Table of Contents

Part 1: Introduction 1
Part 2: The global regulatory landscape 2
Part 3: Security and compliance pains in the healthcare industry 3
Part 4: Technical issues 5
Part 5: Operational issues 7
Part 6: Building a solid security and compliance strategy 9
Part 7: Moving forward 11
Appendix A: Sample risk analysis template 12
Appendix B: User awareness and training tips 13
Appendix C: Security policy template 14
Part 1: Introduction

From protecting patient privacy to ensuring that personal information is kept intact, global information privacy and security regulations are impacting those who work in and around the healthcare industry.

This seven-part healthcare and security guide examines the global regulatory landscape, common pain points for healthcare-based organizations, specific technical and operational security best practices, and strategies for long-term success. In addition, you’ll find checklists and templates that can save you time and maximize productivity.

You’ll also learn how to bring your healthcare business into compliance with the various regulations and create an effective information security program that lasts well into the future.
Part 2: The global regulatory landscape

Back in the day, healthcare providers had information management and security initiatives in place. Today, these initiatives are law and industrialized nations take protective measures to ensure the privacy, confidentiality, integrity, or availability of sensitive healthcare records.

Countries around the world have their unique sets of requirements to ensure healthcare-related information is kept private and secure, including:

» Canada’s Personal Information Protection and Electronic Documents Act (PIPEDA)
» The European Union’s Data Protection Directive
» Hong Kong’s Personal Data (Privacy) Ordinance
» Japan’s Personal Information Protection Act (JPIPA)
» The United Kingdom’s National Health Service directives
» The United States’ Health Insurance Portability and Accountability Act (HIPAA) and Health Information Technology for Economic and Clinical Health Act (HITECH)

Healthcare-related data breaches heard around the world

• Peterborough District Hospital in the UK had a laptop stolen that contained medical records of 1,110 patients. Source: http://bit.ly/aYGEh4
• WellPoint in the US exposed the medical records of 470,000 insurance applicants on its website for five months. Source: http://con.st/10008412
• Caritas Medical Centre in Hong Kong had a hard drive stolen that contained medical records of 3,000 patients. Source: http://bit.ly/aVbDT7

Beyond these types of federal regulations, certain states and provinces have their own laws affecting healthcare records. The reality is compliance is not an option. The vast list of regulations and how they impact healthcare providers around the world underscores the need to understand, achieve and maintain compliance.

If you conduct business in the healthcare industry—in many cases, irrespective of where your business is located—certain responsibilities and minimum standards apply and they require adherence.
Part 3: Security and compliance pains in the healthcare industry

Like businesses in many other industries, healthcare providers often struggle to do more with less. However, working in healthcare presents a unique set of challenges. For example, the heightened public awareness of health concerns creates a situation where more patients are coming in for treatment. This often makes it difficult to work efficiently.

To work more efficiently, electronic healthcare records need to be readily available and stored on many devices in different locations including laptops, removable storage, smartphones, servers and medical equipment.

Unfortunately, having information in various places creates serious information security risks and compliance gaps.

This is especially true considering the depth of sensitive information you need to gather:

- Social Security numbers, Social Insurance numbers, National Insurance numbers, etc.
- Home addresses and telephone numbers
- Personal and family health history
- Bank accounts and credit card numbers

The adoption of healthcare technologies such as electronic medical records and telemedicine is leading to an increase in systems complexity. Complexity is the enemy of security and compliance and, therefore, must be minimized and adequately managed.

Although a necessity, shared computers often create accountability issues related to security and compliance. When a data security breach occurs on a shared system, it can be difficult to determine who was involved. These information management and access control issues facilitate a broader attack surface for electronic records—a problem unique to the healthcare environment.

Working in healthcare requires operational proficiency from you and your co-workers. Also know, third party associates such as billing and diagnostics teams affect operations and how you manage and share healthcare records. If regulations and operations are not properly satisfied, you and your organization can be found indirectly liable.

The difference between security and privacy

The words “security” and “privacy” are often used interchangeably when discussing healthcare regulations. However, they are different.

Security is a process; privacy is a consequence of that process. In other words, security is a set of actions; privacy is a result of those actions.

Privacy is often conveyed as purely a legal issue, but it isn’t always. Likewise, security is often conveyed as a technical issue, but it isn’t always.

The bottom line: Security exists without privacy, but you can’t have privacy without security.
Healthcare professionals don’t want to be constrained in their work. Whether controls mandated by IT, the government, or both, the demands for an open-computing environment contradict the very core of information security and compliance. This breeds an environment of errors and oversights that can ultimately lead to data security breaches and compliance gaps.

Given that both convenience and expediency are critical in these environments, transparent security controls are a must.

Common fallacies related to healthcare security and compliance

The following are dangerous assumptions and misunderstandings related to protecting sensitive healthcare records and issues that need to be dealt with at the highest level of management within the organization:

1. “Privacy and security regulations don’t apply to us.”
2. “We don’t handle sensitive health records.”
3. “Our compliance officer handles everything – there’s no need to involve anyone else.”
4. “The last time we had an audit they didn't find anything of concern.”
5. “We have a security policy to keep our systems protected.”
6. “We’re compliant, therefore, we’re secure.”
7. “Even if we mess up, the regulators aren’t going to come after us.”
Part 4: Technical issues

The need to protect sensitive electronic health records from both external attackers and malicious insiders requires comprehensive technical controls throughout the network. If you're going to protect sensitive health records, you have to go to the level at which they reside: the endpoint.

Most security vulnerabilities that create risk or data breaches are not sophisticated. Elaborate “hacking” is not required. If someone wanted to compromise your organization’s sensitive healthcare records, they could do so with ease. They could either email the records to their personal email account, copy files to a removable storage device, or use free and simple tools to reset passwords on lost or stolen computers that don’t have hard drives encrypted. One seemingly innocuous breach can be detrimental to your business.

Security threats and vulnerabilities don’t discriminate. It doesn’t matter how large or small your business is. If you collect, process, or store sensitive healthcare records, your business could be put at risk.

Here are some common technical security vulnerabilities that affect most healthcare-related businesses:

» Lack of drive encryption for laptops and removable media
» Missing patches
» Weak operating system, application and database passwords
» Lack of content filtering and audit logging
» Insufficient malware controls for viruses, Trojans, spyware and rootkits

All of these vulnerabilities could put sensitive healthcare records in harm’s way.
Technical flaws come about, in large part, because of underlying issues and vulnerabilities, including:

» The global presence of the internet
» The evolution of the mobile workforce
» The complexity of networks, computers and applications
» Poorly written software
» The growing skill sets of attackers and malicious users
» The ease of exploitation, especially given the free and inexpensive tools available

Appendix A contains a risk analysis template to use when determining specific security and compliance risks for your business.

To ensure protection you must consider:

» Confidentiality: Healthcare records are revealed only to those authorized to see them
» Integrity: Healthcare records remain free from unauthorized or unintentional creation, modification or deletion
» Availability: Healthcare records are accessible when needed

Assuring a reasonable level of confidentiality, integrity and availability—and thus compliance—is possible if you implement the right technologies for your level of risk and specific business needs. In addition to traditional technologies such as firewalls and virtual private networks (VPNs), you can employ other technical controls to help minimize security and compliance risks, as shown in Figure 1.

Figure 1: Practical security controls to minimize technical vulnerabilities
Part 5: Operational issues

There’s a “softer” side of security and compliance that contributes to just as many, if not more, business risks. From documented policies to notices of privacy practices to consent forms for sharing healthcare-related information with third parties, operational weaknesses do not appear to be an issue. However, when you take a second look, it’s apparent that many healthcare providers still have a lot of work to do.

Common operational security issues include:

» A lack of responsibility and accountability
» Not knowing which sensitive healthcare records are stored/processed and where they’re located on the network
» Weak or nonexistent security policies and plans
» Poor training and education for users
» System maintenance and monitoring deficiencies
» A lack of ongoing security and compliance assessments

These operational weaknesses not only put sensitive healthcare records at risk, but also are the root cause of most of the technical issues outlined in Part 4.

Operational flaws come about, in large part, with:

» Poor leadership by executive management
» A lack of understanding of IT and security concepts
» A belief that all workers are trustworthy
» Increasing expectations for users to produce
» A shortage of IT and security expertise
» A lack of an established information privacy and security culture that fosters user buy-in
Operational issues also lead to business risks through threats exploiting vulnerabilities. For example, an untrained user (the threat) disables her anti-virus software (the vulnerability) to speed up her computer, which leads to a malware outbreak on the network. The same scenarios can be—and often are—carried out when dealing with patches, drive encryption and data backups.

The value of technical security controls can quickly diminish if operational issues are not addressed and dealt with appropriately.

For your business to maintain the confidentiality, integrity and availability of sensitive healthcare records, everyone involved must be held to a certain standard and made aware of their responsibilities. This is done by combining policies and processes as well as ongoing training. There are also numerous operational controls you can implement to minimize security and compliance risks, as shown in Figure 2.

**Figure 2:** Practical security controls to minimize operational vulnerabilities
Part 6: Building a solid security and compliance strategy

You can implement all the documentation and technologies in the world, but that doesn’t mean your business is going to be in compliance with healthcare privacy and security regulations. Nor does it mean that common information risks are properly addressed.

The reality of security and compliance in healthcare is that there’s nothing new, magical or mysterious. Instead, it’s about using proven best practices and—most importantly—using common sense. Focusing on these two areas will help you overcome most challenges including politics, financial constraints and lack of buy-in.

Creating a security and compliance program is not as difficult as it may seem. Following these steps will get you started down the right path:

1. Identify key individuals who have authority and can take responsibility for managing this program.
2. Perform a high-level gap analysis to compare where you are now with where you need to be according to the specific regulations you’re up against.
3. Perform an in-depth risk analysis to determine specific threats and vulnerabilities that need to be addressed, and document your findings.
4. Prioritize your specific needs.
5. Brief management on your findings.
6. Develop a budget.
7. Create the necessary policies, procedures and business processes to address your urgent and important findings.
8. Implement the proper technologies to help enforce your policies and carry out your procedures.
9. Train your users on what to do and what not to do.

To simplify your security and compliance initiatives, don’t collect and store healthcare information that your business doesn’t need. Keeping things simple can have tremendous payoffs.
Appendix B contains tips and techniques for getting the most out of your users.

Once you get past the initial phase, you can take several additional steps to maintain security and privacy:

» Patch your software
» Keep your anti-malware signatures continually updated
» Monitor your systems for unusual or malicious behavior
» Perform an annual review of your documentation to ensure it’s still appropriate
» Test your security plans to ensure they work
» Conduct ongoing awareness and training programs for users.

Global healthcare privacy and security regulations exist, which you should consider. They are:

» Comprehensiveness
» Technology neutral
» Scalability

Approaching regulations with an open mind can create new business opportunities. Reducing risks and liabilities tied to these regulations can also serve as a competitive advantage as it enables your business to do things it couldn’t do before. For instance, allowing patients to manage their electronic health records and encouraging healthcare professionals to readily share information can ultimately lead to improved healthcare and lower costs.

If you take the approach that it’s not a matter of if a breach will occur but rather when and how often, you’ll be more than prepared should a data breach occur. Securing your healthcare records is less expensive than ignoring the problem and ending up on the wrong side of the law.

Arguably, the most important thing to enable information security and compliance in your business is to think long term. Start thinking today about how your current technologies and business practices will impact compliance and information risks down the road.
Part 7: Moving forward

Data security breaches are on the rise, and savvy lawyers and politicians are taking note. Security and compliance are no longer optional. If healthcare-related security and compliance are anywhere on your radar, these best practices must be a core competency of your business. The good news is that you don’t need perfection. You simply need to get rolling with the formula shown in Figure 3.

As you build out your system of controls, remember security and compliance should never get in the way of business. Healthcare professionals want technology to make their jobs easier, not hinder their work. If you properly assess risk and implement transparent technologies and reasonable policies and processes, sensitive information will be kept secure.

Once you have a solid information security and compliance program in place, you’ll be able to proactively manage risks rather than react every time a new threat, vulnerability or regulation appears. This will not only help you achieve and maintain compliance in the context of healthcare, but also help with related requirements that come up in the normal course of business.

Find out where your business is weak
Re-evaluate on a periodic and consistent basis
Implement the right technologies to help with enforcement
Put reasonable policies and business processes in place
Determine the compliance and security gaps

Figure 3: The proven steps for effectively managing security and compliance
Consider:

- There are varying degrees of risk:
  - Acceptable if the impact or likelihood is low
  - Unacceptable if the impact or likelihood is high, which can be mitigated by:
    - Implementing technical controls
    - Implementing additional policies and procedures
    - Making adjustments to business processes
    - Transferring the risk to a third party (e.g., business associate) or an insurance policy

- Risks change as your business operations and technology change, underscoring the importance of performing a risk analysis on a periodic and consistent basis.
Appendix B: User awareness and training tips

To enhance your overall information security and compliance program, you must establish an ongoing training and awareness program. It should focus on promoting security and compliance within the organization, and communicating secure business practices such as what to look out for, what not to do and how to report a suspected incident.

You can incorporate your awareness and training programs into everyday functions at little or no cost to the business. The following are a few ideas:

» Discuss these programs during new employee orientation.

» Schedule periodic formal classroom training and "lunch and learns."

» Display posters around the office.

» Use computer screensaver reminders.

» Pass out promotional items such as coffee mugs and mouse pads.

It’s also critical that you continually focus on ways to enhance your ongoing security awareness and training program. One of the best ways to keep your awareness and training program stable and visible within the organization is to coordinate everything through a central source, such as the human resources department.

Repeatedly set user expectations. Make sure every employee understands the policies and also the consequences of policy violations. Tying awareness and training into employee reviews and incentive programs often works well. Finally, treat user awareness and training as a long-term investment. If done properly, it can provide quick and tangible payoffs.
Appendix C: Security policy template

The following security policy template* can be used to help ensure everyone’s expectations are set and ensure compliance with most privacy and security regulations:

Introduction: Overview of what you’re covering such as drive encryption, malware protection, system maintenance and monitoring, etc.

Purpose: High-level goal(s) and strategy of the document

Scope: Covered systems such as laptops, desktops, servers, etc.

Exceptions: Specific systems, users or business functions not covered by the policy such as database servers, HR staff, finance, etc.

Roles and responsibilities: Personnel involved and what’s expected of them

Policy statement: Your actual policy that outlines “this is how we do things here”

Procedures: Specific steps describing how you’re actually carrying out the policy

Compliance metrics: Procedures or other means used to measure compliance with the policy

Review and evaluation: Timeframe(s) in which the policy will be reviewed for accuracy, applicability, etc.

Sanctions: Consequences for violating the policy such as this will happen on the first offense, this on the second offense, etc.

References: Laws and regulations the policy applies to such as HIPAA, HITECH, PIPEDA, etc.

Related documents: Other documents that pertain to the policy such as security standards, security plans and related policies

Revisions: Changes made to the policy document such as what, when and why

Notes: Findings, lessons learned and so on that can help with future policy enforcement or management
About Sophos

More than 100 million users in 150 countries rely on Sophos as the best protection against complex threats and data loss. Sophos is committed to providing security and data protection solutions that are simple to manage, deploy and use and that deliver the industry's lowest total cost of ownership. Sophos offers award-winning encryption, endpoint security, web, email, and network access control solutions backed by SophosLabs – a global network of threat intelligence centers. With more than two decades of experience, Sophos is regarded as a leader in security and data protection by top analyst firms and has received many industry awards.

Sophos is headquartered in Boston, US and Oxford, UK. More information is available at www.sophos.com