HEALTHCARE INFORMATION PRIVACY + SECURITY

Regulatory Compliance and Data Security in the Age of Electronic Health Records

BERNARD PETER ROBICHAU

FOREWORD BY MICHAEL CLORE SANDERS, MD

Apress

For your convenience Apress has placed some of the front matter material after the index. Please use the Bookmarks and Contents at a Glance links to access them.

Apress®

Contents

Introduction

This book is not about information security or healthcare information security in general. It is about electronic medical record (EMR) security—the difficult task of ensuring privacy and security in the evolving world of digitized patient data.

I receive so many urgent calls from people seeking assistance and guidance with their EMR security projects that I can't begin to respond to them all. That unmet need motivated me to write this book to impart the methods I have found to work most successfully. Most of it I wrote in hotel rooms and airport lounges during my constant travels as an EMR consultant. I am still amazed (though no longer surprised) when I find myself sitting next to someone in an airport using EMR software. The other day I found myself hammering out a chapter while involuntarily eavesdropping on one end of a conference call about an EMR project. It was as though the EMR buzzwords and project phases I was typing in our specialist space were mysteriously leaking into the public air!

Patient data is being transitioned from paper to electrons very rapidly, and the goal of EMR ubiquity is fast approaching. It is my hope that this book will help those who are struggling with the huge task of securing the EMR. It is a task that is important to me personally and one that should be given top priority in healthcare organizations everywhere because it is, quite simply, the right thing to do.

CHAPTER

1

Introduction

The Long-Awaited Manual

There is no terror in the bang, only in the anticipation of it.

—Alfred Hitchcock

I was a veteran of the information technology world, and IT security had become my specialty—it was a domain I particularly enjoyed. I ventured into the healthcare space to work on a project that was driven largely by the HITECH Act (discussed in Chapter 2) and financial incentives related to the implementation and "meaningful use" of *electronic medical record* (EMR) systems.

Note An *electronic medical record* (EMR) is a system used by a provider to manage patient care. An *electronic health record* (EHR) is the set of patient data associated with an individual and spans multiple providers. An EHR is portable by nature, whereas an EMR is a system used by a provider or group of providers. "Meaningful use" is a term of art deployed by federal agencies to denote conformity to a set of explicit and measurable goals that inform EMR implementation to ensure capabilities such as physician order entry and online access by patients to their patient charts.

My job was to guide analysts through the process of building an application that facilitated efficient workflows while complying with organizational and regulatory standards of access.

I was given my marching orders, and I assembled an interdisciplinary team that would work over the course of the next 18 months to ensure that the application was deployed securely and appropriately to a user base that spanned all stakeholders from surgeons and nurses to environmental service workers and billing employees.

The objective was clear, and the markers for success were identifiable. I should have been on solid footing at the beginning of this project . . . but I was not.

The Problem

What I soon discovered was that there were as many interpretations of the phrase "appropriate access" as there were stakeholders in the project. Moreover, there are significant legal (and therefore financial) implications associated with decisions surrounding application access. The patient data that lie at the core of an EMR system are highly sensitive, and any disclosure of these data due to negligence can lead to costly litigation and fines. The more basic but no less important issue I faced was the fiduciary responsibility to treat the customer's private information with the utmost care.

Professional Ethics

There is an inherent problem with EMR systems: They are built on the assumption that the consolidation of patient data for the purpose of broad, comprehensive access (by healthcare providers) will lead to better patient outcomes, lower costs, and a more efficient healthcare system. The problem is that this assumption about access is often at odds with the nature of the data being handled.

Note *Access*, *availability*, and *privacy* are recurring themes throughout this book. The goal of the healthcare IT professional is to balance these three pillars of healthcare information privacy and security so that efficient care is facilitated while safeguarding private data.

In many cases, the analysts who design and implement access controls are safeguarding not only the confidential data of a generic customer but also their own health records—test results, diagnoses, and sensitive personal information.

Since the birth of modern medicine, we have been taught that our physicians are entitled to know about the most private aspects of our lives so that they can provide the most effective care to us. This is a level of confidentiality that is typically reserved for family members, clergy, and counselors. Healthcare professionals are morally and legally culpable if they ever handle patient data with reckless disregard for the patient's assumption and the law's requirement that all such data will be closely guarded and provided only to those with a demonstrated need to access it legitimately.

Vendor Guidance

A natural place to turn with a question about software is the application vendors. They provide the software deployed by the people charged with implementing and managing complex EMR systems, and it stands to reason that they will have the answers to tough questions.

Application vendors are, however, justifiably hesitant to provide detailed guidance in the realm of security and compliance. They prefer, instead, to facilitate the implementation of their software in alignment with the organization's policies and standards, which presumably address access, availability, and privacy.

What does this mean for the people charged with implementing and managing complex EMR systems?

1. Vendors will be valuable source of information about the options available and how other and often similar customers have done it.
2. Vendors will not offer definitive answers about what the customer should do.
3. Your organization will need to sift through the options and choose the best solution to your unique circumstances.

If your organization does not have mechanisms in place to consider all of the complex issues and make decisions regarding standards of access, there will be sustained disorder in your security and compliance program. This is why it is so important to establish the ground rules and processes that will lead to a consistently built and secure EMR system.

Many Hats

Going into that first EMR project, I had assumed that my thorough knowledge of information security regulations, practices, and technologies would be adequate for the task at hand. I did not realize that my job would require me to be simultaneously a technologist, diviner, and mediator—all in an effort to bring together the complex worlds of access, regulatory compliance, and usability. Recognizing that many different skills are required to achieve success is often the first step in this long journey. It is quite possible to "herd cats" to ensure your users' access to everything they need and your customers' data security.

The Audience

I thought many times during various EMR projects that a guide or manual of some sort would be a godsend. It is my hope that what follows will help bridge the gaps between all of the disparate, often competing interests that accompany the implementation and management of an EMR system. The medical field certainly needs to push ahead with the implementation of new technologies—but not at the expense of privacy and security.

Note How you use this book will differ depending on your role in the privacy and security life cycle. Although some of the more technical chapters might seem irrelevant to managers or directors, do not be fooled! Perhaps a very careful reading of these chapters will not be required by all, but it is important that managers and directors understand what is at stake so that the technical staff can be held accountable for addressing these critical areas.

Who will benefit from this book? First, it is important to understand that this is not a technical manual to aid in each iteration of the project (though it will certainly assist in this regard). Rather, this is a technical book for business operations. It will help each stakeholder understand the issues at hand and the technologies or solutions that can help in achieving organizational goals. These include but are not limited to:

- **Executives:** Those who serve as project sponsors will do well to understand the competing interests surrounding privacy and security.
- **IT directors and managers:** There are enough topics related to the management of people who manage systems to make this book a resource for department directors, office managers, and others with an interest in how organizational goals are being implemented.
- **Technical staff and analysts:** It should not be assumed that the application analyst is the only member of the technical staff who needs to know the ins and outs of EMR privacy and security. System administrators, database administrators (DBAs), and help desk staff all need to understand what is at stake.
- **Information security officers and staff:** It might seem obvious that your information security personnel would need to understand the issues surrounding EMR security, but old staffing models—whereby security

personnel managed antivirus definitions, virtual private networks (VPNs), and firewalls simply don't account for EMR access issues. Your chief information security officer (CISO), security architects, administrators, and provisioning staff will benefit from an understanding of the EMR security.

- **Ancillary compliance offices:** Your health information management (HIM), corporate compliance, and legal staff will benefit from this manual as much as your technical staff will.
- **EMR vendors:** Employees of EMR vendors often have a non- healthcare background (many having entered the field straight out of college) and will benefit from a thorough understanding of privacy and security issues.
- **Consultants:** The outside people who are often brought in to assist with project or program management will need a good foundation in healthcare information privacy and security.

The Goal

Whether your EMR system is pre-, mid-, or post-implementation, your goals are the same: a system built with privacy and security integrated throughout, and a security program that facilitates a continued focus on the same.

- If you are **pre-implementation**, congratulations! You are starting out with a tool chest of information that will help ensure that you build your system, and develop your processes properly.
- If you are **mid-implementation**, struggling to align the competing interests within your organization as you build your EMR system, then you will have the reinforcements you need to get back on track and finish with a huge success.
- If you are **post-implementation**, and struggling with some of the basic concepts addressed in this book, you should be able to tackle each domain related to privacy and security, refine (or redesign if necessary) your existing privacy and security program.

The end result in each case is a sustainable security program that allows the organization to assure its customers that their data is treated with the care that they should expect from any reputable healthcare office or system. A trustworthy security program is not an option in the field of HIM but an obligation. In a world where personal data is proliferating at an exponential rate, it must be properly safeguarded lest it fall into the wrong hands.

You have your marching orders, and you are about to acquire the tools you need to carry them out!

PART

I

The Evolution of a Monster

CHAPTER

2

Waking the Sleeping Giant

A Brief History of Healthcare IT

> *I fear all we have done is to awaken a sleeping giant and fill him with a terrible resolve.*
>
> —Admiral Isoroku Yamamoto, *Tora! Tora! Tora!*

It was 1996, and I had my first job in the IT world. The floppy disk drives I knew in my youth were disappearing, desktop productivity tools were powerful and easy to use, and the World Wide Web was making its way into households across the world.

The Problem with Paper

One thing I noticed soon after arriving at my new job was a process for data sharing that was problematic.

Every morning at about 10 o'clock, an employee in the communications office would emerge in the copy room with a pile of hand-snipped news clippings, which would be assembled and photocopied to form a thick stack of news that was relevant to the industry in which we worked.

This bundle of trade news was then reproduced countless times, stapled, and delivered by the mailroom to division directors and executives for mid-day perusing.

I watched this well-paid middle manager repeat this process each day, using his expert judgment to determine what news was important to share with his colleagues. I even saw this important job handed off to another manager when the original "news clipper" retired.

This stood in stark contrast to the growing number of newspaper websites that shared the same type of information directly with consumers on their Internet-connected computers. I remember looking on with amazement the first time I saw the *USA Today* website slowly render across a computer screen over a dial-up connection several years earlier and wondered just where this new technology was going to take us.

In short order, the venerable tradition of clipping trade articles, photocopying them, and disseminating the packets of information fell by the wayside. It had become obvious that paper was an inefficient way to share information, and businesses were adapting as a result.

By 1998, I had several years of IT experience under my belt. The Internet was proving itself as a productivity tool, and the personal computer was becoming ubiquitous—no longer a toy of hobbyists and geeks. The place to be was telecom or any field related to Internet technologies.

Systems were growing faster, and the demand for new technologies that leveraged ever-increasing bandwidth, which allowed data to flow at greater speeds, was huge. Moore's law was in effect, and any doubt that we were living in the Information Age was laid to rest.[1]

For the next three years I gobbled up the expanding crop of new data-driven technologies. I learned about data packets and the protocols in which they traveled, and I was amazed at how digital content was being used and leveraged to change the way we think and how we do business.

The Downside of Connectivity

Along with my newfound obsession with all things data, I became acutely aware of the inherent dangers of a connected, data-driven digital age. Gone were the days of isolated networks of terminals connected to mainframes that housed an organization's critical data. As PCs were connected to servers and both were connected to the Internet, it became critical to ensure that the data on those servers (and PCs) was carefully guarded from the growing threat of hackers and Internet thieves.

[1]Moore's law is the empirical induction that gains in technology double every two years, allowing for dramatic increases in computing trends from year to year.

Data became the commodity-driving business and, as the currency of the digital age, it was a prime target for theft and sabotage.

It was like a game of cloak-and-dagger: implementing firewalls to protect assets, reviewing logs, adjusting rules for the transmission of data, and trying to stay one step ahead of the "bad guys."

Elsewhere in America …

While the rest of the world scrambled to ensure a smooth transition from paper business transactions to digital commerce and do so securely, the healthcare industry plodded along its course, and the paper chart remained the primary means of reviewing and documenting patient care.

Physician practices and hospitals adopted computerized billing and scheduling systems, in many cases long before the proliferation of the Internet. But patient data—the most important digital asset of the healthcare industry—continued to reside on paper.

Businesses ventured into the digital frontier, finding new ways to use computing power to change the way business was done, but healthcare systems maintained the status quo. The paper chart, made from good old-fashioned milled tree pulp, sat stubbornly at the core of the healthcare business model.

The End Result

Since technology was at best an afterthought in the healthcare world, budgets reflected a lack of commitment to information technologies, and top IT talent did not seek out physician practices and health systems when looking for work.

This lack of innovation created a brain drain in the healthcare IT space at a time when the rest of the business world was finding new ways to drive business through IT. When systems such as e-mail and file management were introduced in healthcare, they often remained static and weren't upgraded as new features were introduced.

Old technologies and aging systems were often propped up to keep them running, and they were not replaced when they should have been. IT was not at the core of the enterprise, because it provided only peripheral value to the organization. Instead of being integrated into the business model, the IT department was often viewed by healthcare executives on the same level as the mailroom or facilities management—necessary, but not critical.

Perhaps a healthcare IT job provided a reliable paycheck for some, but it certainly wasn't a space where the brightest could be challenged and grow. Paper was king, and the healthcare world was fine with this model.

The Problem

Think back to the news clipper, beavering away with a newspaper, a pair of scissors, and a photocopier each day, doing his best to ensure that important information made its way into the hands of the people who needed it.

Few would argue that his task was unimportant—managers and executives certainly need to keep abreast of news and trends in their industries. The issue was this: when information can be digitized, as with the newspaper, sharing it via paper becomes inefficient.

Another problem with paper-based information sharing is the method of aggregating the data. In the case of the news clipper, he was the arbiter of what was important and what was not. In this analog newspaper world, the process of information sharing goes something like this:

1. The newspaper editors determine what is newsworthy and what is not.
2. Stories are written, proofed, edited, and compiled for publication on a daily basis.
3. The paper is printed and assembled.
4. The paper is delivered.
5. The news clipper reads through the paper, making a judgment call as to what is important and what is not.
6. The articles deemed important (by the news clipper) are extracted, collated, and assembled into an information packet.
7. The packets are distributed to management.
8. Managers read through the information packets with an eye for items of relevance to them.

Notice several things about this process:

- The extremely linear system makes it probable that the data will get to management too late. News that arrives in this analog format is likely to become stale quickly.
- Managers are likely to miss articles that are important to them, but were deemed unimportant by the news aggregator, the news clipper.
- An analog process is used when a more efficient, digital process could be employed.

Certainly, there are some stories provided by newspapers that are not time-sensitive, and there is something to be said for the tactile and sensory experience of picking up a freshly printed newspaper and reading it over a cup of coffee. There is nothing I like more than to read the Sunday issue of the *New York Times* front to back, but I don't read it to keep up with breaking news. The *New York Times* has, in turn, refocused on in-depth features and human interest stories, keeping their medium viable in this digital age—but they are still struggling to compete in this world of bits and bytes.

It's a different ball game now, and an attempt to preserve old processes for the sake of nostalgia or familiarity will lead to obsolescence and obscurity—not a worthy goal in any case.

The Healthcare Industry Analog

The goal of a paperless society has proven unrealistic, at least in the short term. By many accounts, indeed, our digital age has *increased* reliance on paper, because we have taken the abundance of new data of all sorts as a call to print even more than ever. Nonetheless, paper transactions have been disappearing steadily as digital transactions replace them.

Think about the financial industry, where withdrawing cash from the bank once required writing out a paper check to "Cash" in front of a human bank teller. Now, an ATM dispenses the same cash, with no face-to-face human involvement, and the customer has the option of taking a paper receipt or declining it.

The obsession with paper in the healthcare world did not subside as it did in other sectors of the business world. Let's look at the (once) common workflow in a physician's office during a patient encounter:

1. The patient arrives for a visit, and the physician makes a general inquiry about the reason for the visit.
2. The patient presents his current state and describes his symptoms as thoroughly as possible.
3. The physician proceeds through an exchange about the symptoms with the patient, which might involve taking notes or might be purely verbal.
4. The physician plans a course of treatment, conveys this to the patient, and documents what transpired in the patient's paper chart.
5. The physician might make a referral on paper to a specialist.

6. The patient arrives at the specialist either with or without a copy of his paper chart, and the specialist asks the same questions the physician had asked on the previous visit.
7. The specialist plans a course of treatment, and the notes about this encounter were placed in yet another paper chart housed at the specialist's office.

In this scenario, the provider should probably follow some better practices, but there is nothing about this paper-based process that facilitates an efficient workflow.

- Perhaps the provider began by reviewing current medications with the patient (always a good place to begin an office visit), or perhaps, being pressed for time, he began addressing symptoms.
- If the primary encounter happened to be documented thoroughly, there would be a fairly high chance that the visit notes would be only partially legible to anyone other than the primary provider.
- In the event of a referral, the original paper chart and all of the valuable data it contains are likely to remain at the primary care provider's office because it is cumbersome to transfer. The specialist will often be starting from scratch.
- Additionally, information such as blood pressure, heart rate, test results, and so on would have resided within the "commotion" of the physician notes, and a correlation of these critical numbers from a series of visits would have been difficult and time-consuming.

There are so many uncontrollable variables introduced by the paper chart that inefficiency is the least of our concerns. Patient care begins to suffer when health data is maintained in multiple places in a linear fashion.

Just as patient care can suffer when all aspects of care are documented on paper, huge gains in patient care can be achieved when best practices are enforced by computer systems and discrete data is maintained in a manner that helps in diagnosis and trending.

Note Among other benefits, the fact that an *electronic medical record* (EMR) stores discrete data allows the key metrics related to the health of a patient to be analyzed and acted on. For instance, when key lab results are maintained as separate fields in a database that can be compared over time, software can find trends that might go unnoticed by a provider, triggering a different approach to patient care.

A Movement Afoot

Even though providers were devoted to the paper chart, it was inevitable that some in the medical field would recognize the potential of technology to benefit patient care. While the giants such as Xerox, Digital Equipment Corporation, and IBM were well on their way to revolutionizing the business world with information technology (IT), a revolutionary idea was brewing in the mind of a recent MIT graduate.

In the 1960s, Neil Pappalardo, a young physics student, was struggling to write his senior thesis when it was suggested that he collaborate with some cardiologists who needed some help. The result was a medical device that examined the electrical signal from a patient's heart. Pappalardo's project was a success, his thesis topic was determined, and his major changed from physics to electrical engineering.

This foray into the medical field led Pappalardo to a job in the computer science lab at Mass General Hospital, where he began to write software to automate the hospital's clinical laboratory and other areas.

Because his position was funded by the National Institutes of Health, his work product was in the public domain. So, in 1968 the programming language MUMPS (Massachusetts General Hospital Utility Multi-Programming System) was created, and the following year Pappalardo founded a company called Meditech (Medical Information Technology) to leverage MUMPS to automate healthcare processes.

The story of Pappalardo and Meditech is perhaps unremarkable. Similar stories can be told about other visionaries and the founding of other companies in any field. But the stage was set, and the healthcare IT world boomed in the following decades to include companies such as General Electric (formerly IDX and Centricity), Cerner, Allscripts, and Epic.

As previously noted, these new trends in healthcare IT did not revolutionize patient care when IT was revolutionizing the rest of the world around us. For the longest time, advances in healthcare IT remained largely confined to business processes (such as scheduling) and order entry (such as prescribing).

What is remarkable about Pappalardo's story is the fact that MUMPS acted as the foundation of many systems that eventually drove the EMR race.

Catching MUMPS

In 1976, eight years after MUMPS was released into the public domain, a graduate student at the University of Wisconsin named Judy Faulkner started developing a program to manage patient information.

Faulkner turned to MUMPS as the foundation of her efforts, and when the resulting program was a success, she began to sell it to hospitals and community health centers.

Note MUMPS, along with the Cache database from InterSystems, acts as the foundation for Epic's EMR as well as others. These might be unfamiliar products to the IT professional who doesn't work in healthcare, but they are essential technologies to understand if you are working with any of the EMR vendors who leverage these notably older technologies.

What followed was the founding of a company called Human Services Computing, which is now Epic Systems. Fast-forward almost 40 years, and Epic Systems now boasts that more than 50 percent of the US population has its health information stored in an Epic digital record.

The Intervening Years

What transpired in the years after the seminal creations by Pappalardo and Faulkner was the creation of a host of systems that introduced technology into medical practice—each with varying degrees of success. There have been leaders in the field, but there was no analog in the healthcare IT space to the Apple versus Microsoft rivalry.

There have been leaders in the field of scheduling and leaders in the field of e-prescribing. Some vendors excelled in the world of ambulatory practice management, and some were the best at order entry. What these niche vendors did from 1970 to 2000 was to highlight the importance of technology in facilitating the complex workflows involved in patient care.

A Voice from Above

With all of the buzz today about the *Affordable Care Act* (ACA a.k.a. Obamacare), *meaningful use*, and the like, people have come to equate federal initiatives related to the adoption of EMR systems with the administration of President Barack Obama.

It was, however, President George W. Bush who created the Office of National Coordinator (ONC) for Healthcare Information Technology within the office of the US Department of Health and Human Services (HHS) in 2004 to coordinate the use of healthcare IT and the electronic exchange of health information.

Note You will need to become familiar with news, rulings, and statements from the `National Coordinator`—the appointed head of the ONC. As standards change or regulations are adjusted in regard to healthcare IT, they are coordinated and communicated through the ONC. For more information, see `healthit.gov/buzz-blog`.

Bush, or perhaps his advisors, saw the compelling need to advance the adoption and use of technology to improve patient care. This was also the first step in the process of controlling spiraling costs triggered by duplicated efforts and fragmented care plans.

The Financial Crisis and the EMR Rush

Just three years after the establishment of the ONC, the world found itself in the midst of financial troubles unlike anything seen since the Great Depression. By 2008 the financial troubles were officially labeled a crisis when the markets plunged and major financial institutions faced the very real possibility of collapse.

To prevent a worldwide financial depression, the US government turned to a series of financial stimulus packages. Troubled assets were purchased by central banks and a series of economic stimulus packages were passed by Congress, the most significant of which was the American Recovery and Reinvestment Act (ARRA) of 2009. Perhaps you have seen the name of this legislative act on signs next to highway construction projects funded by ARRA.

The ARRA legislation included a provision specific to healthcare IT dubbed the *Health Information Technology for Economic and Clinical Health Act* (HITECH Act).

Note The HITECH Act is a critical piece of legislation that it is critical for you to know inside and out, because it clarifies in detail the legal and legislative guidelines related to healthcare information privacy and security. Read more about it online at `http://www.healthit.gov/policy-researchers-implementers/hitech-act-0`.

The HITECH Act was nothing less than a sweeping piece of legislation that was intended to hasten the adoption of EMR systems by providing incentives for the *meaningful* implementation of certified EMRs.

What scores of vendors had sought to promote in isolation for decades—the digitization of critical patient data—was now incentivized by the promise of large government payouts. Questions related to how certain tasks should be accomplished within the EMR were answered by the HITECH Act. If providers and organizations wanted a piece of the nearly $20 billion that was set aside to encourage meaningful EMR implementations, they were obliged to follow the rules laid out in the HITECH Act.

Think about the Possibilities

It is only logical. The financial world was in turmoil and credit had seized up; pumping life into the economy through the healthcare sector, which accounted for almost 20 percent of gross domestic product (GDP) in the United States at this point, was a surefire way to help revive a failing economy.

But the opportunistic legislators in our nation's capital were not primarily concerned with economic health. Although the HITECH Act is clearly concerned with economic health, we need to parse out the phrase "economic and clinical health" in the legislation's title to understand what is at stake.

Let's go back to the figure cited above—the fact that healthcare accounts for almost 20 percent of GDP in the United States. Although this number is actually closer to 17 percent, the figure is staggering and is the highest national percentage of spending on healthcare in the world. Though the United States has, by certain measures of certain portions of its population, the best quality healthcare in the world, its healthcare spending continues to spiral out of control and out of proportion to outcomes. With government programs such as Medicare and Medicaid footing the bill for ever-increasing quantity and cost of visits and procedures, there is a huge incentive to control costs.

It is still possible to provide decent care to a single patient without a digital health record. From the moment he walks in the door of a doctor's office through surgery and postoperative care, a patient with a paper chart can expect good treatment in the United States (though there are certainly efficiencies to be gained through the use of computerized systems).

The huge potential cost savings from the use of digital health records comes through *population health management*. We can speak about the consumer benefits provided by *electronic health records* (EHRs)—and online access to personal health records is mandated in the HITECH Act—but these benefits are peripheral to the primary goal of the EMR.

When information in a patient chart is segmented into *discrete data*, the possibilities for improving patient care and decreasing costs are endless.

Consider the most basic information in a patient chart: the patient's date of birth. This information alone can trigger an automatic appointment for

prostate exams or mammograms that might otherwise be overlooked until a costly and perhaps lethal diagnosis is made later in life.

The paper chart helps doctors understand the patients sitting in front of them. The EMR, on the other hand, helps the organization recognize who is not coming in for a visit that should be.

On a macro level, the data collected in lab draws and even vitals collected over time can help statisticians correlate trends in pathologies and diseases, leading to better preventive care in the future. Perhaps the data collected on you today won't keep you healthier now, but when combined with the data of millions of other patients, it might save thousands of lives a decade from now.

Cost-effective population health management is the ultimate aim of the EMR initiative. With the establishment of the ONC and the enactment of the HITECH Act, we are on our way to realizing the dream if the tools at our disposal are used wisely.

Pandora's Box

With all of that new personal health data in databases across the country, the ONC realized that the risk of privacy violation and identity theft was much higher.

The federal government had previously imposed some guidelines regarding expectations of privacy related to patient data in the *Health Insurance Portability and Accountability Act of 1996* (HIPAA), but most industry officials would tell you that many practitioners were lax in following these rules and the government was lax in enforcing them.

The HITECH Act put teeth in the enforcement of existing HIPAA rules and extended regulations related to:

- *Breach notification*: specifically related to the disclosure of unencrypted patient data (generally of more than 500 patient records).
- *ePHI access*: accommodating digital access to the patient's *protected health information* (PHI) and chart by the patient for a nominal fee and in short order.
- *Business associate regulation*: no longer can organizations turn a blind eye to their business partners. They are required to require that business partners conform to the same standards of privacy and security as their own employees.
- *Willful neglect*: acts of willful neglect that lead to disclosures, or unauthorized access, of PHI will be subject to fines and penalties.

The Stage Is Set

The years of the Great Recession that followed the 2008 financial meltdown coincided with the years of the implementation of the HITECH Act, which propelled the rapid and concerted adoption of EMR systems across the United States. Patient data began to flow into these systems at a staggering rate, and the job of securing this data, ensuring that it was used properly, and didn't fall into the wrong hands was often an afterthought.

As EMR systems begin to do their jobs and hospitals and physician practices settle into operational support mode, key employees must take a hard look at how the data they keep is being used and what they are doing to ensure that they are acting as trustworthy guardians of a very sensitive resource.

Further Reading

"MIT Alumni & Friends Profile: A. Neal & Jane Pappalardo, Pappalardo Fellowships," at http://web.mit.edu/physics/giving/profiles/pappalardo.html (accessed December 31, 2013).

"Meditech Corporate Timeline," at https://www.meditech.com/corporatetimeline/homepage.htm (accessed December 31, 2013).

Moukheiber, Zina, "Epic Systems' Tough Billionaire," Forbes.com, April 18, 2012, at http://www.forbes.com/sites/zinamoukheiber/2012/04/18/epic-systems-tough-billionaire/ (accessed December 31, 2013).

"About ONC," at http://www.healthit.gov/newsroom/about-onc (accessed December 31, 2013).

"Index for Excerpts from the American Recovery and Reinvestment Act of 2009 (ARRA)," at http://www.healthit.gov/sites/default/files/hitech_act_excerpt_from_arra_with_index.pdf.

Davidson, Kavitha, "The Most Efficient Healthcare Systems in the World," *Huffington Post*, August 29, 2013, at http://www.huffingtonpost.com/2013/08/29/most-efficient-healthcare_n_3825477.html (accessed December 31, 2013).

CHAPTER

3

It's Not Just HIPAA

Legislating Privacy and Security

Laws control the lesser man. Right conduct controls the greater one.

—proverb

I remember the first time I signed a HIPAA privacy notice before a routine checkup. It was a rather lengthy form, and the practitioner wasn't terribly interested in having me read the whole thing but was rather insistent that I "initial here" and "sign there" so that the paper could be filed away, I assumed, in case there was some sort of a lawsuit involving the disclosure of my personal information.

In fact, what I had signed was not the medical equivalent of a liability waiver like the ones that I had signed before venturing out on Jet Ski excursions or parasailing adventures. Rather, it was a standard notice describing:

- That the covered entity (in this case, my family doctor) was permitted to use my protected health information for limited purposes and was required to get my permission to use it otherwise.
- That the covered entity was responsible for protecting my privacy.

- My privacy rights, and what I could do if I thought my rights had been violated.
- How to contact the covered entity for more information and to make a complaint.

The *Health Insurance Portability and Accountability Act of 1996* (HIPAA) was crafted primarily to address the growing problems of health insurance cancellations (hence the "portability" provisions of the act), but it also addressed the growing concerns about patient privacy (the "accountability" portion).

For many years, the enforcement of the privacy laws included in HIPAA were confined to checks on whether covered entities, as they were called—which included physician practices, health insurers, hospitals, and other businesses and organizations that regularly handled or processed sensitive patient data—were notifying their customers of their rights to privacy and confidentiality. Businesses knew that HIPAA didn't have a strong enforcement mechanism, and the federal government certainly didn't have the manpower to police the healthcare industry.

Minimum Necessary

A key protection within HIPAA was the license granted the covered entity to transmit *protected health information* (PHI) to the *minimum* extent *necessary* to facilitate medical treatment and billing, freeing practitioners from liability concerns that might otherwise arise in the process of conducting daily operations.

Countervailing limits were placed on the *release of protected information*—or more commonly just *release of information* (ROI)—by the covered entity. Patients had the right to expect that the type of information disclosed in the course of business was relevant to the transaction being processed. Therefore, a nurse would have no business seeing delinquent bills, and a biller would have no business seeing sensitive diagnoses. All of these expectations were clearly outlined in HIPAA.

Note Keep this concept of the *minimum necessary* in mind as you read through the remaining chapters. We return to this standard several times, especially in Chapter 8.

HIPAA did not specify how the covered entities should accomplish these privacy measures but simply stated that this was the standard that should be followed.

More Accountability

In addition to the added layers of privacy that a patient should be able to expect, the covered entities were expected to document their privacy practices and appoint an individual who would be charged with overseeing security, compliance, and privacy oversight and enforcement.

For many small operations, this duty fell to the operations manager, who simply donned the "privacy officer" hat, but in larger organizations with complex operations, this was a daunting task.

Perhaps someone was in charge of information security (think *firewalls* and *antivirus*) while other people were in charge of corporate compliance. This new world blended the worlds of technology and compliance, and it was uncharted territory.

Think about the areas affected by patient privacy. You have many layers of operational staff handling sensitive patient data. You also have administrative staff, such as secretaries and IT professionals, with access to sensitive information. Environmental services employees and patient transport staff are all exposed to certain levels of private information, and these employees have to be trained and monitored. Patient data is copied and kept on hard drives, on paper, on desks, in databases, in file cabinets, or perhaps on removable digital media. How does the organization ensure that the flow of data is controlled and limited to the proper channels? How does the organization handle inappropriate disclosures of data? What's more, how does the organization correct the process that led to the inappropriate disclosure in the first place?

Security Rules

HIPAA was enacted in 1996, but various portions of the law were phased into place over time to give organizations a chance to come into compliance with new standards and expectations.

A key aspect of HIPAA is Part II, called the *Security Standards*, which are broken into three logical groupings: *Administrative Safeguards*, *Physical Safeguards*, and *Technical Safeguards*.

Note Whether you work in the field of corporate compliance, privacy, information technology, health information management, nursing informatics, or a related field, it is important to understand the security rules. The technical rules will apply more to some, and the administrative rules to others, but there are few positions in healthcare IT that will not be concerned (at all) with HIPAA security rules.

The Security Standards specify how the Department of Health and Human Services (HHS) expects each covered entity to ensure privacy and security in regard to protected health information.

Administrative Safeguards

The Administrative Safeguards in HIPAA are intended to force the organization to methodically account for its privacy and security practices. With the final ruling effective in 2003, organizations are legally obliged to have integrated privacy and security in their business practices. Handing out a HIPAA notice to patients annually is not compliance with the ruling!

What application of administrative safeguards looks like differs from organization to organization. The content of the HIPAA rule is more than 50 percent administrative, yet there aren't detailed instructions on how to apply these standards.

What is clear is that existing practices must be evaluated (*audited*), and deficiencies so identified must be addressed.

Some of the Administrative Safeguards that covered entities must address are:

- *Policies and procedures*: These must be documented, and the process of adopting them must be discernible. For example, who approved the policies, and how do they fit in with the compliance framework?
- *Accountability*: The buck has to stop with someone in the organization, and whether this person is called a *privacy officer*, a *chief security officer*, or another title, internal policies must reference that authority in matters of privacy.
- *Access controls*: How does the organization decide who is allowed to access what PHI? What is the process for creating accounts, elevating privileges, and terminating access?
- *Auditing*: How does the organization audit its security and privacy practices and correct for noncompliance? What is the frequency of internal audits, and who performs these? What are your audit processes?

Notice that these safeguards are open to interpretation, but the key factor here is the establishment of standards and subsequent record keeping. If you can't prove that you have complied with these standards, then in the eyes of the law, they simply aren't being followed (even if you are).

Physical Safeguards

Just as the administrative safeguards aim to ensure that an organization weaves privacy and security into its business processes, the physical security rules in HIPAA address the need to ensure that the physical environment where PHI is stored and rendered does not promote the unnecessary sharing of private information. Therefore, covered entities must consider:

- If adequate physical controls (badge-protected doors or physical security guards) protect areas where computer systems reside.
- Whether workstations are protected from unauthorized users, or the general public, by physical/visual barriers.
- How to ensure that PHI is guarded as equipment is introduced to the network and retired from operations. When it discarded, what is the organization's policy for ensuring that all PHI is removed?

The physical security of computers might seem like a no-brainer, but I am always amazed at the new and creative excuses that end users propose as reasons they cannot be bothered with a password or a reasonable timeout period on their system. The HIPAA ruling provides a very clear answer to those who cannot be bothered with the most basic measures that must be in place to ensure the integrity of patient data.

Technical Safeguards

HIPAA is, as noted, almost entirely administrative—mandating that we take care of patient data with good, solid practices in the enterprise. However, there is a certain amount of cybersecurity that must be employed to work with our best practices, ensuring the integrity of PHI.

Technical safeguards, according to HIPAA, should ensure:

- *Data integrity*: An organization is responsible for ensuring that the data in its care remains in an unaltered state. To use a technical term, *checksums* should validate that data is as we expect it to be. We should be able to trust that the blood pressure reading associated with Martha Smith is indeed hers and that her Social Security number is accurate. If we can't be sure that our data is accurate, then we have a problem.

- *Data protection*: The data housed in an enterprise should be safe. It should be encrypted when possible. It should be behind firewalls. It should be safe from viruses and hackers, and the customer should have every reason to believe that it will remain safely in the care of the organization.
- *Configuration management*: To avoid the inadvertent introduction of a change into the system that could lead to productivity or, worse, patient safety issues, the organization is responsible for maintaining a thorough record of configurations pertinent to its patient data systems.
- *Authentication*: How does the organization confirm that the person who is accessing your data is who he or she claims to be? The most basic level of authentication is a user id and password, but some organizations would do well to add a second layer of authentication, force password changes, add complexity to password requirements, and more. These are all aspects of the authentication requirement in HIPAA.

The HIPAA rule, in this case, extends from your administrative staff to the technical staff, and you can see how important it is to make sure that managers work with technical staff to implement and then document how they have complied with HIPAA.

The HIPAA privacy rule set the healthcare privacy and security machine in motion. Target dates were set, and there was an expectation that organizations would begin complying with the regulations that were established. But, as noted, there wasn't a great enforcement mechanism, and this was a problem.

HITECH Security

Chapter 2 touched on the fact that the HITECH Act of 2009 probably did more to encourage the digitization of health data and the adoption of electronic medical record (EMR) systems than the previous four decades of corporate marketing combined. What I did not cover there was the expansion of privacy and security regulations under the provisions of that law.

HIPAA was a valiant effort to raise awareness of the need to protect patient data, but it was just phase one. Those industry officials who were pushing for legislation that would encourage the adoption of EMR systems were also aware of the inherent privacy issues at stake. When you digitize patient data and make it more accessible to those providing care (or using the data for analytics), it can easily fall into the hands of people with nefarious intentions.

Identity thieves and snooping family members alike would love to see the contents of a patient chart, and it would require additional work to ensure that our increasingly connected health systems were increasingly secure and private. The old way of doing business would not be adequate as the healthcare world moved into the twenty-first century, and the architects of the HITECH Act knew that added attention to privacy and security had to be part of the legislation that would push more patient data online.

So the HITECH Act simultaneously guarantees greater patient rights and protections in regard to privacy and security while significantly increasing the potential liability of covered entities if they fail to comply with the regulations.

The beefing up of HIPAA regulations doesn't stop there; the HITECH Act grants HHS broader powers of enforcement against noncompliant providers and covered entities. The HITECH Act was a warning shot across the bow of the healthcare industry, which was, until 2009, operating under the assumption that since the risk of enforcement was low, there was little need to allocate resources to the complex and often expensive arena of privacy and security.

Note *Risk management* is a discipline in the business world that calculates the financial risk of many scenarios and determines the best path for an organization among the multiple options. A low-risk and low-cost scenario will almost always be selected over the low-risk and high-cost scenario, even when the latter is what needs to be done as a matter of integrity, privacy, and security. "What is the likelihood?" executives will ask. The fashioners of the HITECH Act aimed to increase the risk to covered entities from poor privacy practices and thereby incentivize their adherence to the law.

The HITECH legislation specifically singled out the all-too-common practice of "willful neglect," where a covered entity knowingly permitted bad practices, system misuse, security risks, and flagrant disregard for the integrity of PHI. Health systems that might have turned a blind eye to privacy and security in the past will certainly pay attention to fines that can soar to well over $1 million for repeat offenders.

Further delineated in the HITECH Act are standards for breach notification. If a covered entity "loses" data related to, generally, more than 500 patients, standard notification processes kick into gear. The public must be notified of such breaches, and the details of the breach are posted publically on a wall of shame (of sorts) maintained by HHS. This negative deterrent was reinforced by requiring local media to be notified when certain criteria of a breach were met.

Misplace a laptop with spreadsheets full of patient data? Data breach! Depending on the number of records on the laptop, a simple slip-up like this could be a media nightmare for an organization, costing business and the trust of the patient population they serve.

While HIPAA laid down the law about what needed to be done, the HITECH Act was HHS's way of saying, "And we mean it!"

The Omnibus Rule of 2013

A quick note is required regarding what many refer to as the *Omnibus Rule of 2013*.

When it came to *business partners*—those business associates that a healthcare organization might contract with but did not manage directly—there was a convenient document called the *business partner agreement* (BPA) that healthcare organizations loved.

Note Business Partner Agreements will be discussed in detail in Chapter 13, and a sample BPA is provided as an appendix. Business partner relationships must be addressed front and center in your security program and not glossed as peripheral to it.

When the BPA was signed, many organizations believed that they had effectively washed their hands of responsibility for the employees of the contracted organization. "Let *their* managers ensure that our contractors are abiding by the rules," the healthcare company would say.

In 2013, a key feature of HIPAA went into effect that essentially obligates covered entities to ensure that their contracted employees, or business partners, are complying with all aspects of the HIPAA privacy and security regulations.

In other words, how your business partner handles your patients' PHI *does* matter. How your business partner's computer complies with security standards matters. If your business partner loses a laptop or external hard drive with your patient data, that is *your* data breach and *your* responsibility to report it. Does your health information management coding contractor hire work-from-home employees who use the family computer, full of viruses and malware, to accomplish key business processes for your organization? If so, you are liable for the risk you facilitate.

A Method to the Madness

Healthcare systems everywhere have a common goal—quality outcomes, right? Well, we should assume this, but there is an underlying assumption that the systems are going to make a profit in the process (or go down trying). Even the not-for-profit health systems out there boast large buildings with state-of-the-art technologies. Executives make decent salaries in most cases

and, although many providers bemoan the collapse of healthcare as a viable source of income, the reality of the matter is that it is still possible to make a decent living as a doctor or a surgeon. When the federal government stepped in to help healthcare systems implement EMR systems, thereby improving quality outcomes, the same financial drivers remained beneath the surface.

It is simply not viable to continue funding an inefficient system with tax dollars for the long term. By focusing on outcomes, reducing duplicative processes, eliminating readmissions, and mining the data from millions of patients to determine how we might eliminate many of the costly, unnecessary procedures that we pay for day after day, year after year— we just might improve the bottom line.

To do this we need to capture your health data, and we need to capture my health data, and we need to be sure it stays right where it belongs—in the care of the health systems providing our care.

Should our data be used to improve the overall healthcare system? Certainly! Should we expect that our private diagnoses—perhaps cancer one day—will remain confidential and available only to those with whom we chose to share them? Absolutely!

It will, however, take a concerted effort on the part of health systems everywhere to ensure that our health data is handled with no less (and, indeed, I would argue, much *more*) care than our banks use when handling our financial data.

This concerted effort begins by educating healthcare employees about the great responsibility with which they have been entrusted and providing them with the tools they need to do their jobs.

Further Reading

"Notice of Privacy Practices," HHS, http://www.hhs.gov/ocr/privacy/hipaa/understanding/consumers/noticepp.html.

HHS, Office of the Secretary, "Health Insurance Reform: Security Standards; Final Rule," *Federal Register,* 68, no. 34 (2003): 8334–8391, http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/securityrulepdf.pdf.

HHS, "Security Standards: Administrative Safeguards," *HIPAA Security Series*, 2, paper 2 (2005), http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/adminsafeguards.pdf.

"HIMSS Privacy and Security Toolkit," http://www.himss.org/library/healthcare-privacy-security/toolkit?navItemNumber=16480.

PART

II

Divide and Conquer: Defining Ownership to Develop Solutions

CHAPTER

4

Assembling the Team

Bringing the Right Human Resources to the Table

> *It's as simple as this. When people don't unload their opinions and feel like they've been listened to, they won't really get on board.*
>
> —Patrick Lencioni, *The Five Dysfunctions of a Team: A Leadership Fable*

Getting out of bed that Monday morning was one the most difficult things I had ever done, or at least it seemed that way at the time. I had a dilemma on my hands because the work of the team I was leading was running up against some walls.

We had our timelines and deliverable dates—these weren't going to change—but there was a key stakeholder in the project who was entirely opposed to the direction we were going. I was asked by my director to work with the stakeholder and solicit feedback, but there was a flaw in this plan. Because the stakeholder had no formal role in the project, and therefore no real voice, there was little I could do to enlist her support.

We were at a critical point, and there were two directions the project could go:

1. Our deliverables would fall behind schedule, or worse, grind to a halt.
2. I could find a way to formally involve this key stakeholder and keep things on task.

I took the issue straight to the program director and explained the dilemma that without the support of this individual we would be unable to make any meaningful progress toward our goals.

What happened, in short, was not miraculous, nor was it an ingenious, tactical maneuver. (Manipulation as a human resources management tactic never works, by the way.)

When the stakeholder was invited to the table; provided with a meaningful forum in which to offer concerns, criticisms, and feedback; and given assurances that these were being heard and considered, her adversarial approach suddenly changed. Perhaps she was now indifferent rather than supportive, but roadblocks disappeared and progress resumed.

All of this to say that who is on your team is important, and those who might not share your vision can certainly add a certain depth or character that will enhance and provide value to the team in the long run.

Where to Start

Because you are assembling a team that will tackle issues of privacy and security, specifically as it relates to the EMR system, you would do well to establish some assumptions:

1. First, while you might speak of the collective group of those with an interest in securing the medical record as "the team," you need to understand that there will probably be many teams addressing different areas of privacy and security.
2. Because, as you learned in Chapter 2, there are many different domains in the realm of privacy and security, and each organization is different, no two teams are going to look the same.
3. There are many ways to interpret the law or, more basically, the fiduciary responsibility to protect patient data, so a solution that might be appropriate in one scenario might not be the solution that another organization chooses.

With this in mind, let's look at the key aspects of a team that should, in most cases, be involved in the security of patient data.

From the Top Down

It goes without saying that executive leadership is critical to any privacy and security initiative. Some would identify this "leader" as the privacy officer or chief information security officer (CISO), appointed in accordance with HIPAA.

I would go one step further and almost insist that the top executive in any organization should be aware and fully supportive of privacy and security initiatives. This is not to say that the CEO of a major health system needs to be involved in the minutiae of decisions regarding privacy and security throughout the organization, but unless the CEO is aware of the importance of privacy and security and fully supportive of the operation initiatives to implement privacy and security measures, operational staff will encounter countless unnecessary obstacles and roadblocks.

Keep in mind that health systems are often riddled with iterations of power and influence peddling that would be unheard of in other corners of the corporate world.

Physicians are employees of the system and yet powerful members of the community (and often members of the board). Benefactors to hospitals have their agendas and pet projects and want to ensure that their voices are being heard as well.

When privacy and security initiatives are rammed through ("Because we must!") and these powerbrokers and influence peddlers see them as roadblocks to productivity and barriers to effective patient care, then the CEO is liable to stop these initiatives cold without much discussion.

However, any CEOs worth their salaries will likely support security measures that are thoughtful, meaningful, and well justified (though perhaps not politically popular) if they trust their staff.

If you aren't the person to enlist the support of your chief executive, then perhaps you'll want to do some prodding to see who might be able to ensure that he or she is involved on some level in the privacy and security program. At the very least, you'll want some assurances that the work you are doing is supported from the top down!

The Stakeholders

Although executive support is key, it is likewise important to identify stakeholders throughout your organization. While this might seem like a straightforward task, the positions described next will often vary from organization to organization, so it might take some sleuthing to find out who actually holds the responsibility for some of the key roles in your organization.

Nonetheless, what follows is a general grouping of core disciplines in the healthcare world and how they play a role in the privacy and security space.

Information Technology

IT might seem like a no brainer, but you will want to find the key IT personnel to assist in various aspects of securing the patient record. These include, but are not limited to:

- **Chief security officer:** This is going to be your key resource for understanding current policies and will perhaps be a point person for questions about application configuration or system settings for your EMR system.
- **Security administrators:** These folks will be able to assist you in determining how the organization handles day-to-day security operations and how your EMR system might fit into their workflows.
- **System administrators:** These employees are the ones who will assist you with server settings, workstation settings, system timeouts, password settings, authentication configuration, and more. Get to know your system administrators well!
- **Database administrators:** Where your patient data sits is very important, and you will want to understand how the data is stored, encrypted, backed up, and so forth.
- **Help desk/operations staff:** These are often the people charged with provisioning accounts for operational systems, and they will likely take over once an EMR project is complete. You will want to understand their process to account for them in designing the operational security policies for your EMR.

Health Information Management

The HIM office is charged with ensuring that patient data is handled appropriately, released in accordance with legal requirements, coded according to standards, and stored in compliance with privacy guidelines.

When it comes to privacy, the HIM office will likely be one of your key resources.

- **HIM director:** The director will likely be able to offer an abundance of guidance on what the organization has deemed appropriate or inappropriate in regard to protected health information. Even if your EMR project is relatively new, the HIM office has probably been processing patient charts for years, and they understand the laws as they pertain to patient data.

- **HIM analysts:** When your paper charts are digitized, they can be released to a fax machine, an e-mail address, or another health system instantaneously, and it is important to control the flow of information (*routing*) through accurate contact information such as addresses or fax numbers. Your HIM analysts can help you understand their release of information workflows.

Privacy, Compliance, and Legal

While the three areas of privacy, compliance, and legal are typically not a single office, their functions involve so much overlap that it is helpful to include them under a single heading here.

Chapter 3 discussed briefly how the decisions you make regarding your EMR system and how you build it are often driven by risk tolerance. This is not always a negative thing and must be considered quite frankly.

Would it be easy to provide one view into the system for all users (from housekeeping to physicians) and simply tell employees, "Just click on the buttons that you need to do your job!"? Certainly. But you can be sure that the hospital would be served legal papers in short order when the housekeeper entered the room of a VIP and offered condolences on his recent terminal diagnosis before the physician had had a chance to share the bad news with him.

The following stakeholders who can help you in these sensitive areas are:

- **Corporate counsel:** The health system's attorney team will, perhaps, not want to be involved in the minutiae of your design decisions, but you can be sure that when you have a workflow issue that involves very sensitive information, legal will want to be involved.
- **Compliance officer:** Your compliance officer is often charged with ensuring that your organization abides by rules related to everything from patient restraints to accessibility and cleanliness, and you can be sure that HIPAA and HITECH are terms that the compliance officer knows well.
- **Privacy officer:** The privacy officer is often charged with investigating complaints about misuse of patient charts—such as, "My husband was in the hospital last week, and my neighbor that works at the hospital knows all about his diagnosis! I want to know if she accessed his chart!" You will want to ensure that your privacy officer is involved in building your EMR system and understands how to use audit tools for forensic purposes after you have "gone live."

Clinical

I cannot stress enough how important it is to have the appropriate clinical representation on your privacy and security team. You will need to make sure that you understand what your organization has deemed appropriate access for various levels of clinical staff, and the only way to know this is to have a direct line to the appropriate organizational leaders with this knowledge.

- **Director of nursing/nursing informatics:** This individual will be thoroughly versed in what your non-provider, clinical staff do on a regular basis to accomplish their jobs. Which staff document in the chart? Which staff places orders? What should they be able to see in the chart, and what is not pertinent to their job functions? These are all questions that you must answer if you want to build a system with integrity that incorporate privacy and security throughout.
- **Chief medical information officer:** This officer is typically a physician who knows the physician workflows in your organization and what the physicians need. Furthermore, this individual should know and understand what various providers (think nurse practitioners and anesthesiologists) should be able to do in the system.

Revenue Cycle

Just as clinical representation is vital in how you build access for your nurses and doctors, you will need to ensure that you have representation on the revenue cycle side of the organization as you build access for folks such as schedulers, billers and coders.

You saw that the HIM director will be key in helping you discern how to handle the patient chart; this same person will also be helpful in determining what the coders and HIM staff should be able to do.

You will want to consult with your finance director as you build access for your billing employees, and with managers in your scheduling office as you build access for your schedulers.

What is important to understand here is that since the EMR system is so tightly integrated with scheduling and billing now, it is easy to give users access to areas that are not pertinent to their jobs. Think of a hypothetical clinical user who could see delinquent charges; it is likewise possible to give a billing user full access to a patient chart, and this is something that you will want to avoid (almost always). Be thoughtful about how you deploy elements of the EMR across functional roles.

The Build/Support Team

Depending on where you are in your project—whether fully implemented or beginning an implementation doesn't really matter—you will almost always have a core group of analysts who will be responsible for the *security build* of the application. When I say *security build*, I don't mean to imply lines of code, delicately crafted to make it impervious to hackers.

Remember, most of the application vendors out there have cobbled together applications with their own "code"—remember MUMPS? Our friends at Allscripts, Epic, Cerner, Meditech, and the rest typically give *application analysts* a starting point (think LEGO building blocks, if you will), and these building blocks can be assembled, or *built*, to function in any number of ways.

Security build is, for instance, application access designed for a registered nurse that gives the nurse access to do exactly what a nurse *should* be able to do, *not* what a physician should be able to do—optimized with the buttons and tools that a nurse should have in your organization.

Whether your security analysts are building (new implementation) or supporting your EMR system, you will have people who are charged with ensuring that the application complies with the build and access standards decided on by your organizational stakeholders. These application security analysts will be the backbone of your project or your operational support team and can make or break your team.

Note A word to the wise: although there are many theories about staffing and support for projects and operations, I cannot stress enough the importance of hiring the right people for these key positions. The indicators that follow, although not foolproof, will certainly improve your chances of staffing your team with the right people. Key words to keep in mind when hiring are *smart*, *driven*, *goal-oriented*, and *analytical*.

The ideal application security analyst should understand the clinical workflows, but doesn't need to have a clinical background. Key strengths of the analyst are:

- **Analytical:** This is an easy one for people to throw out in an interview: "I'm an analytical person." What is more important is the ability to demonstrate how the analyst's analytical skills have solved problems in the past. You will want to see how the analyst has used these skills in conjunction with the advanced functions of standard tools (such as Microsoft Excel) to solve specific problems.

- **Solution implementer:** You will want to be sure that the analyst can take requirements from the abstract, restate them to a customer, and translate them into a deliverable. None of these are easy tasks, and it is doubly challenging to blend the interpersonal and problem-solving elements successfully.
- **Task-oriented:** Your analyst will have many, many tasks and subtasks to complete to build a secure, efficient system for the end-user. If the analyst cannot stay on task, you will run into problems.
- **Successful:** While you don't need someone who has already achieved every one of their goals, you would do well to choose analysts who have an established pattern of setting their sights on goals and achieving them repeatedly.

You can perhaps find a very personable employee in your organization who has done well in several other positions, but an agreeable person who "works well with others" does not necessarily make a good application security analyst (or an application analyst of any sort for that matter—that's free advice for my non–privacy-and-security counterparts out there).

The EMR Security Team

Your EMR will probably need a team of individuals charged with supporting all aspects of EMR security, including, but not limited to, identity and access. A typical team will include some of the following positions:

- **Security lead/security coordinator:** This person is typically charged with coordinating the work of the various application security analysts, account provisioning analysts, and other related support staff. A thoroughly technical worker is required here, but management and people skills are also requisite.
- **Provisioning and support staff:** Although this role might fall to the help desk (or perhaps be entirely automated), some teams will have employees responsible for provisioning accounts and triaging access-related issues. These are normally midlevel technical support staff.

Note The security team for an Epic EMR install will often include a Provider (or SER) lead, who is tasked with maintaining the provider records that are linked to user records. These are not security-related but peripherally affect access and are essentially related to identity. This position is vital to the security team and is truly more of a "data manager" position.

The Security Workgroup

Your EMR support or project team will need a cross-functional group of analysts who represent various parts of the clinical and business applications. To build a cohesive and secure application, you must communicate. The *security workgroup* will be the mechanism for communication among your team members.

How often you meet will be up to you, but you will certainly need to document your work and coordinate your efforts. Your workgroup will certainly be tasked with following organizational project plans and can expect to work with your security stakeholders.

The Security Stakeholders

This group name, *security stakeholders*, is rather generic, but the group itself should not be theoretical. You must have a formally constituted group of stakeholders charged with deciding how the organization will interpret the mandates of HIPAA and the HITECH Act.

HIPAA states that the covered entity must demonstrate how it arrives at its privacy and security practices and how it formalizes accountability for processes and practices. This means a governing body.

What you decide to call this group of people and who is involved are up to your organization. Perhaps it consists of your CISO, director of nursing, director of HIM, compliance officer, and security coordinator. Maybe it's just your CISO and corporate compliance director—though I hope not! The bottom line is that you have to have a group in charge, and you must document the decisions made by this group.

Onward

What is important is that you have assembled a team, you understand your mission (namely, a secure application), and everyone has a voice in the process. Not everyone will be at the table every step of the way, but you need to have your team assembled, and each person needs to understand just how important their role is in ensuring the success of creating a privacy and security program built around the EMR.

When you have the right people at the table, you can begin the tough but worthwhile work ahead of you.

CHAPTER

5

Sifting through the Wreckage

The Security Audit

War is mainly a catalogue of blunders.

—Winston Churchill, The Second World War

Perhaps my parents thought they had a budding architect or engineer on their hands, I'm not sure, but I remember the birthday present quite well. I was probably 10 years old, and as soon as I opened the Erector construction set with all of its seemingly millions of pieces, I couldn't wait to dive in.

After opening another gift or two, a round of "Happy Birthday," and a piece of birthday cake, I was busy surveying everything that the box contained. It wasn't long before I was bolting pieces of metal together, certain that I was going to be able to build the most magnificent contraptions and structures imaginable.

What I soon realized was that the best intentions, even when coupled with some pretty solid creativity, weren't going to lead to a magnificently-Erected anything.

There were lots of pieces and there were some designs that one could follow, but before I was going to be able to dive in and create anything unique, something that I could call my own, I needed to understand how things were done in Erector world. There was an established pattern.

There were designs that led to certain creations. Perhaps there were better ways of doing things, but unless I took the time to understand what I had sitting in front of me, and how things worked (or were supposed to work), I wasn't going to have much success building something new or something better.

When we are presented with something new, we are often inclined to dive in headfirst. A birthday present, a new car, a new piece of technology, or a new project—we are tempted to say, "Let's hit the ground running!"

But as they say, discretion is the better part of valor. To stop, survey what is sitting in front of you, and ensure that you understand all of the pieces before proceeding is certainly the best path forward.

What Are We Waiting For?

We often like to react and "do something" for the sake of securing information assets, but we would do well to take a step back and understand that efforts, if not organized and deliberate, can often be counterproductive.

You can, for instance, require password changes every week, but if your users are permitted to set their passwords to "cat," "dog," or "password," then you are probably just spinning your wheels!

It is important to understand what you have sitting in front of you before you go about the business of planning change and transformation. Without a solid understanding of the core issues and business practices that affect security and privacy, it is pointless to apply patches and bandages, hoping that some effort is better than none.

The Dreaded "A" Word

Before starting down the road of auditing current practices, you have to come to grips with what a security audit is and what it isn't. You've already determined that a good baseline is required before you can make any method out of the madness.

The results of an audit (the work product) will become the toolkit that will act as the foundation of the rest of the work that you have to accomplish in securing the medical record.

With this in mind, it is helpful to understand that as soon as someone begins to investigate current practices in your organization as part of an audit, guards will go up, people will become defensive, and it is possible that the information you need won't be easy to find. A deficient practice is, after all, nothing to be proud of.

What you need to understand before an audit is that it will often uncover deficient practices that came into use under various conditions: those were initially not recognized as deficient; those that were known risks but could not be addressed due to lack of staffing or funding; and those with known flaws that were condoned for the sake of offsetting goals.

Risks are introduced or accepted for any number of reasons, and the purpose of an audit is primarily to document what exists—not the political, practical, or technical reasons behind each risk. When the people you are working with understand that your goal is not to back people into corners, put jobs at risk, or come out on top in a battle to unearth organizational secrets, your job will be much easier.

What's Your Pitch?

Depending on your role in the process of securing the EMR system, you could be the one doing the security audit or risk assessment (as distinguished in subsequent sections), or you might have delegated an appropriate representative from inside or outside of the organization to accomplish the task.

Note The *security risk assessment* is something that helps an organization understand its risks in regard to potential effects. In addition to being an extremely helpful tool in the audit process, it is a requirement in the first stage of meaningful use attestation. Not only must you complete a risk assessment, you must remediate any deficiencies found in a number of key attestation areas. We cover these core areas in more detail later.

Regardless of who is doing the audit, the goal is twofold:

- To complete the audit with as much cooperation from your staff as possible.
- To have a final product that will assist in the process of securing the EMR system.

The message that needs to be conveyed to the employees in the organization who have a stake in securing the privacy and security of patient data needs to be consistent and in keeping with your stated goals.

Whether you are establishing contact via phone or via email, establish your script, and stick to it:

> *Hello, my name is _____, and I am working with the _____ department to understand our current processes as they relate to patient data privacy and security. Every organization has some areas for improvement, and we understand this; we're just hoping to understand what we do now so that we can factor this into our future workflows. I look forward to working with you to get a better understanding of the part that you play in this important task.*

As soon as you contact one person about the needs related to your audit, your colleagues are going to start talking. "So and so called me today and asked me about _____ . Do you know anything about this?"

If your message is clear and consistent, and you ask the same thing of everybody, there will be little suspicion about your intent. People will not think that you are out to sabotage, dig up dirt, or put your nose where it doesn't belong. Establish from the beginning that your goals are the same as your colleagues'—excellent customer service and patient care— and assure them that you are on the same team.

The last thing someone wants is a cold call with requests for information that seem to be getting at something unspecific but foreboding. When this happens, expect guards to go up and the information you receive to be less than helpful.

Who Is Who?

In the previous chapter we spoke about the need to assemble a team to address privacy and security concerns. In the process of auditing your security practices, you will want to be similarly thorough in reaching out across the organization, but the people who will be able to help you answer your questions about security practices will not necessarily be the same ones who will serve on your cross-application/interdisciplinary team to address security concerns.

With this in mind, it is important to know your audience before you reach out with your message and start gathering data.

Note As you begin to establish contacts in your organization, a key aspect of privacy and security is *identity*. Your human resources management office will become an invaluable ally in your attempts to understand the people in your organization, and you would do well to establish good working relationships with key managers in HR as well as your HR information systems (HRIS) administrators.

Breaking it Down

Don't overthink the process just because you are dealing with a digital system. Some of the stakeholders in the privacy and security process are quite separate from the world of IT, and they will be the ones with the answers to your questions in many cases. Let's take a look at some of the functional areas that will help you in the process of your security audit.

- **Physical security/special police:** Although you might overlook the folks who often occupy the basement office or provide a daunting presence in the Emergency Department on busy weekend evenings, it would be a mistake to overlook your security office in the process of your security audit. They can answer questions about the pre-employment security screening, background checks, badge access standards, nonstandard employment termination procedures, physical safeguards around computer equipment and more.
- **Human resources**: The folks in your HR department will be able to assist you with everything from the onboarding process (when a potential employee is considered a "hire"), pre-employment hiring requirements, and processes that might exist between your HR/HRIS division and the IT department.
- **Training**: The training department can help you understand the steps that you take to ensure that employees are trained on technologies, regulations, standards, and corporate policies as they relate to privacy and security. The training program typically has a role in the onboarding of new employees as well as continuing education of existing employees.
- **Risk management and corporate compliance**: The risk management and corporate compliance office is your go-to source for all matters pertaining to how you should be operating and what organizational policies dictate. Their job is to ensure that the organization adheres to the myriad complex regulatory standards and requirements that each healthcare organization is obliged to follow.

- **Internal audit**: Your internal audit office staff is charged with investigating how operational employees are doing their jobs and whether they are performing according to established guidelines or best practices. The internal auditors are frequently able to help you in your attempts to understand current practices in the organization.
- **Legal affairs**: The legal department will be able to provide you with guidance related to what is permitted from a legal standpoint within your organization. Certainly you can do something one way, but that might be entirely inappropriate from a legal standpoint—it is good to have a firm grasp on these issues when grappling with process and practice. Get to know the employees in your legal department, and ask them when you encounter gray areas that require clarification.
- **Health information management**: The HIM office is uniquely positioned in the organization to blend the complex worlds or regulatory compliance and information technology—how the system treats the digital data, transmitting it from one provider to the next, and from one organization to the next, is the domain of the HIM office. Ensuring that data is correct, that demographic information is accurate, and that overall system integrity is maintained is not a small job, and it is not an easy one either.
- **Network operations**: This large, umbrella category within IT covers a host of employees from server administrators and network engineers to help desk employees. What is important here is that the network operations employees will know the processes employed relevant to data storage, access control, user accounts, remote access, and more. What might make your job more difficult is the process of trying to find out how all of these pieces fit together (or if they fit together). Often one person is charged with a task and has no knowledge of what others in the organization do when it comes to other pieces of the puzzle.

- **Information security**: Hopefully your organization will have an information security officer (or other similarly charged employee) who is responsible for all aspects of information security in your organization. The HIPAA Security rule requires such a position in each healthcare organization, and although this designee might be an office manager with yet another hat, it is important to know where the buck stops when it comes to information security at your site. This individual will, or should, be able to address matters of policy related to information security, privacy, and compliance, and to tell you what initiatives or projects are underway to address areas that are not yet mature.
- **Everyone else**: This might seem like a vague category, but it is important to understand that you need to be open to finding answers to your questions in unexpected places. Perhaps you have answered all of your process questions. You know that HR enters all of new employees into the HRIS system on the first of the month, the help desk analysts create all appropriate user accounts, and the system engineers apply all appropriate network permissions, but the question remains, "How does the end-user get credentials on the first day on the job?" In speaking to the administrative assistant one day, perhaps you find the missing link: "Oh, I get those from the help desk in an e-mail, and I write them on a sticky note, and put them on the user's monitor the night before they start." Don't leave any stone unturned, and don't assume that obvious flaws in a process will be apparent to everyone!

Note Notice the pattern here—no aspect of the privacy and security process can be considered in isolation. What one person does affects the rest, and this has ripple effects all the way down to EMR security. In the process of coordinating EMR privacy and security, it is imperative to build relationships and, above all, understand process.

Brass Tacks

With all of this information at hand, it is important to understand that the audit process will allow you to systematically evaluate data you gather, processes you observe, conversations you have, and documents/policies you review.

However, it is not enough to gather data. A lot of data, whether in a file folder or on a network file share, is still just a lot of data. An audit is not an audit until that data is collected, evaluated based on a set of expert opinions, and compiled into a report.

The purpose of the audit report is to evaluate the effectiveness of current controls and processes and further recommend a set of corrective measures to bring your organization into alignment with best practices, mitigating risk in the process.

Tools of the Trade

You might ask the question, "Where do I start?" I'm sure there are countless others right beside you wondering the same thing.

Fortunately, the road to the healthcare security audit has been well traveled over the years, and there are some tools that can be used, preventing most of us from having to reinvent the wheel, so to speak.

Let's take a look at the specific language provided by HHS:

> *The Security Management Process standard in the Security Rule requires organizations to "[i]mplement policies and procedures to prevent, detect, contain, and correct security violations." (45 C.F.R. § 164.308(a)(l).) Risk analysis is one of four required implementation specifications that provide instructions to implement the Security Management Process standard. Section 164.308(a)(1)(ii)(A) states: RISK ANALYSIS (Required). Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidential, integrity, and availability of electronic protected health information held by the [organization].*[1]

Not only does the HIPAA Security Rule require a thoughtful risk analysis for all organizations storing protected health information, but demonstrated evidence that the organization has completed such a risk assessment is required to receive federal funds under the Stage I Meaningful Use Incentives provided by the Affordable Care Act.

So much for a regulation without teeth! The link of substantial monetary funds is now directly tied to evidence that you have thoroughly evaluated your organization's processes and procedures for risks related to privacy and security. Otherwise you don't get the federal funds tied to meaningful use for EMR systems that you have implemented.

---

[1] US Department of Health & Human Services, "Guidance on Risk Analysis Requirements under the HIPAA Security Rule." Posted July 14, 2010. http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/rafinalguidancepdf.pdf

We Get By with a Little Help from Our Friends . . .

HHS is deliberately vague about what an organization is required to do to meet the requirements of a security risk assessment. They will not tell you what this has to look like, who has to perform the risk assessment, or what your final report should like.

■ **Note** Keep in mind that the risk assessment is a tool to help with the audit (the audit produces findings and recommendations). Although an audit should be independent, don't let the fact that you might be performing the audit for your organization diminish the independent nature of your work—the fact that you are working to determine the propriety of security practices in functional areas across the organization (all of these cannot fall under a single business owner) elevates the objectivity of the task at hand. If you are able to work with an independent auditor to accomplish this important task, you will be ahead of the game, learning (perhaps) more than you would from the inside.

According to HHS, you simply must complete a risk assessment, and it must thoroughly meet the requirements outlined. Unhelpful, right? Perhaps it seems so, until you do a little more digging and realize that HHS has facilitated an industry working group called the *National Learning Consortium* (NLC), which further supports a specific task force devoted to the domain of privacy and security.

This group produced a resource that is invaluable in the healthcare IT security space and an essential tool for anyone charged with privacy and security oversight. The *HIT Security Risk Assessment Tool* is a Microsoft Excel Workbook (macro-enabled) that guides the auditor through the process of evaluating privacy and security practices in the healthcare enterprise.

■ **Note** The easiest way to find the risk assessment tool is to perform a browser search for the complete phrase "HIT Security Risk Assessment Tool" (for the purposes of discussion from this point forward, we simply refer to it as the *Risk Toolkit*). When you find the link, be sure that you are downloading the Excel file from the healthit.gov website, and enable the macro content on launching the file.

There are many ways to accomplish an audit, and this book isn't about to provide a comprehensive evaluation of audit methodologies (you can read books on this topic if you are interested).

What I propose here is that the Risk Toolkit provided by HHS can be used to facilitate the audit process and get you where you need to be as you work to secure your EMR system. The step-by-step process outlined in the toolkit can help you understand the path you are traveling, and, as you begin to enter values in the workbook, you will start to see how all of the pieces fit together.

Once you ask questions, find the answers, and plug in the values, you will see where some of your risks are, where your gaps are, and what recommendations will need to be in your audit report.

Diving In

Once you have downloaded the Risk Toolkit, you'll want to familiarize yourself with the two tabs titled "How to Complete the Forms" and "Risk Guidance" (see Figure 5-1).

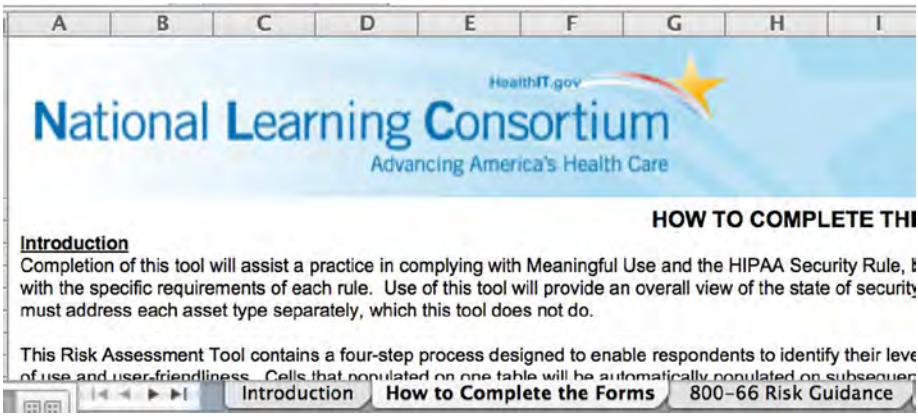


Figure 5-1. The Risk Toolkit

If you were thinking that a spreadsheet would simply provide an assortment of fields to populate with values, numbers, and data, then think again. There is a wealth of information that will help the novice auditor and the veteran alike through the process of performing a security risk assessment in the healthcare space.

You will note on the first tab that the Risk Toolkit is based on standards set forth by the National Institutes of Standards and Technology (NIST), and you would do well to familiarize yourself with these NIST standards. When you see the HIPAA rule, or other HHS document, reference a seemingly cryptic alpha-numeric value such as 164.308(a)(1)(ii)(A), this is not an attempt to obfuscate what could have been stated simply, but a point of reference to information security standards set forth by NIST.

HHS has tried *not* to reinvent the wheel when it comes to implementing privacy and security standards, referring instead to what the information security industry has already accepted as normative.

When you see these references, venture out to the NIST website and do a little more reading. The better equipped you are with the data about why standards are being implemented (that often lead to changes people resent or resist), the better equipped you will be in your attempts to enlist allies in support of your security program.

Four Steps

The Risk Toolkit outlines a logical flow for completing the risk analysis, beginning with some preparatory steps and moving through a three-step process that leads eventually to a concise risk register that can be used as the basis for an audit report.

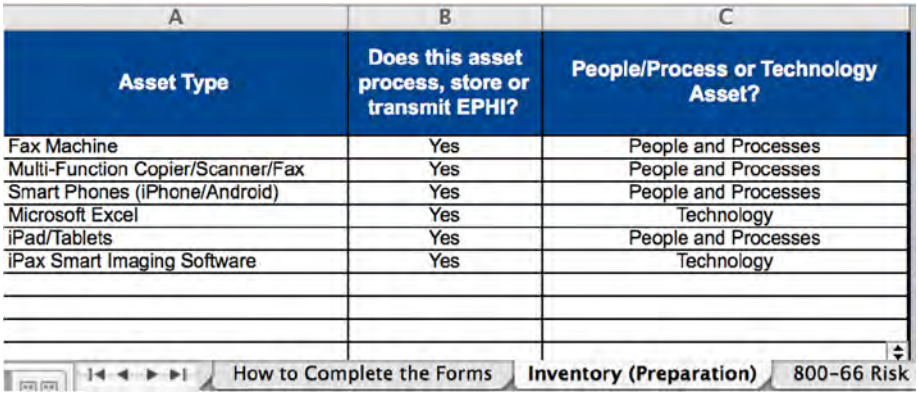
The Preparation Phase and Inventory

The Preparation Tab of the Risk Toolkit is listed as optional, but I would suggest that you do not overlook this important step in the audit process. What you will gain here is invaluable to the risk assessment process, and you will find that this Inventory of Assets will be a point of reference you will use repeatedly in the future.

The questionnaire is straightforward and requires you to take an inventory of all information assets in the organization with a particular mind to the question, "Does this device or software package enable or facilitate the storage or transmission of ePHI?"

In other words, is digital protected health information stored or transmitted by means of this asset? If the answer is yes, then the organization must give an account for how it is managing that information asset.

Let's take a look at some possible entries in the Inventory of Assets tab of the Risk Toolkit. In the example that appears in Figure 5-2, we've begun the process of entering various information assets that the organization should consider in the development of its security program.



A	B	C
Asset Type	Does this asset process, store or transmit EPHI?	People/Process or Technology Asset?
Fax Machine	Yes	People and Processes
Multi-Function Copier/Scanner/Fax	Yes	People and Processes
Smart Phones (iPhone/Android)	Yes	People and Processes
Microsoft Excel	Yes	Technology
iPad/Tablets	Yes	People and Processes
iPax Smart Imaging Software	Yes	Technology

How to Complete the Forms | Inventory (Preparation) | 800-66 Risk

Figure 5-2. Inventory of Assets

Notice that the list includes everything from company-issued (or perhaps personally owned) smart phones to spreadsheet software. The devices, the things that people use, are placed in the "People/Process" category, and the software that simply has the capability to store data is placed in the "Technology" category.

This inventory process should be carried out until every asset or type of asset is listed and categorized so that they can be included in your security program. Note that our primary concern is with the security of the EMR system; while an EMR might have been an island at one point, smart phones, tablets, and fax machines are all integrated into the fabric of these systems. There is no longer a clear line between a device and the EMR, and without a comprehensive picture of what kind of assets an organization is dealing with, we can't get a handle on where patient data begins and ends.

Step 1: The Screening Questions

The first section after the asset inventory is titled "Screening Questions," and it walks you through a set of core questions related to privacy and security practices in your organization.

As you think back to all of the departments and organizational contacts that we listed at the beginning of this chapter, you will see how these various functional areas come into play at this point in the risk assessment. You will be asked to answer questions about the person charged with the duties of security officer, the processes employed for terminations, the process used for pre-employment screenings, controls for secure areas, and more.

You will be asked to evaluate each of these domains with a response of "Addressed," "Not Addressed," or "Partially Addressed."

To the right of your response, you will be offered an opportunity to comment on the response with information that will be helpful in your final report. For instance, in Figure 5-3, when asked in question 1.1, "Has your organization formally appointed a central point of contact for security coordination?" since we answered yes, it is helpful to list the name of the chief information security officer and the date he was appointed.

	Topic	Question	Response	Threat Vulnerability Statement	People/ Processes	Technology
1. Security Program						
1.1	*Roles & Responsibilities*	[1.1] Has your organization formally appointed a central point of contact for security coordination? a) If so, whom, and what is their position within the organization? b) Responsibilities clearly documented? i.e. job descriptions, information security policy	Addressed	Management has not defined responsibilities for the information security program. [TVS001]	James Smith assigned as Chief Information Security Officer (CISO) on 12/15/2011.	N/A
1.2	*External Parties*	[1.2] Do you work with third parties, such as IT service providers, that have access to your patient's information? a) Does your organization have Business Associate agreements in place with these third parties? i.e. REC, IT Vendor, EHR Vendor, etc. b) If not, what controls does your organization have in place to monitor and assess third parties? i.e. Logging of VPN connections, EHR logs, etc.	Not Addressed	Security breaches occur when dealing with third parties due to a lack of security considerations in the related third party agreement. [TVS002]	Business Partner Agreements not signed/filed - need to address as soon as possible.	
2. Security Policy						

How to Complete the Forms | Inventory (Preparation) | 800-66 Risk Guidance | Practice Summary | Screening Questions (Step 1) | People and Processes (Step 2a) | Technology (Step 2b)

Figure 5-3. Question 1.1 response examples

To complete this section properly and thoroughly, you will need to read through each section and question and determine who (from your list of security contacts) can help you determine the answer. Once you have organized these questions, and assigned a subject matter expert to help you address the issue, you are ready to begin the process of gathering data.

Walk though the series of questions, responding to each query with an appropriate response and comment(s) to each of the following security domains:

1. Security Program
2. Security Policy
3. Risk Management and Compliance
4. Training and Awareness
5. Personnel Security
6. Physical Security

7. Network Security
8. Logical Access
9. Operations Management
10. Incident Management
11. Business Continuity Management

Once you complete the answers to each query in this section, you can move on to Step 2.

Step 2a: People and Processes

The second section that you will need to complete is broken down into two sections, the first of which is titled "People and Processes." Here you will be asked to evaluate the human-related processes for what the Risk Toolkit calls "Effectiveness of Control." In essence, you are making a judgment call regarding the effectiveness of your controls, or lack of controls, related to a given security process or discipline.

In the example in Figure 5-4, you will notice that the column titled "Existing Control" pulls data that you previously entered in step 1. When you begin to populate the values for "Existing Control Effectiveness" in this phase, the logic built into the workbook will start to evaluate your risk ratings in regard to the domains and disciplines (or processes) being evaluated.

			Perform Control Analysis		Exposure	Assess Risk		
Asset Management Category	Threat-Vulnerability Statement	Recommended Control Measures	Existing Control	Existing Control Effectiveness	Exposure Potential	Likelihood	Impact	Risk Rating
Security Program	Management has not defined responsibilities for the information security program. [TVS001]	All information security responsibilities are clearly documented . This is to ensure timely, safe and effective handling of all situations, administration user accounts- including additions, deletions, and modifications. [RCM001] - Ensure responsibilities are formalized within	James Smith assigned as Chief Information Security Officer (CISO) on 12/15/2011	Effective			High	
Risk Management & Comoliance	Information around risks and related control options are not presented to management before management decisions are made. [TVS004]	Risk assessments are conducted to identify, quantify, prioritize and manage risks. The prioritization is accomplished by creating and using criteria for risk acceptance and objectives which are important to the organization. [RCM004] - Ensure this risk assessment is accurate with	- REC helping to start the risk assessment process by using this spreadsheet as a foundation for the risk assessment as well as risk management plan. - No prior risk assessments	Not Effective	High	Likely	High	Medium
Risk Management & Compliance	Legislative, statutory, regulatory or contractual obligations related to security are violated due to lack of controls. [TVS005]	Controls, which are applicable to each situation, have been applied to avoid violations of any legal obligations (e.g. statutory, regulatory, or contractual), and of any security requirements. Access controls could be door locks or computer passwords, while other controls could be	- Working with the REC helps to identify new laws and regulations due to the training and guidance with the REC team - State breach guidance also	Effective		Not Likely	High	Low
Network Security	Technical vulnerabilities are exploited to gain inappropriate or unauthorized access to information systems due to lack of controls for those vulnerabilities	Timely information about technical vulnerabilities of information systems being used is obtained, the organization's exposure to the vulnerabilities is evaluated and appropriate measures are taken to address the associated risk. [RCM013] - Vulnerability testing should be performed regularly to obtain information bout technical	- No vulnerability testing has been completed.	Not Effective	High	Very Likely	High	High

How to Complete the Forms | Inventory (Preparation) | 800-66 Risk Guidance | Practice Summary | People and Processes (Step 2a) | Screening Que

Figure 5-4. People and Processes

You will see the far right column of your workbook begin to light up with greens, reds, and yellows depending on how you answer these questions. At this point in the process you are starting to see how your information gathering leads to a meaningful analysis, which can then be conveyed into findings in your audit report when all is said and done.

Once you have completed everything under the People and Processes section, you can move on to the Technology Section.

Step 2b: Technology

The next section covers technologies instead of human-related processes and assigns a logically based risk rating to teach technology (or domain) based on the answers that you previously supplied.

The snapshot in Figure 5-5 shows only part of the data rendered in this section, but it gives you an idea of what you will be seeing as the Risk Toolkit provides you with insights into security risks in your organization.

A	E	F	G	I	L
Asset Management Category	**Existing Control Effectiveness**	**Exposure Potential**	**Likelihood**	**Impact**	**Risk Rating**
Risk Management & Compliance	Not Effective	High	Likely	High	Medium
Personnel Security	Effective	Medium	Not Likely	High	Low
Physical Security	Partially Effective	High	Very Likely	High	High

Figure 5-5. Technology risk ratings

Step 3: Findings and Remediations

The final section collates the data that you provide along with the risk ratings generated by the workbook to offer a comprehensive listing of findings. The top of your Findings and Remediations tab will provide you will a snapshot of risks that you will need to address (see Figure 5-6).

Number of High Risks	6
Number of Medium Risks	5
Total Number of High and Medium Risks	11

Figure 5-6. Risks to address (summary)

Notice that the risks that were rated "Low" are not included here in the summary findings tab. You will not want to gloss entirely the low-risk findings (some of these are areas that an organization will certainly need to improve on). The reality is that low-risk security concerns often fall into categories that should be addressed but are unlikely to happen, and are therefore given little to no weight when it comes to a security program.

Everyone understands that resources are limited, and in the case of a security risk assessment, this is no exception. There just isn't time to address every potential concern.

The goal is to look at those domains where the risk and impact are substantial (causing harm to the organization or the customers you serve) and remediate and address those as quickly as possible.

Below the summary of medium and high risks, you will find detail related to each of these risks (see Figure 5-7). Your notes, as well as information that will help you in the remediation process, are included here. This section can be used as a task list of action items from which to work after the audit is complete.

Risks Found (High and Medium Only)	Risk Rating	Existing Control Measures Applied
People and Processes		
Information around risks and related control options are not presented to management before management decisions are made. [TVS004]	Medium	- REC helping to start the risk assessment process by using this spreadsheet as a foundation for the risk assessment as well as risk management plan. - No prior risk assessments conducted
Technical vulnerabilities are exploited to gain inappropriate or unauthorized access to information systems due to lack of controls for those vulnerabilities. [TVS013]	High	- No vulnerability testing has been completed.

Figure 5-7. Details on risks

Finally, take note that there are fields where you can highlight the steps that you plan to take to remediate the risks discovered, as well as identify the primary owner who will be addressing these risks (Figure 5-8). The target date for remediation is added so that you can associate goals and follow-up with the business owner who has been tasked with addressing the risk.

Owner	Remediation Steps	Target Date
James Smith - CISO	Develop a Risk Management plan, and present to leadership for approval. Then communicate this to business owners and operational staff.	**4/9/15**
Mary Williams - Security Architect	Develop a comprehensive patch management program, and monitor for effectivness.	**11/13/14**

Figure 5-8. Remediation steps, owners, and target dates

Putting It All Together

Once you have completed the risk assessment, you will have something in your hands to help you address EMR security, but you still have to put the pieces together.

Perhaps you gleaned insights during your conversations that weren't thoughtfully displayed in the Risk Toolkit. You'll want to cull those out and put those in narrative form in your *audit report*. Remember that your opinion and findings are the work product of your research and the data that you gathered. You can't require your organization to take action on each of your recommendations, nor can you make everyone agree with each of your opinions, but when you take the time to do the work an audit entails, you owe it to your employer and the patients you serve to put the pieces together in the end.

The Risk Toolkit and all of the detail from it should be included in your final audit report, and you can include any number of supplemental materials that you think might be helpful to those who will use the report. External auditors, security personnel, future employees, and others will appreciate the detail you include, as it will become a benchmark against which to gauge progress.

A Final Note on the Meaningful Use Risk Assessment

As discussed in this chapter, to "attest" to meaningful use of your EMR system, you must demonstrate that you have completed a risk assessment, and the Risk Toolkit meets this requirement.

However, meaningful use requirements are quite specific in regard to controls (and tests for these controls) within your network and in your EMR system. With this in mind, to comply with this aspect of the Meaningful Use Requirement (Stage I), you will need to follow the procedures that follow and include these EMR-specific test results with your risk assessment findings.

The following eight "Meaningful Use Quality Measures" are security specific, and are listed here with their corresponding logical measure name. Included with each of these measures is a corresponding NIST test document that can be followed to demonstrate compliance:

1. **MU 170.302.q, Access Control**: This quality measure is related to the control of unique users to appropriate activities in the EMR system. (Test procedure: http://healthcare.nist.gov/docs/170.302.o_AccessControl_v1.0.pdf)

2. **MU 170.302.p, Emergency Access**: This quality measure is related to the availability of patient data from the EMR during unplanned downtime. (Test procedure: http://healthcare.nist.gov/docs/170.302.p_EmergencyAccess_v1.0.pdf)
3. **MU 170.302.q, Automatic Logoff**: This quality measure is related to EMR system's ability to automatically terminate inactive sessions to prevent unauthorized access to patient data. (Test procedure: http://healthcare.nist.gov/docs/170.302.q_AutomaticLogOff_v1.0.pdf)
4. **MU 170.302.r, Audit Log**: This quality measure is related to the EMR system's ability to record transaction data related to time, date, patient ID, and user ID. (Test procedure: http://healthcare.nist.gov/docs/170.302.r_AuditLog_v1.0.pdf)
5. **MU 170.302.s, Integrity**: This quality measure relates to the integrity of data when exchanged between your EMR system and another party's EMR, ensuring that the data is not altered as it traverses from one system to the other. (Test procedure: http://healthcare.nist.gov/docs/170.302.s_Integrity_v1.0.pdf)
6. **MU 170.302.t, Authentication**: This quality measure is concerned with the manner in which accounts are permitted to access or blocked from accessing the EMR system based on account settings. (Test procedure: http://healthcare.nist.gov/docs/170.302.t_Authentication_v1.0.pdf)
7. **MU 170.302.u, General Encryption**: This quality measure is concerned with the encryption of data in the various components that store ePHI within the EMR system. (Test procedure: http://healthcare.nist.gov/docs/170.302.u_GeneralEncryption_v1.0.pdf)
8. **MU 170.302.v, Encryption HIE:** This quality measure is concerned with the end-to-end encryption of data in a health information exchange (HIE). (Test procedure: http://healthcare.nist.gov/docs/170.302.v_EncryptionHIE_v1.0.pdf)

You will need to test your EMR system for these quality measures and include your test process and findings with your risk assessment. In certain domains such as encryption HIE and integrity, it might be sufficient to supply thorough documentation (line and verse) from your vendor in lieu of testing these technologies on your own.

Armed and Ready?

To this point, you have been covering a lot of background, gathering data, and getting your ducks in a row. Again, I cannot stress enough the importance of having a plan before diving in to do the actual work.

With this in mind, you are almost ready to start working with some solutions. But there is a little more legwork to do. The next and final chapter in Part 2 will cover the last steps that you need to take before diving into the steps of actually securing the EMR.

Further Reading

HealthIT.gov, "How to Implement EHRs: Step 2: Plan Your Approach," HealthIT.gov, http://www.healthit.gov/providers-professionals/ehr-implementation-steps/step-2-plan-your-approach.

HHS, "Guidance on Risk Analysis Requirements under the HIPAA Security Rule," HHS.gov, July 14, 2010, http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/rafinalguidancepdf.pdf.

HealthIT.gov, "About the Health IT National Learning Consortium," HealthIT.gov, http://www.healthit.gov/providers-professionals/national-learning-consortium

Office of the National Coordinator for HIT, "Guide to Privacy and Security of Health Information, Chapter 4: Integrating Privacy and Security," HealthIT.gov, http://www.healthit.gov/sites/default/files/pdf/privacy/privacy-and-security-guide-chapter-4.pdf.

T, U, V, W

X, Y, Z

HEALTHCARE INFORMATION PRIVACY AND SECURITY

REGULATORY COMPLIANCE AND DATA SECURITY IN THE AGE OF ELECTRONIC HEALTH RECORDS

Bernard Peter Robichau

Apress®

Healthcare Information Privacy and Security: Regulatory Compliance and Data Security in the Age of Electronic Health Records

ISBN-13 (pbk): 978-1-4302-6676-1

ISBN-13 (electronic): 978-1-4302-6677-8

Publisher: Heinz Weinheimer
Acquisitions Editor: Jeff Olson
Developmental Editor: Robert Hutchinson
Editorial Board: Steve Anglin, Mark Beckner, Ewan Buckingham, Gary Cornell, Louise Corrigan, James DeWolf, Jonathan Gennick, Jonathan Hassell, Robert Hutchinson, Michelle Lowman, James Markham, Matthew Moodie, Jeff Olson, Jeffrey Pepper, Douglas Pundick, Ben Renow-Clarke, Dominic Shakeshaft, Gwenan Spearing, Matt Wade, Steve Weiss
Coordinating Editor: Rita Fernando
Copy Editor: Laura Poole
Compositor: SPi Global
Indexer: SPi Global
Cover Designer: Anna Ishchenko

Distributed to the book trade worldwide by Springer Science+Business Media New York, 233 Spring Street, 6th Floor, New York, NY 10013. Phone 1-800-SPRINGER, fax (201) 348-4505, e-mail orders-ny@springer-sbm.com, or visit www.springeronline.com. Apress Media, LLC is a California LLC and the sole member (owner) is Springer Science + Business Media Finance Inc (SSBM Finance Inc). SSBM Finance Inc is a Delaware corporation.

For information on translations, please e-mail rights@apress.com, or visit www.apress.com.

Apress and friends of ED books may be purchased in bulk for academic, corporate, or promotional use. eBook versions and licenses are also available for most titles. For more information, reference our Special Bulk Sales–eBook Licensing web page at www.apress.com/bulk-sales.

Any source code or other supplementary materials referenced by the author in this text is available to readers at www.apress.com. For detailed information about how to locate your book's source code, go to www.apress.com/source-code/.

Apress Business: The Unbiased Source of Business Information

Apress business books provide essential information and practical advice, each written for practitioners by recognized experts. Busy managers and professionals in all areas of the business world—and at all levels of technical sophistication—look to our books for the actionable ideas and tools they need to solve problems, update and enhance their professional skills, make their work lives easier, and capitalize on opportunity.

Whatever the topic on the business spectrum—entrepreneurship, finance, sales, marketing, management, regulation, information technology, among others—Apress has been praised for providing the objective information and unbiased advice you need to excel in your daily work life. Our authors have no axes to grind; they understand they have one job only—to deliver up-to-date, accurate information simply, concisely, and with deep insight that addresses the real needs of our readers.

It is increasingly hard to find information—whether in the news media, on the Internet, and now all too often in books—that is even-handed and has your best interests at heart. We therefore hope that you enjoy this book, which has been carefully crafted to meet our standards of quality and unbiased coverage.

We are always interested in your feedback or ideas for new titles. Perhaps you'd even like to write a book yourself. Whatever the case, reach out to us at editorial@apress.com and an editor will respond swiftly. Incidentally, at the back of this book, you will find a list of useful related titles. Please visit us at www.apress.com to sign up for newsletters and discounts on future purchases.

The Apress Business Team

For my dear wife, Christine, who is my constant motivation to strive toward integrity and honor, which is, in the end, the reason for this book.

Foreword

Thoughts on Privacy and Security from a Medical Professional

For those of us who have been on the journey to create an electronic patient medical record, we first must recognize that we are still in our infancy. There is much work to do. Our goal is noble and achievable. We will create one patient record, which all caregivers use. It will be up to date, it will contain all "knowable" information about the patient, and it will be available to all at the point of care—be that the hospital ER, the doctor's office, an ER across the country, or the patient's home. But we must be ever mindful that in our effort to codify the information, we run the risk of losing the rich story of the patient.

Throughout my medical training as well as my 25 years of medical practice, I have been taught by my professors and patients that, if I listen carefully, the patient will tell me what is wrong with them. Yes, I will order some testing, but 90 percent of the time the patient will give me the diagnosis if I just listen to their *story*. My test serves to confirm what I already know to be true. How very precious and sacred is that story! It must be captured in the medical record so that the physicians and nurses who help us deliver the medical care are enlightened by the story.

What's this got to do with the book you have in your hands? Everything! The story will contain very personal and private information that deserves to be kept that way. Only those individuals who are caring for a particular patient should have the privilege of seeing her information.

What Peter Robichau has given you in this marvelous book is not only a great plan for the organization of your EMR security, but also a mindset to approach the data and its care. Follow its principles and your organization will sleep well at night. Ignore some steps, and your organization risks great peril and embarrassment, as well as financial punishment.

Peter points out the importance of regular self-audits as well as preparing for the "surprise letter" from the agency announcing an upcoming external audit. I could not agree more with this practice. In my hospital we refer to this as *systems assurance*—we know where the data is, who has access to it, how we grant them access, and we audit the process regularly to verify its integrity.

Note You really must plan for that audit. With all the *meaningful use* dollars the government has given out, do you really think they are going to sit back and see how this big experiment works? No, they will be demonstrating that they are clawing back as many of those billions of dollars as possible.

Read this book in its entirety. Yes, you will go back to review chapters as you work through your project, but you must have the framework and see the total picture to ensure you have it *right*.

Special emphasis needs to be placed on Chapter 13. As our information becomes more mobile—picture the doctor accessing patient information on her iPhone while at dinner—the importance of "*Training the Masses to Respect the System*" is crucial. For if you have done everything else right but have not educated your staff on how to keep the data private, you will have lost!

You will enjoy this book. It is well written and engagingly sprinkled with personal accounts that make it interesting.

My favorite politician, Sir Winston Churchill, is said to have said: "The Americans will get it right, but only after they have tried everything else." Don't be one of those who try everything else first. Follow the guidelines in the book; you will be glad you did.

Enjoy!

Michael Clore Sanders, M.D., F.A.A.F.P.
Chief Medical Information Officer
Flagler Hospital
Saint Augustine, Florida

About the Author

Bernard Peter Robichau is the owner and chief security consultant at Category 3 Partners, LLC, on contract with a large academic medical system in the mid-Atlantic. He is a Certified Professional in Health Information Management Systems, an Epic Certified Security Coordinator, and a Project Management Professional credential holder. He has nearly two decades of experience in the IT field with an emphasis on information security. Robichau has served as a security officer in the public sector and as a member on various information security advisory committees. He has presented on the topic of information security in public forums. For information related to this book, see its dedicated site at `robichau.com`.

Acknowledgments

Keith, who showed me how to lead well.

Charles, who taught me the importance of stepping up my game.

Jeanne, who cared when it mattered most and taught me to do the same.

Heather, who led with grace in the midst of many storms.

Allison, for showing me what great management looks like.

Michael and Maryanne, for always bringing integrity and excellence to the patient care process.

Martha, Justin, Jonathan, Judy, Mike, Chioma, Andrew, and *all* of the other analysts who raise the bar high.

Tim, for holding down the fort.

Paul and Gerald, for being simply brilliant and giving me something to strive toward.

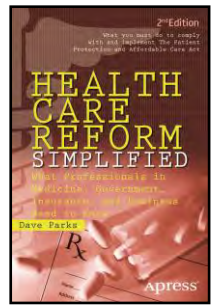
Rick, Paul, Dane, Matt, and Phuong, for being the best team members ever.

Robert and Rita, for their exceeding patience and grace.

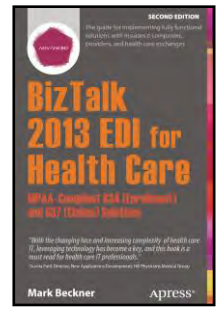
And finally, Mom, Stephan, Nadia, Marina, and Isaac, who are long-suffering and loving toward me always, even when I don't deserve it.

Other Apress Business Titles You Will Find Useful

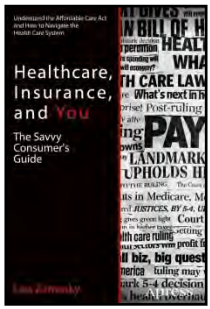
Sensor Technologies
McGrath
978-1-4302-6013-4



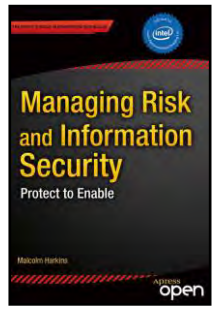
Health Care Reform Simplified, 2nd Edition
Parks
978-1-4302-4896-5



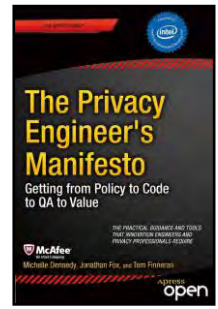
BizTalk 2013 EDI for Health Care
Beckner
978-1-4302-6607-5



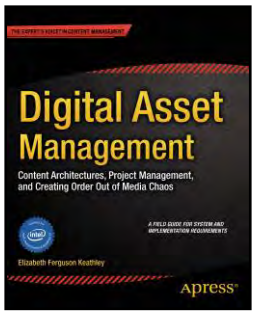
Healthcare, Insurance, and You
Zamosky
978-1-4302-4953-5



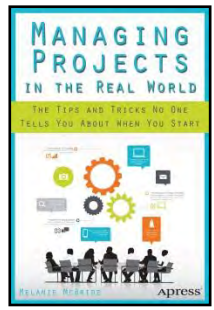
Managing Risk and Information Security
Harkins
978-1-4302-5113-2



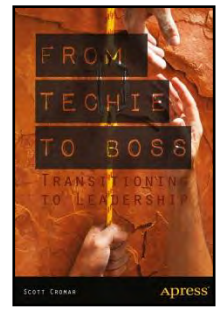
The Privacy Engineer's Manifesto
Dennedy/Fox/Finneran
978-1-4302-6355-5



Digital Asset Management
Keathley
978-1-4302-6376-0



Managing Projects in the Real World
McBride
978-1-4302-6511-5



From Techie to Boss
Cromar
978-1-4302-5932-9

Available at www.apress.com