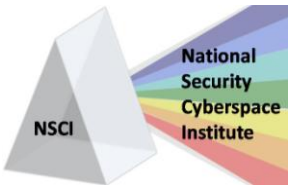

Security and Privacy Implications of Healthcare Digitization

Kathryn Stephens, NSCI
September 22, 2011

If your dread disease alone isn't enough to worry about...

As the healthcare industry makes the transition from paper to electronic medical records, many are concerned that patient records will be vulnerable to unauthorized access, violations of new data breach laws, and exposed to the threat of medical and financial identity theft. A 2010 study of patient privacy and data security from the Ponemon Institute found that data breaches cost the healthcare industry $6 billion annually, and that protecting patient data has been a low priority for healthcare organizations in the past.[1]

According to the Ponemon study, healthcare organizations can expect more fines and disciplinary actions from State Attorneys General and other regulatory organizations, and patients can expect data breaches to increase as criminals look for vulnerabilities in new electronic medical records systems. Dr. Larry Ponemon, chairman and founder of the Ponemon Institute says, "Endemic failure to keep pace with best practices and advancing technology has resulted in antiquated data security, governance, policy plaguing in the healthcare industry. Millions of patients are at risk for medical and financial identity fraud due to inadequate information security. Information security in the healthcare industry is at the fulcrum of economic, technological, and regulatory influence and, to date, it has not demonstrated an ability to adapt to meet the resulting challenges."[2] Given the lack of attention and priority previously given to patient data security, and in light of the healthcare industry's inadequate information security procedures, the government-mandated migration to electronic medical records will certainly increase the risk to individuals' privacy and personal information.

The Federal stimulus bill passed in February 2009 originally provided $19 billion for the migration from paper to electronic medical records, hoping to cut costs and improve efficiency in healthcare organizations. Lawmakers seemed to approve the migration to electronic medical records. Former Speaker of the House and current presidential candidate Newt Gingrich (R-Ga.) called the expansion of electronic record use one of only "two good things" in the federal stimulus package.[3] The stimulus bill requires health care organizations to implement electronic medical records systems no later than 2015 or face monetary penalties such as reductions in Medicare reimbursements.[4] There is concern by many that health care organizations, in a rush to implement EMR systems, will field clunky, flawed systems that fail to provide for the proper data security and privacy of their patients.

There are many important benefits that result from the migration to electronic health records. Patients will be able to easily see their test results and doctor's recommendations as well as treatment and billing records. Patients could also enter their own data, such as their weight, monitor what they have eaten, or track symptoms of chronic illnesses.[5] HHS Secretary Kathleen Sebelius calls the "conversion to electronic health records one of the most transformative issues in the delivery of health care, lowering medical errors, reducing costs and helping to improve the quality of outcomes."[6] Secretary Sebelius is expected to

---

[1] *Experts Forecast Top Seven Trends In Healthcare Information Privacy For 2011.* (2011, January 4). Retrieved from http://www.darkreading.com/security/news/229000092/experts-forecast-top-seven-trends-in-healthcare-information-privacy-for-2011.html
[2] *Experts Forecast Top Seven Trends In Healthcare Information Privacy For 2011.* (2011, January 4). Retrieved from http://www.darkreading.com/security/news/229000092/experts-forecast-top-seven-trends-in-healthcare-information-privacy-for-2011.html
[3] Mostrous, A. (2009, October 25). *Electronic medical records not seen as a cure-all.* Retrieved from http://www.washingtonpost.com/wp-dyn/content/article/2009/10/24/AR2009102400967.html
[4] Mearian, L. (2010, July 14). *What final 'meaningful use' rules on EMRs mean for doctors, hospitals.* Retrieved from http://www.computerworld.com/s/article/9179143/What_final_meaningful_use_rules_on_EMRs_mean_for_doctors_hospitals
[5] *HHS Seeks Better Patient Access to Electronic Records.* (2011, September 12). Retrieved from http://www.newsfactor.com/story.xhtml?story_id=80146
[6] *Data breaches compromise nearly 8 million medical records.* (2011, June 1). Retrieved from http://www.homelandsecuritynewswire.com/data-breaches-compromise-nearly-8-million-medical-records

announce new rules that will make it easier for patients to access and add information to their personal electronic health records. U.S. Surgeon General Regina Benjamin says the new rules will help "patients to take control of their own health and make the choices easy."[7]

So what are we doing...and is it working?

Recognizing the importance of the issue, Congress has passed legislation aimed at providing safeguards. **T**he Health Insurance Portability and Accountability Act (HIPAA) of 1996 addresses the security and privacy of health care information in general; not specifically electronic access. However, HIPAA standards help to encourage the use of electronic data systems in the health care system. HIPAA basically regulates the use of Protected Health Information (PHI), regardless of whether it is in paper or digital form.

More recently, the Health Information Technology for Economic and Clinical Health Act (HITECH) of 2009 addresses privacy and security concerns associated with the electronic transmission of health information. The HITECH Act added breach notification requirements to HIPAA, which includes guidance on how to secure protected health information, and how to notify the proper authorities in the event of a breach or disclosure.

In December 2010, the President's Council of Advisors on Science and Technology (PCAST) released a report, called "Realizing the Full Potential of Health Information Technology to Improve Healthcare for Americans: The Path Forward." The report discusses how the Federal government can assist health care organizations in the migration to electronic medical records and the adoption of a "universal exchange language" that would allow for the transfer of health data while protecting patient privacy.[8]

According to a recent survey, even when companies are compliant with all relevant legislation and regulations, data breaches still occur. "Most healthcare organizations have made compliance with security and privacy regulations a priority, but that hasn't slowed the data-breach bleed."[9] Even when companies work for compliance with HIPAA, HITECH, and other federal regulations, they are still being hacked, and PHI is still being compromised. Enforcing the requirements of HIPAA, HHS has begun imposing financial penalties on healthcare organizations that compromise their patients' records. .[10]

Stanford Hospital in California recently reported that it was a victim of a privacy breach resulting in information about thousands of patients being posted online. Names and diagnosis codes for 20,000 patients remained posted on a commercial Web site for almost a year without being discovered. The Web site also contained medical record numbers, hospital account numbers, emergency room admission and discharge dates, and billing charges.[11]

In 2009, a hacker broke into a database at the Virginia Department of Health Professionals, encrypted the records, and then deleted the backup data. The hacker demanded $10 million in exchange for a password to the encrypted records. The database included patients' names, ages, addresses, Social

---

[7] Kennedy, K. (2011, September 12). *HHS Seeks Better Patient Access to Electronic Records.* Retrieved from http://www.newsfactor.com/story.xhtml?story_id=80146
[8] *Realizing the Full Potential of Health Information Technology to Improve Healthcare for Americans: The Path Forward.* (2010, December). Retrieved from http://www.whitehouse.gov/sites/default/files/microsites/ostp/pcast-health-it-report.pdf
[9] Higgins, K. J. (2011, May 27). *Survey: Breaches Cost Some Healthcare Organizations $100K Per Day.* Retrieved from http://www.darkreading.com/database-security/167901020/security/news/229700106/survey-breaches-cost-some-healthcare-organizations-100K-per--day.html
[10] *Data breaches compromise nearly 8 million medical records.* (2011, June 1). Retrieved from http://www.homelandsecuritynewswire.com/data-breaches-compromise-nearly-8-million-medical-records
[11] *Stanford Privacy Breach Puts Patient Data Online.* (2011, September 12). Retrieved from http://www.newsfactor.com/story.xhtml?story_id=80114

Security and driver's license numbers, which the thief could sell as personal information even if the buyer was not interested in the medical information.[12]

The threat from data breaches is real and potentially very dangerous. Several recent reports and investigations highlight the security and privacy issues related to electronic medical record systems. A report from the Health and Human Services Department found that more than 7.8 million people had their medical information compromised by 252 major breaches in a 15-month period. According to the report, smaller breaches affected another 30,500 people.[13] Another report, "Veriphyr's 2011 Survey of Patient Privacy Breaches" found that more than 70 percent of the organizations surveyed had suffered one or more breaches of PHI in the previous 12 months.[14]

A recent Ponemon Institute study found that 60% of healthcare providers had more than 2 breaches in the past year, with the average breach costing $2 million. In the same study, 70% of hospitals said that protecting patient data is not a priority, and 58% said that they have little or no confidence in their ability to protect patient records in their possession.[15] In a recent investigation of security measures at U.S. health care facilities, the HHS Inspector General found unencrypted personal information on computers in seven large hospitals that could be easily accessed by unauthorized users.[16]

It is no wonder then that in a recent blog post, Dale Peterson writes that security of electronic medical record systems "is essentially 10 years behind" and that even when providers are told that there are vulnerabilities, very little is done to fix them.[17] Ernie Hood, vice president and CIO of the Group Health Cooperative, says, "The healthcare industry is on the verge of a major shift. Organizations are venturing into the electronic world for the first time as practices implementing electronic health records and states are launching health information exchanges. A surge of new data will be brought online by a lot of inexperienced organizations fueled by monetary government incentives. Mistakes are a certainty. Combine this with sophisticated approaches to identity theft by organized crime, and breaches will happen."[18]

There are serious potential consequences for victims whose information is compromised. Patient data can be sold to criminals for identity theft, but can also be used to commit medical identity theft, where stolen patient information is used to obtain medical care for someone else. Medical identity theft taints the medical record of the victim, and can cause problems with future treatment and insurance providers.[19] Electronic medical records could be a prime target for cyber criminals, since healthcare providers bring together personal, medical and financial information all in one place. Many are also concerned that insurance and drug companies could access and use patient information to make decisions for patient

---

[12] Vijayan, J. (2009, May 6). *'Hacker' threatens to expose health data, demands $10M.* Retrieved from http://www.computerworld.com/s/article/9132625/_Hacker_threatens_to_expose_health_data_demands_10M
[13] Pulley, J. (2011, September 7). *Health Data Breaches Documented.* Retrieved from http://healthitupdate.nextgov.com/2011/09/protected_medical_information_including_patient.php
[14] *Over two thirds of hospitals and healthcare service providers suffered privacy breaches last year .* (2011, June 9). Retrieved from http://www.securitypark.co.uk/security_article266684.html
[15] Chronister, R. (2010, December 27). *Healthcare & Security: A Hacker's Perspective.* Retrieved from https://www.infosecisland.com/blogview/10538-Healthcare-and-Security-A-Hackers-Perspective.html
[16] *Data breaches compromise nearly 8 million medical records.* (2011, June 1). Retrieved from http://www.homelandsecuritynewswire.com/data-breaches-compromise-nearly-8-million-medical-records
[17] Sawyer, J. H. (2011, August 18). *Medical Device Security Under Fire At Black Hat, DefCon.* Retrieved from http://www.darkreading.com/blog/231500306/medical-device-security-under-fire-at-black-hat-defcon.html
[18] *Experts Forecast Top Seven Trends In Healthcare Information Privacy For 2011.* (2011, January 4). Retrieved from http://www.darkreading.com/security/news/229000092/experts-forecast-top-seven-trends-in-healthcare-infomration-privacy-for-2011.html
[19] Messmer, E., & Greene, T. (2011, September 9). *Warning: HIPAA has teeth and will bite over healthcare privacy blunders.* Retrieved from http://www.networkworld.com/news/2011/090911-hipaa-250659.html

treatment. It is also difficult to quantify the consequences from leaked records, which can ruin the victim's reputation.

Some are concerned that digital medical files could even be a target for terrorists or a nation state during war. Chad Skidmore, director of network services for Inland Northwest Health Services, explains hackers could infiltrate a health system and change patient records, leading to deadly consequences and destabilizing the population.[20]

Another threat to consider is the threat to patients' health when there are flaws and faulty IT systems. Some doctors say that current computer systems can increase errors, add hours to doctors' workloads and compromise patient care. The Senate Finance Committee has received numerous reports claiming that computer flaws have caused errors in patient care. One report said that faulty software miscalculated intracranial pressures and confused kilograms and pounds. Another anonymous report says that a vendor-updated program miscalculated patient dosages. One computer system accidentally prescribed adult dosages to children, and another misdiagnosed five patients with herpes.[21] Full reliance on IT health care systems seems very dangerous, especially when doctors may not question the information given to them by software programs that could be flawed or tampered with.

There are also financial consequences for healthcare companies as a result of data breaches. In early 2011, a Massachusetts hospital was forced to pay $1 million in penalties after the loss of records containing the personal health information of 192 patients. In addition to the $1 million penalty, Massachusetts General has also agreed to implement a plan to secure patient information including encryption policies for data on laptops and portable devices.[22]

Take two aspirins and call me in the morning...

Because many medical records are lost when laptops or hard drives are stolen or lost, it is important to look at solutions that address securing data at rest. Patient information should always be encrypted when stored and healthcare organizations could also consider using software to prevent sensitive data from being saved on unencrypted hardware. There should be clear standards for storing HIPAA-governed data on PCs and laptops, and storage methods should be monitored for compliance.

Insider threats are particularly difficult to defend against with electronic record security, since health professionals must have access to patient records in order to treat them. "It is important to keep in mind that covered entities can be doing everything possible to protect information, by having policies, procedures, training, physical and technical controls in place. But, they have to give their workers enough access to information to do their job responsibilities. It is a fact of human nature that some people will do bad things with their authorized access if they are sufficiently motivated."[23] So what does this mean? If security policies do not always work, and training does not always work, there must be a different approach to combating insider threats. The only solution for health care organizations is to limit health care workers' access to very specific information sets, and only the information that is necessary for them to perform their job. "Unless an employee needs access to sensitive data to successfully complete their job function, they shouldn't have access. Levels of access controls need to be implemented. Meaning, a

[20] Brewin, B. (2009, November 20). *Electronic health records could be a deadly target during a cyberwar.* Retrieved from http://www.nextgov.com/nextgov/ng_20091120_8634.php
[21] Mostrous, A. (2009, October 25). *Electronic medical records not seen as a cure-all.* Retrieved from http://www.washingtonpost.com/wp-dyn/content/article/2009/10/24/AR2009102400967.html
[22] Wilson, T. (2011, March 1). *Hospital Pays $1 Million Penalty For Loss Of Patient Data.* Retrieved from http://www.darkreading.com/insider-threat/167801100/security/privacy/229219606/index.html
[23] *HIPAA Compliance Investigations And The Insider Threat.* (2011, February 2). Retrieved from http://privacyguidance.com/blog/2011/02/02/hipaa-compliance-investigations-and-the-insider-threat/

receptionist/front desk person should not have the same access permission to patient data or any other sensitive data that a doctor would have access to."[24]

Health care organizations could also consider software solutions to some privacy issues. There is already a software program, patented by the National Institute of Standards and Technology, which allows an algorithm to be placed in larger software, controlling access to information systems. John Barkley, the algorithm's controller, says the software could improve security and patient privacy by limiting access to patient information. The software compartmentalizes medical workers and automatically provides them access to records when they need them. Barkley explains, "Once you've been admitted to the hospital, the admissions staff doesn't necessarily need access to your records anymore…Using the algorithm we patented, those staffers would only be able to access your record during admission processing. After that, they would find your information unavailable – though the doctor treating you would still have access to it."[25]

Some experts suggest that we will never be able to design a system that prevents all compromises, and that we should instead work on legislation that makes it illegal for insurance companies and employers to discriminate against individuals based on medical conditions. Dr. David Brailer, the first national coordinator of health information under President George W. Bush, says that it is unrealistic to believe that medical records will never be compromised, and that "hacks are unfortunately going to be part of the landscape."[26] Health care organizations are beginning to shift their focus from the implementation of secure EMR systems to developing policies on how they will share patient information and records.

Health care organizations should already require background checks for employees. Careful screening is required for professionals who will handle sensitive data. Organizations can also improve their physical security and must especially emphasize the importance of never leaving laptops and mobile devices unattended, as a large number of medical record breaches occur from the loss or theft of laptops and storage devices. Health care organizations must also invest in an IT staff that can perform penetration testing, website security assessments and social engineering exercises, especially to see where policies and procedures fail and where human error can hurt security.[27]

Health care organizations should take additional precautions to ensure they are HIPAA compliant, and to better understand vulnerabilities. Every health care organization, even smaller companies, should designate an information security officer. Access control is also very important, and every user in a health care organization should have their own unique log-in credentials when accessing patient systems. Outdated information should be stored securely or destroyed.[28]

Many security issues cannot be fixed with more robust IT policies, since many medical data breaches are caused by poor decisions from managers and employees. "You can put up all the firewalls, anti-malware, and intrusion prevention you want for the outside of your network, but you are your own enemy on the inside of your network," says Jeff Bills, vice president of IT at Solutions Healthcare Management. Staff

---

[24] Chronister, R. (2010, December 28). *Healthcare and Security: A Hacker's Perspective.* Retrieved from https://www.infosecisland.com/blogview/10538-Healthcare-and-Security-A-Hackers-Perspective.html
[25] *NIST Developed Software to be Used to Protect Health Data.* (2010, July 13). Retrieved from http://www.thenewnewinternet.com/2010/07/13/nist-developed-software-to-be-used-to-protect-health-data/
[26] *Data breaches compromise nearly 8 million medical records.* (2011, June 1). Retrieved from http://www.homelandsecuritynewswire.com/data-breaches-compromise-nearly-8-million-medical-records
[27] Chronister, R. (2010, December 28). *Healthcare and Security: A Hacker's Perspective.* Retrieved from https://www.infosecisland.com/blogview/10538-Healthcare-and-Security-A-Hackers-Perspective.html
[28] Baumstein, A. (2009, February 28). *Time to get serious about HIPAA.* Retrieved from http://www.informationweek.com/story/showArticle.jhtml?articleID=214600332

members must be trained carefully and taught to maintain "an atmosphere of privacy."[29] Employees must be trained on what data is sensitive, what cannot leave the premises, how information can leave the premises and how to properly secure and monitor information. "Proper IT staff security training is essential to better lock down networks, wireless, mobile devices, and more."[30]

Finally, there's the role of the patient. Patients feel that they have not been properly educated on the benefits and risks with electronic records. A recent poll of 2,720 U.S. adults found that less than one in five adults have discussed electronic medical records with their health care providers. Almost four out of five of the respondents said they worried that hackers would steal their information, and two-thirds worried that their information would be misused.[31] These concerns can and should be alleviated by better education on how EMRs are used, the advantages and cost savings to the patient of using such a system, and the ongoing efforts to protect patients' privacy. After all, the patient's physical condition will likely depend on it. And although patients have only a limited role in protecting the security of their EMRs, they should be involved in ensuring their accuracy. Patients and providers need to work together to ensure that only authorized users have access to a patients' information, and that information contained in a patient's electronic record is accurate.

Current legislation and regulations governing the migration to electronic medical record systems have not resulted in the fielding of effective and secure EMR systems. The rush to digitize health information and the lack of priority given to patient privacy and data security has left patient information vulnerable to insider threats, breaches, and financial or medical identity theft. To improve patient data security, health care organizations must improve physical security and policies that address transferring and storing patient information. Health care organizations must also focus heavily on training employees on the importance of patient data privacy, while simultaneously implementing access control solutions to minimize access to sensitive patient information as much as possible. Organizations should also begin educating patients about how their information is used, and how it can be accessed. The transition to digital medical records could transform the health care industry by ensuring better patient care, improved efficiency, cost savings, and reductions in medical errors, but the rush to implement digital systems must not come at the cost of patient privacy and security.

[29] Messmer, E., & Greene, T. (2011, September 9). *Warning: HIPAA has teeth and will bite over healthcare privacy blunders.* Retrieved from http://www.networkworld.com/news/2011/090911-hipaa-250659.html
[30] Chronister, R. (2010, December 28). *Healthcare and Security: A Hacker's Perspective.* Retrieved from https://www.infosecisland.com/blogview/10538-Healthcare-and-Security-A-Hackers-Perspective.html
[31] Pulley, J. (2011, September 7). *Health Data Breaches Documented.* Retrieved from http://healthitupdate.nextgov.com/2011/09/protected_medical_information_including_patient.php