Connecting the Dots Between Cyber Risk and Patient Safety


By
Bob Chaput, MA, CISSP, HCISPP, CRISC, CIPP/US
CEO Clearwater Compliance LLC
# Table of Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Executive Summary</td>
<td>3</td>
</tr>
<tr>
<td>The Cybersecurity-Patient Safety Link</td>
<td>3</td>
</tr>
<tr>
<td>The Threat is Real</td>
<td>4</td>
</tr>
<tr>
<td>Challenges to Protecting Against Emerging Threats</td>
<td>5</td>
</tr>
<tr>
<td>Privacy/Security – Together or Separate?</td>
<td>6</td>
</tr>
<tr>
<td>Considerations &amp; Recommendations for an Information Risk Management (IRM) Approach</td>
<td>7</td>
</tr>
<tr>
<td>Conclusion</td>
<td>8</td>
</tr>
<tr>
<td>About Clearwater Compliance LLC</td>
<td>9</td>
</tr>
<tr>
<td>Endnotes</td>
<td>10</td>
</tr>
</tbody>
</table>
Executive Summary

Today the information needed to provide care resides in more places than ever before, including electronic health records, the smartphones, tablets and laptops carried by physicians and other caregivers, intelligent medical devices like smart pumps, monitors and implants, patient portals and mobile health apps, not to mention provider partners, business associates and other members of the patient care ecosystem. Safe, quality care depends on timely access to this information. Therefore, any threats to the confidentiality, integrity or availability of information represent threats to patient safety.

This white paper highlights how information security and patient safety are linked, identifies emerging PHI-related threats to patient safety, documents relevant incidents and the lessons that can be learned from them, and suggests how hospitals can enhance their risk management approach to better protect patients against new cybersecurity-related threats to patient safety.

The Cybersecurity-Patient Safety Link

Traditional threats to protected health information and the security programs to thwart them have focused on preventing PHI from being stolen or accidentally disclosed from hospital information systems. Most security programs have evolved and expanded to cover mobile devices and remote data access, but frameworks that extend protections to intelligent medical devices or consider threats other than data loss are much less common.

Security approaches need to continue to evolve to address emerging threats. Because data is driving more decisions, and modern care depends on timely access to data that is shared among multiple systems and sources (both inside and outside the hospital), organizations must expand efforts to ensure the confidentiality, integrity or availability of their information. Besides protecting data from being disclosed or stolen, it must also be protected from being blocked, deleted or altered. While such events would seem unlikely in the traditional threat environment, health care leaders now must consider what could happen if hackers planned to do something with PHI other than resell it.

That “What if?” scenario became reality in February 2016 when hackers blocked authorized users from accessing Hollywood Presbyterian Medical Center’s electronic health record system until a ransom was paid. The successful “ransomware” attack against a hospital was highly unusual and provides a clear example of the new types of threats for which health care providers must implement safeguards.

While data breaches are a fairly routine occurrence, the Hollywood Presbyterian incident garnered the attention of health care IT, compliance and risk management professionals because of its novelty. “Can you provide care if your
EHR becomes compromised? – that’s a question all CIOs are now asking,” says José Perdomo, senior vice president of ethics and chief compliance and privacy officer of Nicklaus Children’s Hospital in Miami.

One executive that considered how an EHR ransomware attack would affect her hospital concluded the facility could still provide care because it plans and trains for downtime and has safeguards and redundancy built into its processes. However, she believed that restoring records and dealing with the aftermath of such a breach would place a significant burden on the organization.

Lack of access to medical records and other clinical information creates a risk. There are also obvious risks associated with missing, incomplete or inaccurate records, which hackers could intentionally create.

“The Threat Is Real

2015 was a watershed year because it was the first time more patient records were exposed by hacking than by accidental disclosures. Also in 2015, malware surpassed all other threats to become the leading concern among health care information security professionals. Eighty-one percent of health care organizations reported they had been compromised by a cyber attack within the last two years. These developments highlight how PHI is being targeted more aggressively and in more ways.

The volume of attacks and number of PHI records disclosed continue to increase but the numbers do not show how the threat environment has changed – and thus do not provide guidance on how organizations can better protect themselves. A key consideration is whether the type of EHR breach Hollywood Presbyterian experienced was an outlier or an indicator of the future state. Unfortunately, a growing body of evidence suggests the latter. For example, post-incident investigations at three hospitals that experienced PHI data breaches also found that malware had been installed on medical devices.

Intelligent medical devices are increasingly viewed as relatively easy targets for hackers.
After white hat hacker Billy Rios demonstrated vulnerabilities in IV pumps (a concern that developed while he was hospitalized), the FDA took what its cybersecurity coordinator called “precedent-setting” action against one device manufacturer because of the ease with which unauthorized users could remotely take control of its pumps and change dosage settings. The FDA followed up in January 2016 by issuing its first draft guidance on cybersecurity management for medical devices.

The insurance industry is taking these and other emerging threats seriously. Insurers and clients report that a health care organization’s cybersecurity competency is being factored more heavily in malpractice premium calculations.

**Challenges to Protecting Against Emerging Threats**

If the threat profile is changing, it follows that the approach to protecting patient data may also need to change. Making this pivot can be very challenging because organizations may not know what specifically they need to protect against. Precedents and best practices are still emerging in some areas, for example how best to work with business associates to optimize end-to-end protection for PHI, or how to extend security to medical devices that produce and store data and may be integrated with other information systems.

One challenge is to ensure a hospital’s patient data is protected when it is outside the hospital. Most hospitals have an expanding ecosystem of business associates that includes community health partners, outpatient facilities, home care providers, wellness coaches and others that operate outside the organizations security/privacy perimeter. Many hospitals are also offering patient portals and/or mobile applications, which also change and challenge traditional security boundaries. Within the facility, many medical devices do not have a native level of security that matches the standards hospitals have set for protecting PHI, which prompted the aforementioned FDA actions.

The vulnerabilities described above are somewhat specific and can be remedied by point solutions, such as writing data security covenants into contracts with business associates, or implementing authentication technology for medical devices. A point-by-point approach itself creates challenges. First, organizations tend to always be playing catch-up and focusing on preventing a recurrence of the last incident. Second, they may not develop a clear understanding of their entire privacy and security environment and risk profile when they take a linear, point-by-point approach. This can lead to redundant efforts by teams that are responsible for different aspects of information security, patient safety, privacy and risk management. Such redundancy can prevent an organization from achieving synergies and economies of scale.
Privacy/Security – Together or Separate?

An effective way to mitigate redundant privacy and security efforts is to establish consistent, proactive communication among stakeholders. Privacy, security, risk management and other disciplines within the organization should regularly share information about the incidents and potential risks they have identified and the actions they are taking to protect them. Such information sharing helps organizations develop a more comprehensive understanding of their threat profile and can lead to more effective collaboration. The downside is the possibility of creating risk fatigue, where notifications and recommendations are so frequent that their perceived importance diminishes.

“...The issue is maintaining vigilance and awareness about all the potential threats, but you can’t be alarmist, or frontline workers will tune it out,” says Perdomo.

Hospitals could institutionalize collaboration by making one organization responsible for managing patient safety, information security and risk management. Today most hospitals assign separate leadership for these functions and responsibilities. In the current era where patient safety increasingly depends on the confidentiality, integrity or availability of information, managing information security and patient safety in different departments can create risk, according to a RAND Corporation study commissioned by the U.S. Office of the National Coordinator for Health Information Technology. It noted:

Adoption of health IT is sufficiently recent in most health care organizations that the methods, practices, and management of health IT risks may be quite variable across organizations. Even those with decades of experience with health IT may not be fully prepared to manage the health IT–specific risks that can be created as they modify their systems. In hospitals, managing health IT safety risks may require collaboration across executive leadership; departments overseeing IT, risk management, and quality management; and the variety of professionals delivering care.

Combining patient safety, information security and risk management responsibilities helps an organization develop a broader perspective about its threats. The strategies, processes and protections that result will be designed to provide comprehensive protection that goes beyond meeting specific guidelines or compliance requirements.
Considerations & Recommendations for an Information Risk Management (IRM) Approach

The current risk environment is changing quickly and continually and includes a wide spectrum of threats, ranging from traditional intrusions designed to steal PHI to more novel and emerging attacks, such as tampering with medical devices or blocking access to essential records systems. The changing threat environment is blurring the lines between information security and patient safety and is requiring each discipline to expand its scope. Rather than pursuing parallel paths, organizations instead can adopt a comprehensive framework for managing security, safety, privacy and risk.

A comprehensive information risk management (IRM) approach is not a checklist. It provides a structure to organize and prioritize various aspects of protection. It provides for elements like governance, people, process, technology and organizational engagement. These elements include the processes and specific solutions used for risk assessments, data protection, identity management, authorization, compliance reporting, incident detection, incident response and more. A thoughtful approach can help organizations logically assign these roles, develop an effective governance structure, and ensure activities are coordinated.

The FDA is encouraging medical device makers to adopt the Framework for Improving Critical Infrastructure Cybersecurity that was been developed by the National Institute of Standards and Technology (NIST). The NIST cybersecurity framework specifically calls for the use of a separate, formal information risk management process.

Clearwater Compliance strongly advocates that health care organizations take a formal approach to their overall information risk management, patient safety and security efforts, using the NIST Information Risk Management (IRM) approach.

The NIST Information Risk Management approach has three components:

1. **NIST Cybersecurity Framework** – Presents a way for organizations to combine current standards, guidelines and best practices to reduce cybersecurity risk.

2. **NIST IRM Process** – The NIST Information Risk Management Process (NIST SP 800-39) provides detailed steps for framing, assessing, responding to and monitoring risks. The steps are organized into responsibilities for different levels and roles within an organization.

3. **Maturity Model** – The approach encourages adoption of a maturity model to ensure proper implementation and ongoing use, but gives organizations to use the maturity model of their choosing. Think the Deming model: Plan, Do, Check, Act.

For more detailed information about the NIST Information Risk Management approach and how health care organizations can apply it, see the Clearwater Compliance white paper Harnessing the Power of NIST: Your Practical Guide to Effective Information Risk Management.
Conclusion

Information security has become an essential component of patient safety. Concurrently, the threat environment for information security has significantly changed and expanded. The net effect of these developments is that traditional approaches to patient safety and information security may not be aligned with the current threat environment, which can lead to gaps in how patient safety and medical data are protected.

In response, health care organizations are implementing not only new methods to protect patients and systems, but new models for their patient safety, information security and risk management efforts. One effective model is to implement a framework that combines patient safety, information security and risk management authority. The framework approach helps organizations develop the comprehensive outlook that the fast-evolving threat environment requires and helps gaps from emerging between efforts to protect patient safety and information.

The NIST Information Risk Management Approach provides a standardized framework that is highly appropriate and adaptable for health care organizations. One of its components is the NIST Framework for Improving Critical Infrastructure Cybersecurity, which the FDA encourages health care organizations to use to protect critical infrastructure.
Clearwater Compliance, LLC, helps hospitals, health systems and their business associates improve patient safety and quality of care by assisting them establish, operationalize and mature their compliance and cybersecurity programs. Led by veteran, C-suite health care executives, Clearwater’s award-winning software, educational events and expert professional services provide scalable, cost-effective solutions for all sizes of organizations. Since 2009, the company has served hundreds of clients ranging from major health systems, hospitals, health plans and Fortune 100 companies, to medical practices and health care startups.

Find out more about Clearwater’s compliance, cybersecurity and information risk management solutions at clearwatercompliance.com

Copyright © 2015 Clearwater Compliance LLC. All Rights Reserved.
Any replication or dissemination shall only be authorized by the express written permission of Clearwater Compliance LLC.

Health Care Information Privacy, Security, Compliance and Risk Management Solutions from Clearwater Compliance LLC have earned the exclusive endorsement of the American Hospital Association.
Endnotes

3. Ibid.