DOING IT RIGHT: GETTING A JUMP ON PRIVACY AND SECURITY

Global Institute for Emerging Healthcare Practices

New data sources, changing regulations, and tighter enforcement of privacy and security rules are requiring healthcare leaders to be vigilant about protecting sensitive health information. More data are coming from more sources than ever before, including remote monitoring, mobile devices, and social media. Additionally, the stakes are higher as new enforcement efforts take effect and the HIPAA audit program reaches its stride. In this paper, we identify six basic things that every health delivery organization can do now to improve privacy and security.

Achieving excellence in privacy and security is essential to the delivery of integrated, quality care in our changing healthcare environment. Yet, to many hospital executives, privacy and security can seem like a continuously moving target. Shifting technologies, changing regulations, and tighter monitoring of breaches and other adverse incidents keep leaders vigilant. With new changes to the HIPAA Privacy and Security Rule expected to be released sometime in the second half of 2012, the time to refocus on protecting sensitive patient information is now.

More Data to Protect, in More Places

Health delivery organizations are dealing with an immense amount of data and an ever-growing array of systems, interfaces and end-user devices. More data are available than ever before for internal and external use. Data are not just for patient care anymore; they are for research, operations and marketing.

Hospitals have amassed terabyte-sized databases from patient encounters, and executives are rightfully eager to convert these data to knowledge in order to improve care, reduce costs and enhance overall performance. In the past, organizations have protected their assets in part by maintaining a centralized architecture. However, as these data warehouses and repositories continue to grow, there is increasing pressure to transition to shared architectures and cloud-based models for performance, integration, and analytical purposes. Best practices for ensuring privacy and security while employing the cloud are still emerging.

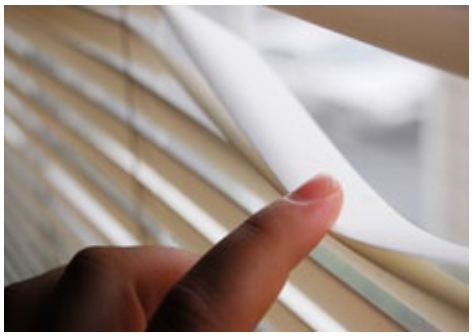
Other new developments, such as the rise of social media, add to the overall complexity of data protection. There are now more outlets, or "channels," to monitor in order to ensure that protected health information (PHI) is not made public. Organizations may wish to encourage patients and doctors to engage each other in online communities about symptoms, medications and therapies. But without clear policies and protections in place, sensitive PHI can — intentionally or unintentionally — end up on blogs, Facebook, Twitter or YouTube.

A recent survey of 192 U.S. executives in various industries (including healthcare and life sciences) found that 27 percent believe that social media-related risks will become an increasingly important part of the overall risk environment.

"Key Risks Not Being Continually Monitored" Deloitte and Forbes Insights, June 28, 2012

The Stakes Are Higher

The need to get privacy and security right has never been higher, for two main reasons: 1) patient trust is the lynchpin of the next generation of care delivery, and 2) the enforcement of privacy and security rules and regulations is rising sharply.



Ensuring privacy and security is critical to building trust with patients. Little progress can be made with initiatives such as electronic health records (EHRs), health information exchanges (HIEs), electronic prescribing (eRx) or advanced analytics if patients do not feel comfortable with their delivery organization's ability to protect personal information. Without system-wide trust and consent, the next generation of care — which relies so critically on patient engagement, shared accountability and data exchange — will suffer from lack of participation by patients and providers and will ultimately fail.

Protecting data with the proper safeguards is not just the *right* thing to do; it also is increasingly a *legal and regulatory requirement*. Although the Department of Health and Human Services (HHS) traditionally has not followed through with the existing HIPAA requirement to perform regular audits of covered entities, enforcement is now on the rise. For instance, the HITECH Act has strengthened civil and criminal enforcement of privacy and security rules, with new civil monetary penalties reaching up to $50,000 per violation (with an annual maximum of $1.5 million), and carrying a potential prison sentence of up to 10 years. Imprisonment, while new and relatively rare today, will be increasingly used for punishing serious breaches in the future.

Already there has been an uptick in federal, state and consumer lawsuits against covered entities and their business associates.[1] In May 2012, federal prosecutors filed suit against one East Coast academic medical center over an alleged failure to protect patient information that had been downloaded to a laptop.[2] In January 2012, Minnesota's Attorney General filed suit against a revenue cycle management company for allegedly violating state and federal privacy laws. Even small physician practices are feeling the tighter enforcement. In April 2012, a five-physician Arizona-based practice entered into a resolution agreement that included a $100,000 civil money penalty over allegations of HIPAA violations.[3]

Another thorn for covered entities is the fact that, starting in 2014, patients who are harmed by a data breach will be able to collect a portion of the penalty money as damages. While this is a fair and perhaps overdue remedy for patients who are genuinely harmed, it could also motivate some individuals to initiate legal action over the smallest of transgressions.

HIPAA Audits: The Next Generation in Enforcement Is Here

The HITECH Act also requires HHS to establish a system of periodic audits to ensure that covered entities and business associates comply with HIPAA rules. After having completed its first set of 20 pilot audits, the Office of Civil Rights (OCR) announced in June 2012 the revised protocol it will use to conduct further HIPAA audits required by the law.[4] The audit program addresses a total 165 performance criteria and instructs auditors to analyze processes, controls and policies in the following broad areas:

- Notice of privacy practices for PHI
- Processes for requesting privacy protection for PHI
- Access of individuals to their own PHI and that of family members (where allowed)
- Administrative requirements such as training and procedures for handling complaints
- Uses and disclosures of PHI
- Making amendments and corrections to PHI
- Accounting of disclosures
- Security-related administrative, technical, and physical safeguards
- Breach notification

While the audits in the initial round were designed to provide a broad, representative sample of the industry, future audit selections will be random and business associates will be included. Poor performance on the audit could result in investigation and sanctions. OCR is advising covered entities to use the protocol as a tool for measuring their own compliance.

The biggest threats to privacy and security often do not come from sophisticated external sources. Of the top ten healthcare security breaches in the first half of 2012, just one was the work of an outside hacker. Half of the ten largest incidents were cases of lost or stolen property, such as laptops, thumb drives, and backup tapes. (Often, equipment is stolen after being left unattended in the car of an employee or contractor.) The rest of the top incidents were either "inside jobs" perpetrated by employees, or unintentional failures to follow policies and procedures.

McNickle, M. "Top 10 Data Security Breaches in 2012" *Healthcare Finance News*, June 2012

Understanding the Risks and Challenges

Privacy and security threats come in a wide variety of forms. Generally, all entail some form of unauthorized entry or access. Some of these include:

- Unauthorized access by external intruders (i.e., non-hospital staff)
- Unauthorized access by caregivers and employees
- Stolen laptops and other end-user devices
- Medical identity theft, including use of a deceased person's PHI or social security number
- Injection of viruses or malware
- Attacks designed to deceive, compromise or incapacitate legitimate users
- Social engineering to gain passwords and information
- Dumpster diving for improperly discarded equipment
- Unauthorized access by former disgruntled employees with knowledge of key systems

Not all organizations have the same number and the same types of vulnerabilities. In the pilot test of the HIPAA audit program, for example, the government found that small covered entities had more deficiencies than large ones, and that providers (hospitals and individuals) had more deficiencies than health plans or clearinghouses.[5]

Your risk profile is unique based on the myriad choices in technologies, architectures, and policies and procedures that your organization has accumulated over time. Having a history of mergers and acquisitions can increase an organization's risk profile. A good way to understand the relative risks associated with your organization is to conduct a comprehensive privacy and security risk assessment, similar to the one that is now required to attest for the meaningful use EHR incentive program.

The risk assessment measure under the EHR incentive program calls for organizations to analyze the relevant electronic health information technologies, identify and document technical and administrative updates that are needed, and address and document deficiencies that are found. The cardinal rule of conducting such a risk assessment is to document all findings and decisions pertaining to actions taken, not taken or deferred for later, and why various actions were not taken or why they were deferred.

Healthcare providers often find that security poses a bigger challenge than privacy. Security-related vulnerabilities usually require the implementation of technical tools and solutions, such as user activity monitoring, secure authentication, and role-based user access management and provisioning. (Setting up automated alerts can enable staff to monitor larger environments than would be possible manually.) Top privacy vulnerabilities tend to be more process-based and can be remedied with improved policies and better diligence, like ensuring thorough business associate contracts, documenting disclosures and formalizing the review process for denials of patient access to records.

Getting a Jump on Privacy and Security

As the industry awaits the release of the final omnibus rule from the Office of Management and Budget (OMB) entitled, "Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules," healthcare delivery organizations can get a jump on their remediation efforts and better prepare

themselves for a possible audit. The rule, while it is expected to enact some changes, such as extending the penalty provisions to business associates and clarifying the definition of "marketing activities" with regard to PHI, will not alter the ongoing need for organizations to assess and improve their privacy and security practices.

Whatever the details of the final rule turn out to be, here are six things that every health delivery organization should consider closely. We recommend that organizations address these areas now while interest is high and before the audit program launches into full swing:

1) **Establish a Chief Privacy Officer (CPO)**. Key duties of the CPO should include monitoring information systems, establishing and revising policies and procedures, providing training, and advising on privacy matters with business associates. Larger organizations should be able to make the CPO a full-time dedicated position. Small and medium-sized organizations may need to make the role a function of the compliance officer. A technically savvy person should hold it, but it should not be a role that is buried deep in the IT department. Make sure that the CPO is strategically reflected in the organizational structure and has the ear of leadership.
2) **Conduct a security risk assessment *before* you get the audit notice**. Look at *every* system and process, and document every decision you make, including reasons for addressing or not addressing a particular risk. Under the new HIPAA audit program, organizations are required to produce documents within 15 days of OCR's initial request, and it has already been determined that no extensions will be granted. This leaves very little time to compile things like lists of electronic assets and copies of current procedures — and sort out which are up to date. To save time and stay focused on the questions that matter, use the new audit tool released by the HHS Office of Civil Rights as a guide.
3) **Make risk identification and mitigation subject to continuous improvement**. Don't let your risk mitigation action plan accumulate multiple years' worth of delays and deferments. Software patches and updates should be applied on a regular basis. Take the opportunity to update and refine physical, technical and administrative safeguards. Additionally, do not just look at systems that are operational today. Get ahead of the curve by applying changes to planned and future systems. Some exploits may seem very small until they lead to large data breaches, so fine-tune your systems as soon as needs are identified. Include a risk review and audit with every new system implemented and included in the organization's application portfolio. Be willing to migrate some applications to a hosted environment (i.e., software-as-a-service) if you find you cannot invest the time or money internally to maintain a high level of security.
4) **Communicate with employees**. Ensure that everyone in your organization who has access to PHI has had the required training and is up-to-date on policies and procedures. Customized, role-based training is more effective than requiring each employee to sit through a generic presentation. Make sure that employees realize that privacy and security is everyone's responsibility, not just the concern of the Chief Privacy Officer or the people in the IT department. When issues arise, use them as teachable moments and cultivate a culture of enforcement at all levels. In addition to organizational-level oversight, give individual groups and departments the responsibility of oversight. Make sure the organizational environment is a safe place for employees and clinicians to raise concerns so communication and corrective actions are based on improvement not blame.
5) **Communicate with patients**. Patients need to be assured that their information will be treated confidentially and protected at all times. Under HIPAA, covered entities are required to obtain authorization from individuals before using their PHI to market a product or service. Give patients confidence by communicating openly with them about the safeguards that are in place, and explain to them in plain English how their information will

be used. Use educational handouts, pamphlets and digital signage in waiting areas to help patients understand the benefits of EHRs and health information exchange. Patients are well-informed; it is likely they will be familiar with some of the high-profile data breaches that have occurred. They may be skeptical, but they will be interested. Organizations must assure patients with concrete facts and evidence that their privacy is respected and their PHI is well-protected.

6) **Expand your purview to include mobile devices and social media**. Do not assume that employees know how to apply existing rules about privacy and security to new devices and new forms of media. Address these new areas explicitly to avoid breaches and failures of communication. Although many best practices are still emerging, that is not an excuse for offering zero guidance. Employees *want* to do the right thing. The federal government's Office of the National Coordinator for Health Information Technology (ONC) and OCR are working collaboratively to define the best way to extend existing HIPAA guidelines to mobile devices and social media. Follow those developments closely, get involved in the public roundtables and public comment periods, and evaluate organizational policies and procedures for continuous improvements.

Acknowledgments

The author would like to thank Linda Ricca with CSC's Healthcare Group; Richard Staynings, CSC's Cyber Security and Privacy Officer; and Jordan Battani, Managing Director of CSC's Global Institute for Emerging Healthcare Practices, for their contributions.

About the Author

Jared Rhoads is a senior research specialist with CSC's Global Institute for Emerging Healthcare Practices, the research arm of CSC's Healthcare Group.

References

1. Klein, M. "Health Care: What HIPAA Means for Data Centers" *Data Center Knowledge*, June 29, 2012
2. Schultz, D. "Medical Data Breaches Raising Alarm" *Washington Post*, June 2, 2012
3. Dolan, P. "$100,000 HIPAA Fine Designed to Send Message to Small Physician Practices" *American Medical News*, May 2, 2012
4. Health Information Privacy: Audit Protocol, U.S. Department of Health and Human Services, June 2012, http://ocrnotifications.hhs.gov/hipaa.html
5. Niewnhous, M.D., "OCR Share Preliminary HITECH Audit Results; What Regulated Entities Can Expect Next" *Health Care Attorneys*, June 11, 2012

BUSINESS SOLUTIONS
TECHNOLOGY
OUTSOURCING

Healthcare Group
3170 Fairview Park Drive
Falls Church, VA 22042
+1.800.345.7672
healthcaresector@csc.com

Worldwide CSC Headquarters

The Americas
3170 Fairview Park Drive
Falls Church, VA 22042
United States
+1.703.876.1000

Europe, Middle East, Africa
Royal Pavilion
Wellesley Road
Aldershot, Hampshire GU11 1PZ
United Kingdom
+44(0)1252.534000

Australia
26 Talavera Road
Macquarie Park, NSW 2113
Australia
+61(0)29034.3000

Asia
20 Anson Road #11-01
Twenty Anson
Singapore 079912
Republic of Singapore
+65.6221.9095

About CSC

The mission of CSC is to be a global leader in providing technology-enabled business solutions and services.

With the broadest range of capabilities, CSC offers clients the solutions they need to manage complexity, focus on core businesses, collaborate with partners and clients, and improve operations.

CSC makes a special point of understanding its clients and provides experts with real-world experience to work with them. CSC is vendor-independent, delivering solutions that best meet each client's unique requirements.

For more than 50 years, clients in industries and governments worldwide have trusted CSC with their business process and information systems outsourcing, systems integration and consulting needs.

The company trades on the New York Stock Exchange under the symbol "CSC."

www.csc.com

WA12_0164 HCG
July 2012