Protecting Digital Health Information—Where to Start?

An NJVC® Executive White Paper

Terri Schoenrock
Director, Healthcare Solutions

June 2013

NJVC
Driven by Your Mission®

I. Executive Summary

Healthcare provider organizations everywhere are evolving patient health data access and management, making individually identifiable information more digital, mobile and available. With this move comes a quantum increase in the exposure of individually identifiable information within the enterprise and across the extended value chain. The balancing act is to address the need to be agile and responsive to stakeholders, and therefore more competitive, while managing the risk of compromised security with consistently dwindling budgets.

We ask healthcare leaders, "What could someone do with your health record?" With the black market value of a patient health record at $50, or five times that of other individually identifiable information, the answer is "a lot." According to the Third Annual Benchmark Study on Patient Privacy & Data Security (Ponemon Institute, 2012), only four in 10 healthcare organizations feel that they can prevent a data breach. Breaches of individually identifiable information are increasing, frequently involve millions of records, and make billions of dollars for black marketers. Ponemon asserts that fewer than half of all health providers conduct annual security assessments. Cyber attacks on health provider organizations are increasing and becoming harder to control, with breaches costing healthcare organizations an average of $2.4 million per year (Ponemon, 2012). This comes when U.S. health providers are expecting reductions in topline revenue beginning in 2014, and will have to rely on reduced operating budgets to combat these security vulnerabilities.

Health providers understand that before they can make a diagnosis, they must assess the patient. This applies equally to cyber security in health IT. From there, a health provider can set the plan to manage care with the patient and his or her caregivers. "An ounce of prevention is worth a pound of cure." Assessing the security of the health enterprise for cyber threats and vulnerabilities can identify issues before they become overwhelming problems. Partnering with a vendor who understands managed security architectures provides a safety net that assures stakeholders that you are protecting and securing sensitive information.

II. An Evolving Healthcare Environment

Every healthcare enterprise in the United States must evolve at an unprecedented pace to meet the financial and quality-of-care challenges brought on by chronic disease management and an aging population. The percentage of the U.S. gross domestic product related to healthcare is the highest of any of the developed countries. Yet, of those developed countries, the life expectancy and availability of care for U.S. residents are among the lowest. In addition, hypertension, asthma, obesity, diabetes, arthritis and other chronic diseases are experiencing unprecedented growth.

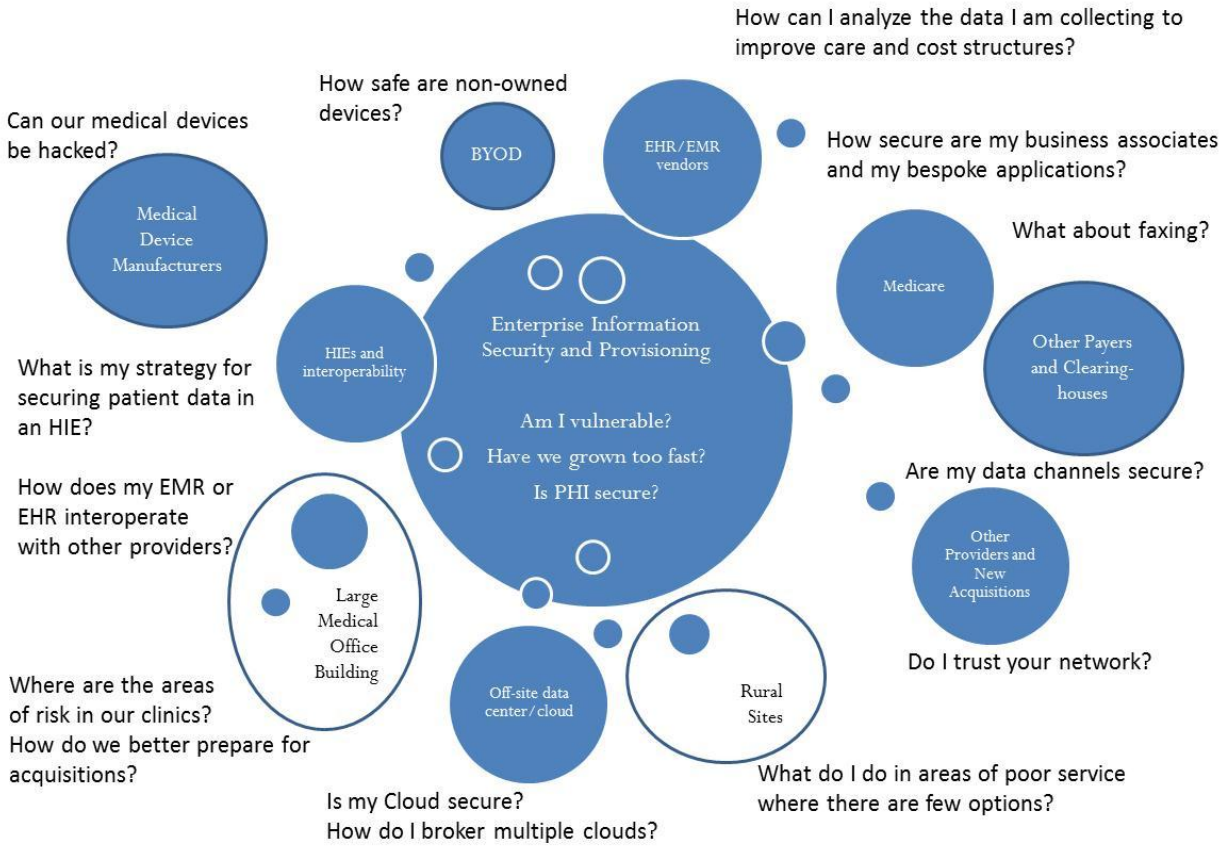
Employers, health payers (health insurers and the government), the government and health providers are reacting to these high costs and the growth (and required management) of chronic disease. Retail businesses, such as Walmart, are becoming health providers, health providers and payers are becoming software developers, and employers are offering health and disease

management and providing care, such as flu shots, to employees. As the health provider enterprise continues to expand, it must become more interconnected and interoperable. By definition, the healthcare enterprise must share more personal health information and other critical and sensitive data, exposing itself to increased cyber security risks.

To improve the quality of care and manage chronic disease states, telemedicine and increased use of the Internet, the use of patient portals, mobile devices and applications, and social media is increasing. There is a seismic shift today from a more traditional brick-and-mortar health provider environment to one that is increasingly digital. Healthcare provider organizations are expanding the use of electronic records, and mining the data that has been collected to analyze and develop useful information that will improve care and cost structures. Longitudinal patient records are being created from electronic systems within and outside the managed enterprise. Increasingly healthcare providers are entrusting their patient data to third parties, broadening the scope and scale of what must be secured. At the same time, the "teeth" within the Health Insurance Portability and Accountability Act of 1996 (HIPAA) have been sharpened to focus more broadly on breaches by health organizations and their vendors.

Failure to meet the standard of care for securing health information (mandated by federal and state governments, patients and communities) is costly. Breaches expose health provider organizations, and the individuals involved, to criminal and civil actions and extraordinary fines. However, a failure to meet the competitive challenge of interoperating with peers, enabling accountable care, automating manual and paper-based processes, and participating in health exchanges creates an even larger competitive challenge. Executives need tools and information to make smart and prioritized decisions that support interoperability, enable accountable care, support mergers and acquisitions, and allow for the secure exchange and transmission of protected information to other organizations and through patient portals.

The stakeholder community of U.S. healthcare is complex, with many public and private actors of all sizes, and many levels of cyber security sophistication. Disparate information stores, a vast array of input and access methods, and interoperability challenges present a target-rich atmosphere for thieves. If one asks health providers what keeps them up at night, these are some of the questions they ask.



III. Ongoing Breaches, Threats, and Increased Vulnerability

The exploding level of data exchange and connectivity mandates greater vigilance by health provider organizations. Many security technologies and structured procedures are being adopted by organizations in lieu of the ad hoc processes of the past. However, shortages of funding for critical changes and competition for IT project dollars have caused many health provider organizations to fall behind their peers in other industries, such as financial services and energy, in the area of managed cyber security architectures. Although investments in personnel training on HIPAA are high, investment in the technological assurances that would support HIPAA are lower. Ninety-four percent of healthcare provider organizations reported a data breach in the two-year period between 2010 and 2012, and 45 percent reported more than five breaches in that period, with the most incidents in health information management (patients' medical files) and financial accounting (billing and insurance) (Ponemon, 2012). Increasingly, the point of sale system used to collect fees (billing and co-payments) is also at risk.

None of this is news. The U.S. Health and Human Services' Breach Tool provides daily updates on breaches of individually identifiable patient information, such as the cyber attack on the Utah Department of Health compromising the patient health information of almost 800,000 individuals.

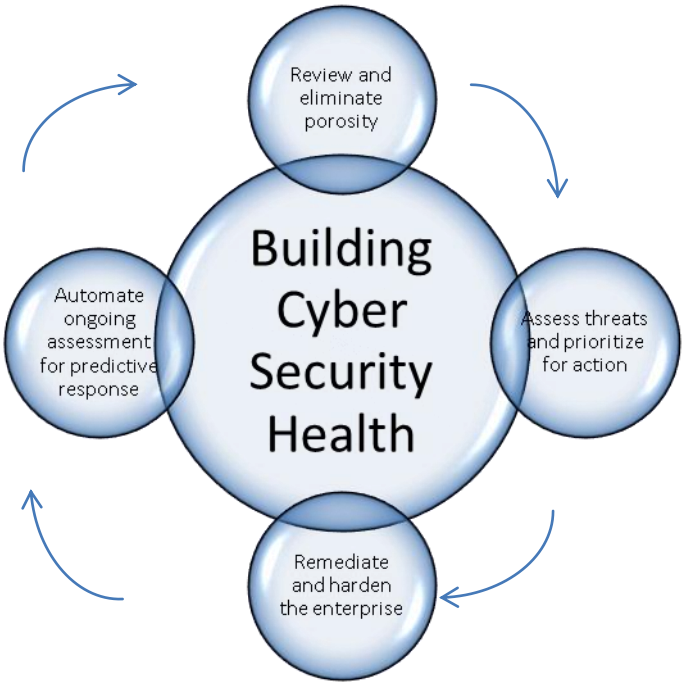
IV. Developing a Safety Net: Cyber Security Technical Assessments

The highest priority for protection is the information stores, holding individually identifiable patient health information (whether at rest, in use or in transit), employee information and sensitive organizational information. However, a chain is only as strong as its weakest link.

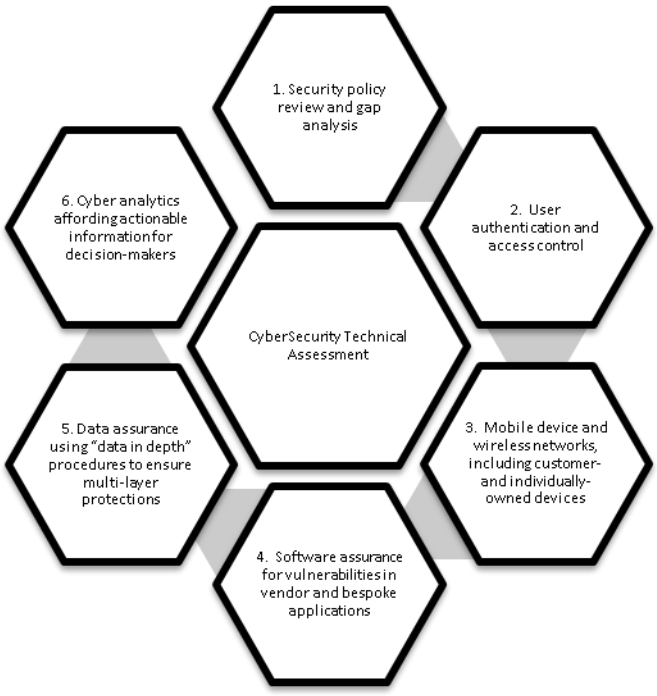
You may ask, "What can my organization do?" Consider your enterprise as a fortress with many different levels of protection for the people and valuable goods held within its walls. In the case of the fortress, the drawbridge allows information and actors to pass in and out of the fortress efficiently and securely with the proper controls. The wall or moat around the fortress constantly protects its boundaries, deflecting bad actors. Turrets manned with soldiers scan for danger. Continual reporting on the safety of the fortress and its contents must be provided to its leadership. The health enterprise is no different. Without the drawbridge, allowing just the correct information in and out (with the proper controls), the moat to assure deflection of threats and attacks, the continual scanning to provide alerts, and a security dashboard to ensure management reporting, the health IT enterprise is vulnerable.

The first step in assessing cyber security health is to determine how susceptible the enterprise is to privacy and security breaches. Porosity indicates security holes in the enterprise, and determines and determines their size, severity and type. The next step is to assess the threats faced by the enterprise, and prioritize those threats for immediate action. The third step is to harden the enterprise by remediating issues via a prioritized roadmap.

Unfortunately, cyber attacks are growing, and the bad actors get better at their job every day. Information security as a service automates an ongoing assessment to ensure that healthcare providers know immediately when a vulnerability is exposed and can react immediately.



A comprehensive assessment of the security posture of the healthcare extended enterprise should offer an end-to-end analysis of the health IT infrastructure and supporting business processes across six dimensions.



The assessment yields a detailed analysis of threats and vulnerabilities, with an actionable roadmap for remediation and ongoing protection. This assessment provides the information that healthcare provider organizations require in order to act. The net result for a covered entity is information on vulnerabilities, and on the activities of personnel, visitors and business associates, that helps prevent breaches of information security. After a Cyber Security Technical Assessment, a healthcare provider organization can remediate the issues, and implement a managed security and cyber-healing strategy that supports an ongoing safety net of protection.

V. Conclusion

Breaches of individually identifiable patient health information result in financial loss, criminal fines, and loss of reputation. The total economic burden created by data breaches in the healthcare industry is nearly $6 billion annually. The impact of a data breach over a two-year period is approximately $2 million per organization, and the lifetime value of a lost patient is $107,580 (Ponemon, 2012). Most breaches can be prevented with a small investment in the future. Equal in impact is the loss of trust by the stakeholder community after a breach. Independent physicians and most patients have a choice in their healthcare and where that care is provided.

Protect your fortress with the right controls at the drawbridge, the best moat available, the right guards at the gate and a dashboard that can report critical information as it occurs (and not after an attack). Privacy and security breaches in healthcare are newsworthy, and are breeding new litigation. It is critical to find a partner to help diagnose your current situation, and help create the safety net that will limit the risk to the health enterprise and its stakeholders, including cloud and other service providers.

About the Author

Terri Schoenrock is NJVC Director, Healthcare Solutions, serving the company's health and life sciences customers.

Ms. Schoenrock is an experienced executive with an extensive background in health IT, business development and consulting, enterprise architecture, IT strategy and governance and global business management. Prior to NJVC, she was Business Process Executive, Health IT, with Kaiser Permanente, where she supported organizational change initiatives within five IT mega process initiatives, and applied Six Sigma, ITIL, COBIT and TOGAF to process initiatives, including SDLC and tools reduction within IT.

Earlier, Ms. Schoenrock was Business Consulting Executive, Health and Life Sciences, with HP—her second stint with the company. She developed healthcare imaging, workflow and office automation solutions for the largest healthcare organizations in the United States. Ms. Schoenrock also was Executive Director, IT Program Management Office, with NANA Development Corporation. She ensured that IT process standards conformed to the needs of NANA and its family of companies; led project and portfolio management, including system lifecycle management; and managed compliance and security initiatives for this 8(a) contractor (10,000 staff). Prior to NANA, Ms. Schoenrock owned her own business, Reece Computer Systems, which focused on building and supporting smarter networks for the small business market.

Ms. Schoenrock also spent several years as Executive Director, Service Oriented Architecture, Healthcare, with HP, where she directed program and solution development across multiple industry, functional and technology disciplines, and across the value chain at the company. Prior to HP, Ms. Schoenrock founded The Axean Group, a consulting company that was named as one of the fastest-growing privately held companies in the San Francisco Bay area. Earlier, she led Nestlé's North American data teams, administration systems, Web services and IT training. She also worked at Oracle Corporation.

Ms. Schoenrock is the recipient of numerous professional awards and serves on several corporate boards of directors. She is Six Sigma and ITIL certified, and the co-owner of a patent for a healthcare emulation and testing system.

About NJVC®

NJVC® provides customers with innovative solutions to critical mission, business and technology challenges. As a proven systems integrator for more than a decade, NJVC offers a wide breadth of IT and strategic solutions to clients focusing on IT automation and services integration, real-time predictive analytics, secure cloud services, managed security services and printing solutions. NJVC provides services to both government and commercial customers whose operations depend on high performance, agility and advanced security. We partner with our clients to support their missions with security-cleared, dedicated and talented employees ready to deploy globally. To learn more, visit www.njvc.com

NJVC
14295 Park Meadow Drive
Chantilly, VA 20151
703.429.9000

www.njvc.com

Learn more about NJVC Cyber Security solutions