Why do I have to change it?

JF: [pause] When you get a ques-, question like that, how do you deal with it?

Subj: Well, it's . . . it's *difficult*. I just try to explain what a password *means* and would they like to share their ATM password with *me*, or their online banking account password, assuming that they ever change those, just to try to make it a little more personal. We've got to protect our information. One [redacted] values is respect. I like to use that one, too, and say it's respect for our patients, too, and their privacy, as well. And what were they doin' in their record is important.

JF: What skills would *you* like to acquire?

Subj: I would like to have a little more of an auditing background. You asked before about what, in the future, auditing would be something that we could use here. I see a . . . we have a pretty good program here for information privacy and security. I would like to-, to take it to the next level. A little more proactive auditing and a little more being able to *prove* that we're doin' a good job, other than we're not reading about ourselves in the paper, as a measure.

JF: What didn't I ask?

Subj: [pause] I don't know. You didn't ask how *long* I've been doin' this.

JF: OK. How long?

Subj: [laughs] Well, now, I started in [redacted].

JF: OK. So you're well-familiar with the processes.

Subj: Yes.

JF: It’s the . . . then what didn’t I ask could also be translated as . . . you’ve seen the type of questions I’m trying to answer . . .

Subj: Well, right. No, and this is . . .

JF: . . . And what else? What else would you like to tell me?

Subj: You’ve got the Health Information Privacy and Security Officers in it, and I do think there is a difference between what someone in the *healthcare* does for information privacy and security as opposed to some of the other industries. ‘Cuz we are a little bit *different.*

JF: Right.

Subj: And so that . . . that makes a-, a big, big difference.

END OF RECORDING

Interview 3

JF: Let's see, today is February the 14th, 2012. We're talking at-, at noon on Valentine's Day. I'm Justin Fletcher, and if you could give me your name and your role?

Subj: My name's [redacted]

JF: OK. And I'm interviewing in [redacted] at the [redacted]. And are you willing to participate in this? As it-, and is it all right if I keep the recorders going?

Subj: Yes, it is.

JF: Thank you very much. So . . . again, would you mind repeating your title and your role inside [redacted]?

Subj: [redacted] And my primary job is to oversee our security risk assessment and risk analysis program. So everything from the way we do it, what we-, what we evaluate from a security risk perspective, how we document that, how we communicate it, where we prioritize work and where we *don't* prioritize work. So that we make sure we're getting-, we're doing a reasonable and appropriate job of managing security risks rather than focusing on things we shouldn't be focusing on.

JF: [redacted] It's got to be a very large responsibility.

Subj: It *is*, I mean, like-, like so many things, it's all a matter of having the right people . . . *doing* the work, trained the right way. Speaking a common language, and that's been-, I've been here for-, for four years now . . . And that was, you know, the better part of a year and a half was spent making sure that we did that, getting a common lexicon to speak about risk. Doing a lot of training with people, putting people in the right positions, so that they could build the relationships to get the information that's needed to *do* that kind of work.

JF: That's *exactly* the sort of information I'm looking for. You've identified the right people, trained the right way. What does that mean to you?

Subj: So . . . it's . . . it's organizational . . . it's organizationally specific, first of all. It's also vertically specific so industry-wise. So if you're talking to a security professional who works in critical infrastructure or in financial services, or in government, it might be-, well, it *would be* different, and I've worked in multiple different verticals earlier in my career. The healthcare one . . . and-, and the reason it's so different is . . . well, there are several. The-, the risk appetite and the compliance requirements and the-, and the legal requirements are *different* across those verticals. But I think even more important, the language and the culture and the *business*, though we don't certainly like to call healthcare a business necessarily. Nor does . . . nor does OHSU for that matter. Is different, and there's a language and a culture around *that*, as well. So communicating risk to I.T. people and communicating I.T. risk to I.T. people is-, is *one* matter, and there's little consistency across verticals in that. But the minute you get to the more important area of communicating it to the Board of Directors, to Senior Leadership, all the way on down that line, you really have to put it in *relative* terms with *other* risks that they deal with. So in Healthcare, those risks are decidedly different than they are in a-, in a DOD, you know, governed organization, confidentiality is certainly very important. But availability and data integrity are also very important, to varying degrees from one organization to the next. So that-, that's a huge factor, is being able to communicate appropriately for the organization that you're with.

JF: A lexicon and language is something that surprises me a bit. I haven't heard of that before. Can you give me an example of . . . of having to come up with a right language through the organization?

Subj: Absolutely so . . . The-, the word 'risk' has to be-, has to have a meaning and a definition if you're gonna start using it in reports or in conversations with a certain level of leadership in the organization, and even, probably even more importantly, everybody uses some sort of risk ranking methodology. So is it a one, two, three, red, yellow, green? A high, medium, low, severe, critical, moderate, that kind of thing. That’s all gotta be defined and understood all the way down, you know, to the analyst’s level that’s doing risk analyst and assessment, to the people they’re communicating with to fix ‘em. But it also has to be understood up at the highest levels of the organization, and the problem that security folks, and *other* disciplines audit can run into, is if they’re not using a consistent, you know, a critical risk, when communicated to a server engineer, versus a critical risk at the Board level, are probably two entirely different things, because the scope that that server engineer has influence over, is *narrower*. Whereas the scope that the Board has is-, is broader and significantly more-, or much more significant. So a critical risk at the Board level might be something that has a dollar or human life value directly attributable to that risk. Whereas a server engineer might not have that perspective about a *patch* that hasn’t been applied to his server, which makes it vulnerable to a virus or something like that. That discussion would be fruitless with the Board of Directors or a Compliance Committee because they would start saying, ‘I don’t know-, tell me what’s gonna happen if this risk you’re talking about gets realized, if it gets exploited. You know, is it going to cause the organization to potentially not be able to do its mission anymore? They’re interested in *that*. They’re not necessarily interested in the, oh, you know, we might have a clinic slowdown for an hour and not be able to register patients or something like-, and they *might* be interested in that, but maybe less so. So that lexicon has to be, at least we used-, have gone through great efforts to make sure that that's consistent. So when we say 'critical' at the analyst and engineer level, it really is critical at this Board of Director's level because it all winds up getting reported across, and they're typically at the *highest* levels, and only wanna know about the severe, high and critical risks. Whereas, the cumulative effect of lots of moderate risks or low risks at the engineer level needs to be addressed, as well.

JF: But there *is* some possibility that at-, actually for the server engineer, if . . . if a risk is activated, that it could be, have significant financial impacts or even life-threatening impacts.

Subj: Absolutely.

JF: Are you sure your engineers are aware of that?

Subj: Absolutely. And this is a great example of the difference between the verticals. So you have that discussion a healthcare environment. Application and server engineering for I.T. in general will usually have as one of their key criteria, is this-, does a *change* that we're making, or a vulnerability that exists in the system, or a move or a downtime that's planned, does it pose any sort of likely risk to human health and safety, in the clinical care setting? When you go to Financial Services, that's not-, that's not typically a question I.T. has on their-, on their protocol, in change management because, you know, their thoughts are: Well, if it, you know, if our banking system or our wire transfer system is down for an hour, their question would be: What's the revenue impact to the organization? Which is very important to them, and it's important, you know, to us, as well, but more important would be the-, the question of . . . well, we don't wanna cause a death or an adverse outcome.

JF: What's your background and how did you end up in this role?

Subj: My background . . . so I was a . . . I majored in computer science in college, and then I spent a few years as [redacted]. And when I decided that I wanted to leave that line of work, I knew I wanted to go into Information Systems and Security, in particular. It was just a . . . it *suited* my personality and structure and kind of protocol oriented person. There are other disciplines that it would have made sense. It just was a . . . it was a good *match*. So I went into Security Engineering and Network Engineering, doing consulting work. And then I worked in the [redacted] for a few years, doing that and kind of moving into more of the management. And it was . . . risk management and . . . I.T. and Information Security Risk Management and I.T., itself, weren't really separated at that point in-, because of the size of the organization. But I was doing more of that kind of work, for the compliance and risk analysis work, as well, and I really *liked* doing that when I was consulting, as well. So I actively was looking to move into healthcare security, with the advent of HIPAA and everything because it affected us there, a little bit, but not nearly as much as it does at a-, at a-, at the provider level. So I moved, applied for a position, actually at OHSU, specifically for that reason, and because of the organization. I liked the . . . non-profit healthcare and the academic mission and all of that is much more appealing to me than the commercial, you know, profit-driven one that I was in . . . before. And then . . . so it was almost entirely involved in the governance and-, and compliance piece there, as I am here. And it suits me, I think, well from again, from a personality side. It's more consulting with I.T. and the-, and the clinical delivery side of the house.

JF: Did you have any formal training in Security?

Subj: So I did . . . the undergraduate education, there was certainly a little bit of it, as part-, as part of the curriculum. Much more so now, today, I mean, I look at the curriculum for a computer science undergrad today versus back then, and there's a lot more emphasis on it. I also went through a number of . . . some vendor and some non-vendor training courses for specific technologies and security around those, and then the Certified Information Systems Security Professional or CISSP certification, I studied for that and actually . . . earned that certification and then the company I was at, at the time, brought the training curriculum in and trained a whole like 30 people at the organization. I don't know how many of them actually went and sought the certification. But that was *after* I'd gone through the training. So . . . as far as formal . . . that's . . . I think that pretty much covers it.

JF: Yeah. Can you describe your day-to-day responsibilities?

[redacted]

[redacted]

Subj: [redacted] The number one thing for me is that that means at least one other person knows what our voice is on that topic, so that when the question gets asked again. . . . And then once it’s finalized, it goes up through-, it goes up through our [redacted], and gets . . . *published* and shared back with whoever it would be interested, stakeholders. And then it goes into our analytic library so that we’ve *got* it, it’s searchable. We can go back and answer the same question the same way, instead of the analysts [redacted], three months later, going their way and doing the same exact work, and coming up with a different or even the same answer. They can just go reference it. So . . . that's a *huge* part of my day, is managing our-, our-, we have a activity tracking system where we keep track of all of the analysis work that we're doing, and I make sure that we . . . know when one's gonna be done. If we have a backlog of things that people *want* an analyst to be working on, some of 'em we don't *do*, just because the potential risk isn't there. Or you know, we gotta prioritize everything. So that's a lot of the work I do is prioritizing that, and making sure that we're doing what we . . . what makes the most sense to do.

And then the other chunk of my time is spent going to or participating in a lot of meetings and initial discovery meetings on a topic that we're gonna need to do risk analysis on, and figuring out who the right analyst is to assign to that. That, so I do a lot of that tri-, that initial triage. Unfortunately, I-, I don't get to do a lot of the *analysis* anymore, but I'm not supposed to so . . . That's why we have the . . . the analysts. Though I do, still, occasionally.

JF: So your day-to-day activities are . . . would you say would be primarily management and oversight?

Subj: Yeah.

JF: I have to ask: Do you enjoy it?

Subj: I-, you know, I really *do*. The . . . it's a . . . it's not a technical job anymore. What I was doing ten years ago on the security engineering side, was figuring out a business problem and applying a technology solution to it. Now it's kind of translating from either the *solution*, translating what risks are present and what needs to be done about them, or taking a business solution and identifying those risks and telling technology how to solve them. And not always technology. There's a lot of *process* stuff and physical stuff that we do to address risks, as well. So it's *different,* and again, the more of the management and oversight stuff, the less I'm involved in the actual analysis. Sometimes that's frustrating but I do . . . I do still get to do enough and be involved in the peer review process, so I get to see-, and it's . . . in-, incredibly rewarding to . . . help people with security backgrounds or non-security backgrounds, get into this line of work and develop and kinda show them what's been successful, and-, and teach them that process along the way And we've got people in our department who've been at [redacted] for 30 years, who've done all manner of things and are now doing this work and really love the-, the process that we've got.

JF: What skills do you think are really necessary to-, for a Security Officer to have?

Subj: Communication is the-, *the* number one. The-, the people that I've worked with [redacted] who probably have the most challenges are the ones who just aren't effective at *general* interpersonal communication, and then communication, making communications relevant to the organization that they're at. You know, beating the fear, uncertainty and doubt drum, and saying, you know, 'The bad Romanian hackers are comin' to get us. We have to do *absolutely* everything. We're totally insecure.' Well, no-, you know, every organization is dealing with scarce resources. You've got to apply them at the best place, so you gotta be able to communicate that you *understand* the constraints, and *why* the specific risks that you want to address are the ones that should be addressed because they are significant and real to the organization.

The other . . . the other one, and this kinda depends on the organization's definition of that Security Officer *role,* is understanding the boundaries around what you . . . what you are accountable for and what you can *influence*, and there's a big difference. So not-, not trying to dictate things that really *should* belong to someone *else* as their domain. Not that we, you know, turf wars aren't-, aren't a *big* thing but you gotta be sensitive to the fact that if you're in a oversight governance and risk management role, you're not a I.T. Security Director. But again, some organizations expect the CISO to be *both* of those, and then as long as you're aware of that, you're OK.

JF: Let's take a-, a complementary role, that of a Privacy Officer.   What sort of skills do you think they should have?

Subj: So again, I think it's very defined by . . . how the organization defines that role. Communication still is *tops*, I think, number one. Most . . . well, in both of 'em I'm kind of . . . I'm kind of leaving unsaid they're at-, to me there's an implied-, they have to be-, they have to have-, be *experts* in that field. They have to have a full understanding of the security control requirements and compliance requirements, regulations, corporate culture and policy, and how that influences what is OK and what's not OK. And for privacy, that's certainly the same. I think there's maybe a little bit more of an expectation and-, and valid, that a Privacy Officer would have a deep understanding of . . . medical records management and requirements around that. Healthcare kind of uniquely has this separation between those. There's, you know, the Privacy Officer and there's a Security Officer at most places. If you go to Financial Services, there'd be a . . . Security Officer or whatever the title would be, and that's, I think that's almost entirely a function of HIPAA, creating a privacy rule and saying you have to have a designated privacy official and a security rule in saying you have to have a designated security official. Well, they *could* be the-, and often *are* the same person. But the backgrounds are often different. Your Privacy Officer will come from a medical records or healthcare delivery. You know, in the case of [redacted], when I was there it was a senior-, it was [redacted]. And the Security folks would ten to maybe come from the I.T. side or the-, or the network infrastructure side, or whatever.

So I-, I still think that the communication piece is number one, and in my experience, they've been very *similar* roles, often the same person [pause]. And the ability to collaborate between the two is huge. I mean, if your privacy and your security functions *can't* . . . *aren't* on the same page, it goes back to that lexicon and-, and the language and do we . . . are-, do we talk the same way and do we view risk the same way? We certainly *better*. Otherwise, at the Board of Director level and even at the, you know, at the analyst level, they look at that disconnected risk function and would throw their hands up and say, 'I'm getting conflicting guidance from people that, to me, seem the same. You know, what's the difference between privacy and security officer?'

JF: Can you give me an ex-, an example of an incident or two where your-, where communication was critical towards resolving the incident?

Subj: So I can give you two generalized incidents from across numerous organizations, both ones I've worked for and haven't.

JF: Yeah.

Subj: So a typical, classic security event would be a . . . malware, you know, virus infestation that gets discovered. Communication, and I can think of some big ones, communication was . . . *huge*-, hugely important because with a lot of those, as you discover an infected machine for example, it's the-, the time it takes you to get that machine remediated or isolated or whatever, you know, it's . . . it's like quarantined, the faster you can identify it. I . . . one of the things I love about working in healthcare is all of the analogies that we can draw on, like health surveillance and, 'Hey, guys, we're-, you know, we're working in an environment that has been-, and-, and, you know, you work in healthcare informatics. I've consistently gone with the wealth of data that I.T. gathers on system health and performance, and management and that kinda things, and . . . and they try to use business analytics tools, and I say, 'You know, we've also got this entire discipline inside the organization that does this same kind of work with health information. You know, disease monitoring and management and all of them, and I'm like, 'They're good, smart people around *data*. If you boil everything down, it's just, you know, information. And you're looking for patterns and trends and statistical variance and *all* of that.' So back to your original question, the communication around that was the timeliness was-, was what was most important and making sure that you've got the right list of people you know who would-, you know who you need to contact when you need to contact them. And usually what happens in organizations, is the first time that happens, you discover you *don't* have the-, those call trees and that kind of stuff. You can't triage quickly and you-, there an opportunity *lost* for quickly isolating, and all of a sudden you've got a much bigger problem than you would have otherwise. So usually that becomes a inflection point in the maturity of your incident management, and you say, 'We were horrible.' You focus a lot of effort, you get better, and then if you either exercise that capability or . . . or *don't* exercise it, but actually experience *real* incidents, again, it *stays* somewhat good. If you *don't* it goes back down to where it was, and then you have another inflection point and you get better, and then you have a, you know, a long quiet period and then it goes again, and you wind up at this horrible peak and value syndrome.

The other type of incident is pretty common in healthcare is the if a device gets lost or stolen. That may or may not have confidential information on it and now with all of the privacy protection laws, increasingly, there's not even a risk attached. There's a: Did it have something on it or not? Not true in all cases, but in-, in some states now it's we don't care. It's, you know, it's reportable, it's a breach of what . . . Typically, we'll still do the analysis of: What's the risk to the patient or the consumer? Is it-, can this information conceivably be misused? How difficult would it be to *get* to? But the communication for *us* is critical there because, for instance, if a laptop gets stolen, we have a very narrow window of time where we can actually try to execute a remote wipe of the system so if it gets on the Internet it checks in with a server and it can be told to wipe all the data off of it. Now, that's a-, that's an additional control on top of the encryption that's there, but we'd still like to have that be successful, and say, 'Look, it was encrypted, and it got wiped, you know, six hours after it was stolen.' So we've got safe harbor and we don't-, the-, the risk really is miniscule at that point. But if we don't, if the person that lost it doesn't communicate it to the operation center for a *week*, you know, who knows where that thing is at that point. It's been parted out and sold for repair parts or . . .

JF: Doesn't the fact that it's en-, encrypted give you that safe harbor?

Subj: It *does* and that's if we can-, if we're comfortable that the encryption was effective at the time it was lost or stolen, and there are things that can be done, like if it's left in a hibernated state, the encryption is a hundred percent effective. So we'd still have to look at-, then we'd have to ask the question: What data was on it? And that's a difficult question for many organizations to answer, particularly with laptops, unless you're doing some extensive logging of what information is going to and from that system. So it's easier for most organizations to just say, ‘It was encrypted. That was effective, oh, and it got wiped so . . . ‘ We like to have both available.

JF: What sort of skills do you see as becoming critical in the near future?

Subj: One of the things that we’ve . . . been focusing on a lot in the last year is . . . well, two I would say are gonna be really important, particularly for Security Officers and Senior level security analysts. Emerging threats, so not paying attention to the emerging threat landscape is gonna be a huge problem for some people who like to-, who-, who are consistently looking at bug track and things like, ‘Oh, what’s been discovered and what patches are we missing?’ That’s good but that’s a little bit reactive. You know, the trend towards-, and it’s not *new*, but towards socially engineered attacks. I mean, that’s been around for . . . that’s . . . that’s how it’s been done for *centuries* so . . . that’s *evolving* and there are different mechanisms and ways.

Subj: The other one is integration with-, with the Enterprise risks. So not keeping security risk isolated and privacy risk isolated and physical security risk isolated and kind of blending all of it into one program so that we know that . . . *revenue* risk and security risk can be set together in front of decision-makers in terms of prioritizing. No, this is, you know, the fact that-, that we’ve got single points of failure in our-, in our, you know, oh, we just use an Epic organization. If that system comes down it’s hugely disruptive to every, you know, silo within the organization, from care to billing to registration. And that’s somethin’ that once you're on a centralized, you know medical records system, and everybody's forgotten how to do things manually and by paper, it can become a *huge* problem. So speaking at the Enterprise risk level, it's another huge one that I think security officers are gonna have to be comfortable talking with chief legal counsel, you know, claims and administration, clinical quality, they all need to be exposed to each other, even though it's, you know, it can sometimes be intimidating for-, for people coming out of an I.T. side, all of a sudden sitting next to the Senior Attorney at an organization and the-, and the CEO, who are having a discussion. But they've got to be comfortable in that area.

JF: Good. So that brings up: If you had a new member who was becoming, who was joining your organization, what skills would you like to have-, would you like *them* to have when they came into the organization?

Subj: So . . . a *timely* question. So we just have a new hire [redacted] who works for me at our-, our headquarters, who I was just up there with last week and then again yesterday. And we were going over his 100 day plan for assimilation or-, or getting comfortable [redacted], and again, we are a . . . like pretty much every organization I've ever been at, we're a very social organization, so his 100-day plan is almost entirely taken up with meeting with the people that he's going to be doing work for and *with*, getting familiar with them, understanding the work that *they* do,. What-, 'cuz he did-, and he's coming from a non-security and non-healthcare background, and it was *intentional*. I mean, we hired him specifically, because I said, 'You know what? It's healthy. He's got great customer service background and that's where everything was oriented in the interview process. So that's where his 100 days are, and at the same time, he's currently finishing up [redacted], which again, thinking back to my back-, that didn't even *exist* when I was in college. And not that that's the be-all, end-all. You know, a formal-, formal education isn't everything but . . . so he's getting a lot out of there and I'm also putting him on some specific . . . assessments, working with one of our senior analysts, to kind of get the ropes.

We have a formal training program for-, for the analysts, as well, that shows them our entire tool set, how we do things. Here-, here's what an assessment report should look like, here's how you track your work, here's our lexicon and here's what it means. So getting comfortable with that and he's a lot different from somebody who's-, we would hire who'd come from an audit background or from security at another organization, who would have, you know, potentially some good and bad . . . stuff they'd be bringing with them, compared to how we think we should be doing it.

So I-, I mean, I hate to harp on it, but I would go back to it's that communication capability. 'Cuz an-, a security analyst, that's *all* they *do*. I mean, they-, all they do is communicate and-, and analyze the data that they get from those communications. And then communicate it back out, you know, recommendations. So if they're not effective at that, I don't care . . . how good their analysis is, then they're unable to take-, carry that message forward and get anything done on it. I guess, if you had a big enough organization, you know, there are analysts that can be buried in the basement, turning through numbers and data, and coming up with the, you know, statistical validity tests and all of that, but . . . that's really not the organization we've got.

JF: In many ways it makes the next question I have-, had on my list here almost irrelevant because it's the question says: How do you keep up? How do you keep up your-, your skills and skills inside your organization on technology? But it seems like you have another skill you really find more important.

Subj: So we do need to-, actually, the way that-, that an analyst stays up on relevant technology is as part of a specific assessment or analysis that they're doing . . . if they don't know it, they have to go out and learn it. So if we-, a lot of the day-to-day work that analyst does is when a new vendor solution or a new technology solution or a *change* is-, is being considered, they have to go out and look at the impact of that change to security, of that system or process and systems or processes that it *touches*. So if they don't understand . . . I'll take Pyxis, so if we were to throw out Pyxis and throw in a new solution for it, they'd have to go out and understand, OK, first of all, what does this thing *do*? You know, in-, in the first place? I don't understand this pharmacy management system and med dispensing system. They'd have to go *learn* that. They'd have to go learn the-, the regulatory impact of that, and-, and the operational impact of that, and go through a checklist that we've got for technology solutions. That answers: Does it do the follow-, does it support individual, unique user identification and authentication? Does it-, can it enforce strong passwords? Does it have patch program? Is it running commercially available and secure sys-, you know, operating system. All . . . it's a long checklist but it goes through those that they would go through with the vendor. So they typically learn that, the technology side of the house through an assessment that they'd be doing. More generalized security and risk knowledge, professional development and ongoing education is something a lot of them get through going to conferences. But we do all hands, where we cover, you know, somebody will give a presentation on a specific *topic* that they've studied or they've gone and learned about somewhere.

JF: Thank you. What skills would *you* like to acquire?

Subj: Boy, that's a good question. I think I . . . When I was at-, [redacted] I was doing kind of a back and forth with-, with the Privacy Officer on getting much more up to speed on privacy stuff, that when I left, that took a little bit of a . . . 'cuz I was . . . going to be the [redacted] there, as well because it was a smaller shop and we basically had to be able to answer both questions, the privacy and the security side. Again, like there's some weird line between the two. I kinda got out of that once I got here because we have a very defined privacy group, and-, and privacy officers in each region . . . who get to handle that, so I just know when to pitch it off. So I don't answer it as much anymore, so I probably would try to get back up to speed, but not that I'm out of speed. It's just I don't wanna answer questions that I'm not the one to answer. So that.

And then the enterprise risk side, I think, more exposure on . . . things beyond security risks. And we've been doing-, my boss is actually running the [redacted] Program now. So bringing in all of the risk stakeholders from everywhere. So I think I'm gonna *get* that, and I-, I wanna get that when we get more ver-, well-versed in enterprise risk.

JF: What sort of-, what questions didn't I ask?

Subj: What didn't you ask? [pause]

JF: And if you feel like we've . . .

Subj: It was very positive, I mean, all the questions were very-, they're, it's refreshing 'cuz I'm a security guy so everything is always negative. It's always the: Tell me what the problem is and how *bad* is it and this was all, you know, what are the *good* things? So I guess you didn't- I guess I didn't get-, there wasn't an ask about what is the, you know, what are the biggest risks? I'm so used to being asked *that* kind of question. What's the number one problem in Healthcare Information Security? Though I don't-, now that I'm telling you that, I'm like, I don't know that I have a really good answer . . .

JF: [laughs]

Subj: . . . for what the *top* risk is [pause] And you asked about organizations. You know, and I didn't-, I didn't talk about . . . though I probably could have on one of the questions, professional associations and peer . . . I wanna say peer credibility but, you know, the community standard concept in Information

Security or in Healthcare Information Security, because that's always been . . . you know, in Healthcare everybody wants to know: Well, what's, you know, what is the *best* protocol? What are our peers doing? And that's an interesting . . . that's an interesting concept for a group that does risk analysis *internally* and comes up with what they think is right. And then if you look at what other people are doing, sometimes it doesn't match up.

JF: Do you have other organizations that you *do* work with/

Subj: Yeah, actually everywhere I've-, particularly in healthcare, when I was at OHSU, we did a lot of work . . . so I-, I talked with a lot of peers at academic medical centers – Hopkins, Duke, Georgetown, University of Washington and Stanford and we would talk about topics and then a little bit of apples to oranges, right? 'Cuz the sizes of some of these organizations are so different. And then there was actually a formal organization called the . . . University Healthcare Consortium, or UHC, and we had a formal security working group . . . security and privacy working group, where we talked about-, we actually *established* a non-binding, you know, community standard. In UHC *terms*, this is what your audit log review program of your information systems should look like, and then it had kind of a: Here's minimum, here's your better and here's the-, you're the platinum standard. That was a great exercise to go through and it was very academic. I mean, you can, that's exactly the kind of thing that the university world would *do*.

Where I am *now*, there is a . . . there are a couple different organizations HIMSS, AHIMA, OrHIMA in Oregon, the Association of Hospitals and Health Systems. They all have different security and privacy working groups that are valuable in different ways. And then the Catholic Healthcare Association, which is, as you can imagine, an association of all of the non-profit Catholic Healthcare Organizations. It does similar stuff. And . . . relevant and the-, the relevance of different ones is different, so if you're talking about something that's related to our culture or the mission in what we're doing, Catholic Healthcare Association is probably better. If you're talking about, 'Hey, I need to look at another, you know, [redacted]hospital system [redacted] how *they* address this problem . . . ' Well, we only have two of those peers maybe in CHA, but if we to go to HIMSS, we can certainly talk to a lot more people like that. So that's a good-when I-, when you asked about how do you keep *current* on security, that's one of the big ways, is by networking with those people, and reading the articles that they write.

And then on the question I gave you about the, you know, *top* security risk, I mean, I could go to our . . . I could go to our [redacted]reporting and tell you which we're currently saying is the biggest one.

JF: But to be honest, I'm more-, more-, interested instead of the actual risk, of how people are prepared to *deal* with those risks.

Subj: I-, I think rate of *change* is probably the-, the biggest one, and I mean, it doesn't just affect the security folks. This is I.T. I mean, everybody that works in healthcare, stuff changes so fast, and the incentive to *move* . . . Yeah, you kidding me? The portable devices? And I think the-, the biggest-, one of the biggest risks is if you-, if you're *not* agile enough as a security, or an I.T., or as a business organization, to *adapt* to that reality . . . you're-, you're . . . gonna just get bypassed. You're gonna be irrelevant and there's gonna be no review or control. Even if it's not the *best* from your security perspective? Better is better than nothing. Or good is better than nothing and that's the problem. If you're too *slow*, you-, you pointed to the, you know, personally owned devices? I'm . . . we're *huge* proponents of it. I mean, if I could get everybody to *not* be using [redacted]-owned laptops anymore, and just be using iPads for, you know, 90 percent of the workforce, but not-, but giving them the ability to not have the data *sitting* on there, so they didn't pose *that* risk. Are you kidding? Our desktop support folks would be in heaven, too, 'cuz they wouldn't have to be managing all these things, *uniquely* for each person that had their own need.

And the other-, another big one is if you're-, if the I.T. and the Security folks, and-, and budgeting are not agile enough to provide a solution to a department, for example? They'll just go out and *find it*. And they'll pay for it however they want, and you'll never *see* it. You know, it'll all be cloud-based solutions and they're out there, and they come in and we sometimes find out about 'em *after* the fact, or kind of late in the process, and we say, 'Well, you know, we'd really love to be . . . ‘ Again, not saying they’re not *good* solutions. They just have to be done in the right way.

JF: That’s been scary, to discover something that’s implemented without review.

Subj: Thankfully, most of ‘em are . . . we’ve got a big enough staff that’s engaged in enough with the departments that most of those are things that *were*-, we’re gonna pose a problem anyway ‘cuz the data that’s involved with the business process it involved isn’t-, isn’t a confidential thing. It’d be-, I’d be very surprised, for example, if a . . . you know, a radiology department came and said, ‘Hey, by the way, we just outsourced our, you know, image-viewing technology to this, you know, *cloud* provider and didn’t think to involve anybody.’ And hopefully, the contracting process would catch that, as well.

END OF RECORDING

Interview 4

JF: So, today is noon on March 2nd, I am Justin Fletcher and I am talking with –

Subj: [redacted].

JF: And your title is?

Subj: I am the [redacted] and I am also the designated privacy official.

JF: Thank you and we are actually interviewing today at a [redacted] office. Is it, are you interested in participating in the study?

Subj: I am.

JF: And is it alright to continue to record?

Subj: Yes it is.

JF: Great, thank you very much. So, would you mind repeating your title and telling me the role inside [redacted].

Subj: Sure, so ah, my primary role is the [redacted] which has um, some basic pillars, one of which is HIPAA privacy and security. Ah, and HIPAA privacy and security is the um, the godfather of regulations that healthcare entities or what we call covered entities ah, must follow to safeguard protected health information. Um, and there ah is another person that I work very closely with who is in our IT department who is our designated security official because HIPAA has two components; it has a privacy component and it has a security component. It has two separate roles, a privacy role and a security role and I can speak, ah, to privacy pretty in depth, um, and to security I know enough to be dangerous um, but would be happy to give you contact information for our security official if you want to interview him at a later date.

JF: Thank you, I appreciate that.

Subj: Um, so my role is essentially to uh, ensure that the organization is following the seven elements of a compliance program as defined by the Office of the Inspector General uh, and they have guidance that is specific to healthcare, uh, that uh basically states that although voluntary, their expectation with healthcare entities is that because they are contractors receiving Medicare and Medicaid dollars from the U.S. Government, that they have to maintain the utmost integrity through various compliance recommendations which include things like uh, making sure that you have an infrastructure that supports compliance so a compliance officer, a compliance committee and those are items that I staff, um, making sure that you conduct risk assessments which is what my department does, making sure that you have an ability for people to report, ah, which my folks staff as well. We have hotlines that the organization provides both internally and externally for folks to report things and then making sure that we are following other various recommendations such as, um, not employing or doing business with people who are considered excluded from contracts with uh, the government, uh, making sure that we have robust followup when things are reported, and making sure that we are addressing issues when they are brought to our attention. Um, and then the final piece of that is um, making sure that we provide a sufficient amount of education for folks regarding compliance. So that is in a nutshell what we do, um, and it's about 40% reactionary with people calling in and saying, I am not sure what to do with this situation or, my (inaudible) list serve is telling us there is a new state law or there is this going on or that going on and we would like your assessment on whether or not it is compliant so about 40% of what we do is that. The other 60% of what we do is actually process related, ah, one of which is um, centralizing all of the audits for potential privacy and security violations, so we may get a call from a manager that says, you know, I have an employee who I think might be snooping in medical records where they shouldn't be snooping, can you audit, um, audit them and see what they have been looking at? My staff will do that with the help of our IT department and then we will work with the manager to determine if there is actually any, um, anything going on. Um, we also do proactive audits where we may have a high-profile patient come in and we will audit their account retrospectively to make sure that everyone that was in the records should have appropriately been in the record, um, and then we will respond to outside regulators. You know, as large as we are, it is not uncommon for us to get uh, you know, uh patient complaints. The avenue for a patient to complain about privacy and security is through the Office of Civil Rights. Their regional office is in Seattle and we have a very good working relationship with that office where if they field a complaint, they will contact us and we will conduct an investigation and provide them with details on the outcome of our investigation. Sometimes it is a slam dunk, it was a misunderstanding, or it was a miscommunication and is easily resolved, other times we have to go into more depth, but um, to the, as long as I have been on board, we haven't had any significant findings. So, that's what we do.

JF: It sounds like it keeps you busy.

Subj: It is very busy, it is very busy and I have an analyst that is my education expert and she spends, you know, probably half of her time just conducting education.

JF: What's your background and how did you end up doing what you do?

Subj: (Laughing) So, this is an interesting story. [redacted] and it has just been an amazing fit.

JF: How did you learn the responsibilities for the role?

Subj: Ah, project by project. So, I think that for ah this position, what I typically see with my peers are people who um, are very analytical as far as their ability to um, read and digest very complex topics and more specifically state and federal law.

A lot of my peers are attorneys, um or have some kind of advanced degree in public policy, uh, and uh they have a very strong working knowledge of Medicare billing rules as well as privacy and security rules which are again, really the pillars of what we do. Um, I think those of us that are successful have very strong facilitation skills because it is very common where we have a compliance issue that touches several different departments and our role is to come in and bring everyone to the table and determine how we are going to comply. Um, or if we have a mess on our hands to determine how we are going to get through that, overcome it, and make improvements, especially if there is, you know, some drama with the parties involved. Um, for me, I think the importance of having that technical knowledge is also the ability to build culture in an organization where people are not afraid to report. Um, I think that what you will find with compliance professionals and with HIPAA privacy and security officials is, you know, two different possibilities. You will find the law enforcer which is really um, all about coming in and telling you what you are doing wrong and trying to scare the bejesus out of you and so they use more of a fear tactic to get their way or you will find the collaborator and they are uh, the technical expertise but um, they also have an inability to build a relationship in the operations world so that when people do have things going wrong, they are more inclined to call you and ask for your assistance, um instead of being afraid to tell you because they are worried about getting in trouble. My motto is you catch more flies with honey and so I totally embrace a more collaborative model and I am highly critical of my peers who use the law enforcement model and quite frankly I don't hire staff that use the law enforcement model. It is all about what value we can add when we come to the table. So, an organization this big, we don't have enough people to even embrace a law enforcement mode if that was the personality I had. I need people coming to me. So, but as far as you know the skills that people need, uh, you know, it really is project by project because healthcare is constantly changing, you know with all of the healthcare reform, you really just need an ability to read the Federal Register line by line and ah, and figure out how that applies to your current environment. You need to know how to conduct a risk assessment. You need to, uh, have some tribal knowledge of other laws because often times things are intersecting and a perfect example of that is um, all of the health reform going on where we are looking at, um, medical um, medical homes or uh, coordinating care where you know, the government really wants hospitals and providers and um, government agencies to come together to take care of the patient to make them better. Um, well everyone is used to sitting in their own camp and safeguarding their own medical records for patients; in order for us to collaborate we have to open everything up and a lot of times that contradicts with what privacy and security laws tell us to do.

JF: Okay. I know you have covered a lot of items that you do. What would you say you do on an um, day-to-day basis? What are your day-to-day responsibilities?

Subj: Sure, so a portion of the day is spent on e-mail and on the phone, uh, you know, reacting to people reaching out to me and asking questions. Another portion of the day is spent in meetings where I am typically sitting on some kind of a project or helping to facilitate some kind of an issue so that we can um, either beef up our compliance or come into compliance with something we may be struggling with. Um, I do spend a portion of my day on education as well. Um, [redacted] we have new employee orientation and I staff a portion of those where I actually go and present myself. And then I have standing committee where I have multi-disciplinary teams sitting around the table vetting issues that are directed to come through us through various processes. An example of that is I have a HIPAA (inaudible) committee [redacted] and our primary role is to sit there and answer questions um, in regards to folks who may want access to medical records that isn't typical to how we provide access. So, we sit there and we look at those issues and we figure them out.

JF: Do you enjoy what you do?

Subj: Love it, absolutely love it. It was the best change I have ever made. So it is like a big puzzle for me and so it's very, and I get to, I get to work with the whole system, I am not pigeon-holed into one clinic or um, a finance department or um, one particular area. I get to work with the whole system and I just love that.

JF: How would you describe the structure of your organization?

Subj: Uh, as far as compliance and privacy and security concerns?

JF: Well actually, what sort of teams do you have working for (inaudible) have working for and who do you work for?

Subj: [redacted]

JF: As a privacy officer, what skills do you think are important for a privacy officer?

Subj: Um, I think that the skills that are important are well, that is hard to define. I can you tell what skills I need to do my job. I need to understand the law that I represent so I need to understand HIPAA privacy in and out so the skill that I need there is the ability to read the laws and to read the updates and to understand how they apply to us. Um, I definitely need the skill to work with people um, and not just internal people but external people. It could be as simple as educating a line person on how to appropriately talk about patient information, you know, don't do it in the elevator, don't do it in the cafeteria. You know, make sure you are definitely not doing anything on Facebook or anything like that, you know, some of the obvious stuff. But it could be as elevated as, you know, talking to a very irritate patient and then even more so, there is this delicate balance on how to communicate with regulators. So, being able to behave in a transparent manner but at the same time not letting them walk all over you when some of their demands seem cumbersome or you know, inefficient. So, uh, I think you need a lot of people skills, um but I also think that you need to have a technical side to you, some attention to detail because there is a lot of reading and I think that folks that have um, I am envious of folks that have gone to law school, although I think those of us that have gone to graduate school, um benefited as well. Um, you know, there is a lot of research skills that you gain from those advanced degrees that I truly believe is a requirement to do some of the work that I do. I would not have, it would have been more challenging if I hadn't had that technical training and graduate school and I know the same to be true with some of the attorneys I work with. They say that the legal training they received in school was just, you know, knowing how to look up laws and regulations, can be very cumbersome, so.

JF: Of these skills, which are the most crucial?

Subj: The most crucial skills, if you are going to hit the ground running then you know, being a subject matter expert on whatever law you are going to be representing so for a privacy or security official, you know, an in and out understanding of the HIPAA privacy and security rules.

JF: Let's take your counterpart, since you are mostly working with the security officer, what do you think are the most important skills for security?

Subj: Um, security, I would say, you have to be very much of an IT person, a technical person, and know the ins and outs of the physical safeguards and the technical safeguards required to protect information. I mean, I lean on Joe a lot. What may seem easy to me, um you know, I will use password protection as an example, may not be such as an easy thing logistically when you have multiple systems. Um being able to have multiple systems, um the whole electronic medical record implementation we just went through. You know, understanding the ins and outs of technically how that works. I mean, I can say I expect this to work this way and say for example, here's a good example, when we built access for folks for our electronic medical record, one of the things that we safeguarded very well was social security numbers for patients. And so, when we built what we call profiles for folks, so a nurse would have a certain type profile, an admitter would have a certain kind of profile, a biller would have another kind of profile, those profiles would have parameters built in as far as what kinds of information they could view for a patient. And we kept the profiles very generic because we didn't want to have hundredss of profiles that we would constantly have to manage because that becomes a logistical nightmare. What we found is there are these special pockets of folks that needed access to a social security number to do the basics of their job. Um, we didn't consider that when we initially built our profiles and so now, we have folks that need access to social security numbers but because we have massive populations in these profiles, if we were to turn it on for one person, we would be turning it on for the entire population and that's not what we want to do, it defeats the purpose, you know. My thought was, oh, but we would just be able to add a la carte to people who need social security number access to their profile. [redacted] was able to research and say no, that's not how it works. So I wouldn't have had any kind of knowledge of his whole profile set up or the logistics that go behind being able to provide that kind of access without his expertise. You know, what we know is that he is able to go back and advocate with developers and say, we need the ability to add certain things a la carte to different profiles without changing it for the masses and that's where he comes in to play to help have these conversations.

JF: Which of his skills is the most important to you when you work with him?

Subj: Um, his technical understanding of the systems.

JF: Do you have example incidents that you could describe where your skills have been, have been used?

Subj: Incidents as in privacy and security incidents? You know, I probably couldn't go into a lot of detail being recorded about certain incidents but I can tell you that the skills that we have um, that are very important when we have an incident um, is being able to communicate with the patient, being able to communicate with the regulator and being prepared to respond to any kind of um, PR-type inquiry. So, um, for me, it is really about making sure I have all the players on the table and making sure that they are aware of the details of what has happened.

JF: Okay. How often do you have to exercise that?

Subj: Um, hopefully not very often. I mean, I have a rapid response team that whenever we have an incident that has potential, I gather them and I get everyone in the know so there are no surprises, but my team will concurrently conduct an investigation to ensure that we have all the facts before we pull the trigger on anything.

JF: Mm-hmm.

Subj: I mean we have mandatory reporting laws that we have to abide by and we have certain timelines to report to patients and report to the government if we have a massive breach so, and those are all through HIPAA and another regulation called HITECH that went into effect in 2009.

JF: What skills do you see as becoming critical in the near future?

Subj: Um, I think the skills again are the ability to analyze and comprehend where the, you know, the ACO/CCO environment, this whole you know, care model that came out of the Obama administration to bring providers and hospitals uh, and billers and uh, the government all together to create these models where we are all working together to take care of the patient. Uh, you know I think the skills needed there is the ability to negotiate. I think advocacy is huge. Understanding where our various laws are going to you know, collide. Um, there is a task force that we sit in being all networked and knowing who to call whether it is through the hospital association or you know, my peer through OHSU to you know, help get them on board to advocate.

JF: What skills would you like to see in a potential new staff member?

Subj: Um, for a new staff member, I think the skills that I am always looking for is analytical skills and an attention to detail. Um, obviously honesty and integrity, I think that is just absolutely paramount, I mean that we are in the business of um, figuring out what we did wrong, or figuring it out how we can do it so we don't do it wrong and you know, there quite frankly, isn't any room for ego. I mean we all have to be able to sit down and say these are the issues in a non-blaming way and um, I will always ask in my interview questions, you know, tell me about something that didn't go wrong and how you responded or tell me about an incident that was your fault and you know, I look for people's grace and ability to eat crow. We have to do that and I think that by being able to demonstrate that again, it creates that culture of reporting. People can't be afraid to report. Um, so I look for examples of you know, that humility and that grace and that collaborative attitude, I think that's huge. I can teach anyone who has any kind of you know, an analytical intelligence how to read a law, and quite frankly it is constantly changing. So, even if we have a law that came out in 2009, that doesn't mean it is not going to change in the next election year. So, we have the um, quite frankly we have a very robust legal department so I can lean legal support anytime I need to if I have issues interpreting but, I am looking for people who are willing to, I am looking for project managers too. I think that building a project/manage a project is huge. So the organizational skills, the being analytical, being a collaborator and then of course if they have any kind of background or technical expertise in our primary laws which is really our compliance guidelines and HIPAA um, anything related to privacy and security is huge.

JF: What skills would you like to acquire?

Subj: Um, you know, I'm at a point in my career where, uh, I am doing less and less of the heavy lifting and more and more of you know, triaging of projects. I really am starting to enjoy a lot of the advocacy work and so being able to move more into those leadership roles and those visionary roles is where I really look forward to. But, you know, [redacted] that's uh, a great place to be, especially with all this change because we can get it, you know, my concept of being able to set it up right from the get-go so we are not so far above the project, you know 10,000 feet, that we have no control, we are just conveying the vision, but we are not so far in the trenches that we can't get anything done because we are busy in the weeds. Um, you know as far as, I have no desire to go back to school so I don't think there is any kind of educational needs there. For me at this point, you know, my growth comes from, you know, the variety in the projects and we have a lot of those.

JF: Great, thank you. What didn't I ask?

Subj: I think we covered it.

JF: Great, I am happy to hear that.

Subj: (Laughing).

END OF RECORDING

Interview 5

JF: So, today is Friday, April 20, and at about little after 3:00 in the afternoon. I am Justin Fletcher from Oregon Health and Science University, and I'm speaking with --

Subj: [redacted]

JF: Thank you. And we're actually interviewing [redacted] – are you interesting in participating in this study?

Subj: Sure.

JF: And is it all right to record?

Subj: Sure.

JF: Good, thank you. Thank you very much. So, let's just start with the questions as we work through it.

Subj: That's fine.

JF: Can you give me your title and your role inside your organization?

Subj: My title is [redacted] And to that end, I am responsible for maintaining and implementing and maintaining process and structure within which we maintain our compliance with various healthcare regulations, mostly around billing, coding regulations and – and the three big laws that we pay attention to in the compliance world, the anti-kickback statute, STARK, and the False Claims Act. [redacted]

JF: In other words, you have a lot of responsibilities across a lot of areas.

Subj: It's – yeah, it's spread fairly thinly. Yeah, yeah. Yeah, so, I think that pretty much covers it, and I – you probably don't need me to talk about my job duties as privacy officer, I would expect.

JF: Actually, it's going to be the privacy officer I'll be most interested in.

Subj: Right.

JF: So, it's going to sound like an odd question but do you enjoy what you do?

Subj: Yes and no.

JF: Okay. Are you willing to elaborate?

Subj: There – there are I think, as – as anybody would have a certain – with their job, there are certain aspects that I – that I truly enjoy. And some of those actually surprised me. I actually enjoy investigating or researching laws and regulations, and – and making sure that we are doing the right thing. There are the political aspects and I’m not talking about national or – or state or – or, you know, political-political kinds of things but there are, you know, internal political aspects that are – are less enjoyable. And – and there are some constraints that are placed on me that – that make it difficult to do a good job. And that – that makes my job less satisfying.

JF: Okay. Can you describe your background and how it led to this current role?

Subj: [redacted]

[redacted]

JF: Did you receive any specific training for these responsibilities?

Subj: [redacted]

JF: What would you describe as your day-to-day responsibilities?

Subj: Wow, let's see. Day-to-day responsibilities include ongoing maintenance and updates of our various online resources for compliance and for HIPAA compliance as well. We have quite a wide variety of online resources to support our – our caregivers, our employees in the field. Boy, let's see. Handling breaches of confidentiality, I – that's the stuff that comes to mind on the privacy side of things, also oh, we're constantly updating our – our training offers. We have internal training for privacy and security in other things. So, I’m always working on that kind of stuff. I'll just take a look at my to-do list here and see what other kinds of things. I would say also keeping an eye on – on – in the privacy world on national discussions on privacy and so forth, and seeing whether we need to adjust our own policies, that kind of thing. So, I’m involved in regular review and revisions of our – the various policies around privacy and security as well. I also work with about probably a half a dozen different committees that are specific to compliance, just kind of different flavors of compliance, if you will, or different aspects. I work with a lab compliance committee. I work with an endovascular compliance committee. I work with a regional compliance committee that is more generalized. I work with a couple of different committees that are devoted to privacy and security and breaches, that kind of thing. There's three of those actually. And yeah, I think that pretty much sums it up.

JF: How would you describe your organizational structure for privacy and security?

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

JF: How do you identify a breach or potential breach?

Subj: Well, in large part, we look at – we look to co-workers that tattle on each other, people who report breaches. But we also – I think that probably the vast majority of the breaches that we process are inappropriate access to our information systems and we police those systems pretty thoroughly. And we look for certain types of things that end up being red flags. You know, for example, one that just comes to mind is if the person accessing a particular patient's record has the same last name as the patient, that's an automatic red flag, and we'll look into that for other – if they're any relation, then we process that as a breach incident and so forth. So, those are the main ways that we become aware of breach or potential breaches.

JF: Okay. What skills do you see as being required by a privacy officer?

Subj: Critical thinking tops the list. I think the ability to read and interpret regulatory language and legal language. You know, I should have gone into law in retrospect but, you know, I’m way too old to do that now. The ability to, you know, think and act independently as well. What else? Well, and – and then there's the opposite of that. There is the ability to work collaboratively. I – I think a – a privacy officer is most successful if they are able to integrate themselves into the day-to-day operations of the organization. That's a very tough challenge. Certainly, in my experience and in talking with other privacy officers that I know, we're often seen as the police, as outsiders, and not necessarily welcome. And I’ve been doing this work, you know, since the – from the beginning before, you know, the HIPAA privacy regulations were final. And it's really only within the last two or three years that I feel like I’m really starting to make inroads with our operations folks. Other skills, certainly communication and that probably should have been at the top of the list. You got to be a good communicator and I won't say that I’m that great. You have to be patient and I’m certainly not that great at that either. But communication skills and being able to collaborate and – and some critical thinking. I think one can look at the regulations and – and while there's always room for interpretation in the years since HIPAA has been in existence, the interpretations are becoming fewer and narrower. People are honing in on really what it means and how to work it. But I think discussions or disagreements on what a particular part of the regulations really means or intends are becoming fewer and fewer. So, we're getting down to where it's becoming more and more black and white. And to be honest with you, Justin, I have no idea where I was going with that thought train. So, I think we'll just have to let it off the air. Where was I going? I'm sure I'll remember two or three questions down the road.

JF: Okay, and we can always come back to it.

Subj: Okay. I have no idea where I was going with that.

JF: Let's take your compatriots as a security officer. What skills do you think are really required for a security officer?

Subj: Oh, man, that's a tough one because it's not really my world. Even though I worked in user security for our, you know, our EHR system [redacted] I learned everything I needed to know on the job for a great extent, you know, and but so I don't really know on a day-to-day basis what our technical security person does. But one would think that the skills would be kind of similar, that, you know, certainly you got to know a lot of the technical stuff. You know, you got to know what our IT folks are talking about when they're – when they're raising concerns and so forth. But you also have to be a good communicator. You have to be a good critical thinker. That's where I was going, critical thinking. So – so I'm going to go back to that for a second while I've got it fresh in my mind. So, you look at, you know, I mean there – you look at how people are interpreting a given say rule and – and the critical thinking comes in well, how does that really apply to us in this situation in our organization. And – and – and if we don't comply, what's the risk; what's the risk to us as an organization; what's the risk to the patient, and really, the patient comes first; what's best for the patient. So, in my critical thinking, I'm always considering what's in the best interest of the patient and what's in the best interest of the organization as I am attempting to apply the rules. And so, that ends up perhaps being some inconsistent application from time to time. I hope that makes sense. So, in so far as the technical security person and their skills, back to that, sorry to jump around but critical thinking and so, you know, how does one apply the – the -- kind of the industry-wide technical standards, security standards in our situation with our culture, our people, and – and what's in the best interest of everybody involved. And with our organization, our IT technical security person needs to be extremely patient. That's about all I can come up with right now.

JF: Sounds great. Can you describe some example incidents where these skills were applied?

Subj: You know, for some reason, I seem to be stuck on critical thinking for a moment but so, with trying to codify how we comply with – with HIPAA regulations in our policies, and – and try to put those policies into everyday language as much as possible. There's only so much possible. And sometimes we end up with some policy statements that while they are technically in compliance with the law and with regulations, and – and consistent with our over-arching policy philosophy, if you will, a given policy provision standing alone may make not – may not make a lot of sense. And in fact, it may be something we don't want to communicate widely to people so there's some critical thinking involved in – in how we apply our policies as well as how we apply the regulations and so forth. And I think in when I described in critical thinking, I described, you know, how that gets applied as well, you know, I think earlier on. You know, probably not a day goes by that I don’t pull off of my shelf my copy of the HIPAA privacy regulations and read through – remind myself what it says about this or that or the other thing. So, the ability to read and interpret the legal language, it's not just the HIPAA privacy regulations, it is state law and – and that sort of stuff. And – and the ability to converse with our legal authorities. You know, we do have a go-to attorney on staff for questions about HIPAA but you have to really stop and think about how you're going to express your question because it's a different world. And this person has no operational experience in healthcare so doesn't really know when you're describing a situation what you're talking about other than perhaps from the patient's perspective. So, it really requires some – some high communication skills to bridge that gap between the legal stuff and the day-to-day practical operational stuff.

JF: Is there an incident you could describe and how you handled it?

Subj: Sorry, that was your question. That was your question.

JF: And as a privacy officer, you could also say well, no.

Subj: Yeah. Well, you know, yeah, I suppose so. You know, and this gets a little long-winded so – so I guess bear with me as the watch word here and don't hesitate to reach out and just stop me if I'm going too far. I heard HIPAA patients have certain rights and in two of them kind of work together. One of them is the right to have access or obtain copies of their own health information, and kind of along with that one is the right to request an amendment to your health information. So, you know, the assumption is you review your records and you see something that you think is incorrect or incomplete or just plain wrong. And so, you go back to your healthcare provider and request an amendment. Those are not very straightforward [redacted]

[redacted]

[redacted] This person – so I of course notified this person of all of that and they continued to object strenuously to that. And so, it was a matter where I needed to consult with our attorney and make sure that – that we are – that we are in fact doing what we needed to do, that we are complying with the law and so forth. And – and explaining all of what I just explained to you to our attorney who really has no experience with any of this stuff was a bit of a challenge. But ultimately, we got the point across and found that, you know, we really couldn't do anything more, that we had done what we should do. So, I hope that makes sense.

JF: Perfectly, thank you. You ran through a number of – oh, I'll call them critical skills that are very important to your daily operations. Are there other skills that you see becoming important in the near future?

Subj: Well, I – I want to – I may have to ask you to remind me of that question because I will – I just want to remark on some skills that I think that are other skills that are probably necessary that I hadn't mentioned before that I don’t necessarily own and I think they're the soft skills, the people skills. I'm a great technical person [redacted] So, soft people skills is another one but as far as in the future – well, I tell you I sure wish that – that many of the regulatory changes, the HIPAA regulatory changes related to high-tech were actually published at this point because that would give me a clue about where we're going. And – and there had been a rumor that – that we would see them in April and we haven't yet of course. At – and but – but, you know, high-tech had, you know, some changes to HIPAA privacy and security regulations. It also – I mean really what it's promoted as is this possibility of money for meaningful use of – for the HR. And there's some very – there's a lot of real detailed technicalities around meaningful use and so forth that I have not been following very closely and regretting that because some of those questions are starting to circle back around to me as privacy officer. And in the – as the development of health information exchange and more widespread use of electronic health record systems becomes our reality, I think that privacy officers would be well served by understanding some of the technical aspects of that stuff, not – I mean there are certain sort of high-level kind of philosophical aspects about gee, if you are entering into a health information exchange and making the patient information that you contain within your electronic health records system more available to a wider community, how – how does that – how can you maintain that consistently with HIPAA privacy and the patient's rights to perhaps control who gets to see their records and so forth? And so I think understanding the – the – some of the – the in-the-weeds details of health information exchange and meaningful use would – would be a good thing for privacy officers.

JF: Are the HIE questions the ones that are circulating back to you?

Subj: Not so directly. You know, the weird thing is just that – that when we implemented our current electronic health records system, it was seen from the beginning as what HIE is now seen as. It was – it was called and still is called the Community Health Record. We have from the very beginning granted access to it to community providers who – their probably only connection with us is that they're on the medical staff. And we even provide access to – direct access as a user to providers who are not on our medical staff but if they refer patients to us, then they may kind of meet criteria for having access to it. So, we've been doing HIE kinds of stuff for a long time, not necessarily within the same structure or framework that has been envisioned for HIE and I'm not even clear what the vision for HIE is but it's – the questions that are starting to come up are – are some of those yeah, you know, so I guess in going around here in circles a little bit, yes, to a certain extent they are but it's stuff that we've been doing all along. And it's questions like gee, I’ve got a request from this community provider for a report of, you know, of data about certain patients who have certain criteria, you know, perhaps patients that he's treated in the hospital, that sort of thing; can I provide that. It's those kinds of questions that – that of sharing information with community providers and so forth about where are the boundaries around that. They're still pretty hazy for people if that helps. I feel like I’m going around in circles and answering very vaguely so forgive me but --

JF: I think that may simply be indicative of the state of the field right now.

Subj: [redacted]

JF: If you're going to hire another person into your organization, a potential staff member, what skills would you like to see in them?

Subj: To assist with my work, that – is that what you're thinking? Or what – what types of work?

JF: To assist – to assist with your work or to assist with a – another – perhaps a peer level inside the organization.

Subj: Okay. Well, we did that recently [redacted] And – and that person has been on board for a couple months now, just a couple of months. So, yeah, I – we – I helped interview this person and so forth. What kinds of skills? I think and certainly, this person being hired into that particular position, there are certain aspects of that that at Southwest that we needed a certain skill mix for. They're brand new to [redacted] so – so this person is kind of being thrown into the deep end and so far as we're implementing [redacted] So, there's some – there's certain aspects of that person's – the skills we were looking for in that person that – that are unique to that position but it had to be a strong person. They had to be able to assert themselves and – and understand the – the policies, procedures, guidelines, all of that kind of stuff and be able to stand on that firmly and say this is the way it will be. They had to have that critical thinking, how do – do these [redacted] system-wide policies apply to all these other regions and facilities and so forth, how can we make those work here at this facility that has never had to think about that kind of stuff before. So, they – so, [redacted] had to be an excellent communicator and have good – those good soft people skills, and at the same time be confident in – in where she stands. And I think we found the right person. But those are the things that come to mind anyway, you know. I don’t think, you know, any of the skills that I mentioned early on would be what I would be looking for if I were hiring somebody to assist me in this kind of work as well.

JF: Okay. What skills would you like to acquire?

Subj: Well, the soft people skills would be nice. [redacted] You know, I have no patience for incompetence. So, certainly more patience would be a godsend. I don’t know how one goes about acquiring patience but, you know, if there's a – if there's some route to that, I would be interested in that. But the soft people skills, you know, I – and diplomacy, wording those – those different – those difficult sort of confrontory kinds of things, you know, where you have to go to somebody and say, you know, what you're doing is not correct or not right, and we need to work on changing that. [redacted] I, you know, here's another skill and I think one that should go on your list of skills that any privacy officer should have and that is being comfortable with the new and the different, and, you know, basically being willing and able to get out of one's comfort zone, and to be adventurous. You know, it's really easy for me to be comfortable here behind my desk in my office, head down, working away at whatever kind of – of word – wordy, you know, processing task or, you know, working on policies, working on procedures, things of that, and not getting out into the field and talking with the people who are doing the real work of our organization caring for patients. And so I think it's important for somebody to have that kind of adventurous spirit to be able to go out into the clinical areas or wherever that may be outside their comfort zone and to talk to those people in the field and work with them to make sure that whatever policies and procedures that we're making up back here in our little ivory tower actually work in a practical reality.

JF: What questions haven't I asked?

Subj: Well, I’m looking else at what your – the study information sheet and – and your – the purpose of your study is to determine skills and background and to determine the requirements for such a position. So, what questions haven't you asked. Yeah, you know, I mean what comes to mind is what are the biggest challenges that are faced on a day-to-day basis, and perhaps I suppose, you know, if you had to do it all over again, would you.

JF: Would you care to answer to both?

Subj: Well, to the latter question, yeah, I probably still would. I really didn't know what I was getting into. I – I enjoy the privacy and security aspects of my job more than I enjoy the general compliance aspects but it's, you know, it's partly because I have become an expert in the privacy aspects and haven't really had an opportunity to become an expert in the other areas so much so it's not as comfortable. But yes, I probably would. The biggest challenges are – are helping our caregivers to understand the boundaries in a way that – that makes sense within their work. You know, of – here's a good example. We – we – the Oregon Association of Hospitals and Health Systems Compliance Advisory Committee recently revised a set of guidelines for disclosure of patient information to law enforcement. And I was involved in that project, and so I took those revised guidelines and boiled it down to or boiled them down to a two-page kind of a cheat sheet for our staff who are most likely to have interaction with law enforcement, emergency department staff, nursing supervisors, patient registration staff, our security folks, people of that nature. And I was called down to the emergency department just a couple weeks ago by the charge nurse who wanted to talk over this cheat sheet because he didn't understand part of it, and – and what it came down to was that this cheat sheet was derived – at the end of the day, you know, through a couple of steps but directly from the regulations and it uses some regulatory language. And there was one term in there that was just throwing this guy, the charge nurse, for a loop and that was about that law enforcement was – must represent that withholding information will – in a certain circumstance, withholding information will interfere with their investigation. So, it's the represent that; it’s the use of the word represent in this context that he didn't understand, and it just didn't make sense to him. It was a good lesson to me about, you know, even after all this time, it's still an ongoing challenge to put this stuff into everyday English such that our caregivers get it and – and act on it. It's – it's really difficult though because there are nuances. There's always a yes, this is the rule except and there's always these exceptions and you end up, you know, in trying to make sure that they have the whole picture, it ends up too big, too long, too detailed. If you try to put it in bullet points, then it shortcuts all of that stuff and then they can end up making mistakes. It's really difficult to find that middle ground. That would be the biggest challenge ongoing, not that it helps your skill set though.

END OF RECORDING