Security and Privacy: Clinical Case Studies

Neal Sikka, M.D.
The George Washington School of Medicine and Health Sciences
The Department of Emergency Medicine

Report GW-CSPRI-2011-3

April 8, 2011

Abstract

While information systems are rapidly becoming the backbone for providing health care services, education, and research, a clinical perspective of security and privacy issues in health care is often missing from technology discussions. Without this perspective, it is likely that systems produced will not be optimal from either a medical or computer science point of view. We here use clinical case studies to bring to life the effect of regulations related to the Health Insurance Portability and Accountability Act (HIPAA). Impacts on medical research, public health, emergency preparedness, mobile health care, and implementation of new Health Information Technology (HIT) systems are discussed.

Work supported by the Office of the Vice President for Academic Affairs and the School of Engineering and Applied Science of the George Washington University

Security and Privacy: Clinical Case Studies

Neal Sikka, M.D.
The George Washington School of Medicine and Health Sciences
The Department of Emergency Medicine

While it may seem that physician ethics, morals, and commitment to the Hippocratic Oath should be the cornerstone of privacy in healthcare, the rapid reliance of technology in health care with widespread digitalization of health care data required the development of formal regulation. The Federal government recognized the need for strict, but flexible standards for privacy and security in health care through the 1996 Health Care Insurance Portability and Accountability Act (HIPAA). This document will discuss the key principles and applications of HIPAA, special topics as addressed by the Department of Health and Human Services (HHS), and breach as a driver to investments in technology.

The enactment of new HITECH rules since November 2009 have raised penalties for breach of personal health information (PHI) by covered entities to fines that range from $100 to $50,000 per individual patient violation. It is obvious the financial impact that federal regulations related to health care privacy and security can have on an individual provider or hospital. However, from a patient perspective, they often do not recognize the investment and effort involved in maintaining their privacy and security. It is perceived that a patient just signs a sheet a paper that authorizes use of their information; but, there is little explanation around the details of the disclosures outlined in what seems to be complicated legalese.

HIPAA has two major elements: Privacy and Security. The privacy framework relates to how a covered entity (CE) discloses PHI and the individual patient's right to privacy. The CE should ensure that individual's PHI remains confidential, that the integrity of the PHI is maintained, and that the PHI is made available to those entities the individual has authorized disclosure. These three warrantees apply to any PHI that the CE creates, maintains, or transmits. The CE should also ensure that the individual has access to their PHI and that it will protect PHI from threats to patient privacy (1). The security framework is applied through three safeguards: administrative, technical, and physical.

The Privacy framework serves as the building blocks for security. Regulations, privacy principles, standards, and business needs are the very bottom layer(3). The next layer that builds upon those elements is the goals and objectives of the health care organization(3). These two layers must be viewed in the context of a risk assessment that is conducted when new business is initiated, new workflows are created, or at some regular interval (2,3).

The administrative block of the security framework is made up of elements such as data minimization, training, and auditing(3). The physical block includes elements such as secure

use, transport and storage (3). Finally, the technical block is often considered encryption, but may also include new security solution technologies in software, hardware, and services (2,3).

The HIPAA privacy and security principles ensure certain rights for the patient and their health care information. First, patients have the right to correct an error in their medical record. Next, they should have access to their record within a reasonable amount of time and are able to make the determination of to whom their data can be disclosed. The covered entity is accountable to discloses your private medical data to only those you have authorized disclosure. The covered entity is also accountable to put in place security safeguards to protect patient PHI as well as for auditing who access to PHI and reporting breaches of PHI. The covered entity has obligations to make notifications to the individual patient whose data was breached as well as report to HHS and potentially the media based on the number of records breached. A breach investigation may ensue and could incur financial penalties for the covered entity (2).

One of the key principles in health care privacy management is the "minimum necessary standard."

> *"The Privacy Rule generally requires covered entities to take reasonable steps to limit the use or disclosure of PHI to the minimum necessary to accomplish the intended purpose."(2)*

This wording is vague and flexible to allow for the ease and expediency often required to provide high quality clinical care, clinical information management, and medical billing. Especially in clinical care, the minimum necessary standard may be not be applied, as in requests by a health care provider for treatment purposes.

Covered Entities

So, who are covered entities and who are not covered entities? There are essentially three buckets that covered entities fit into:

> Health Care Providers – Doctors, Clinics, Psychologists, Dentists, Chiropractors, Nursing Homes, Pharmacies
>
> Health Plans - Health insurance companies, HMOs, Company health plans, Federal and State Health care programs
>
> Health care clearinghouse – organizations that process or facilitate the process of nonstandard format health information into standard formats

Organizations that are not considered covered entities include: Life Insurance, Employers, Workers Compensation Carriers, Schools, Child Protective Services, Law Enforcement, and Municipal Offices. It is important to note that these types of organizations do not need follow

HIPAA regulations. They may have their own internally develop privacy and security policies or may follow of local or state guidelines (2).

Organizations that are covered entities must bear the burden of proof that they train their workforce on implemented policies and procedures as related to HIPAA regulations. They must also document and be able to provide an audit report of training for employees as well as user level access to PHI. The CE must be able to demonstrate that all appropriate notifications for breach were made or that no breach occurred (2).

To determine if an organization is a covered entity, use the decision trees available at https://www.cms.gov/HIPAAGenInfo/Downloads/CoveredEntitycharts.pdf

Business Associates

Business Associates (BA) perform functions or assist in functions or activities that involve the use of or disclosure of PHI for covered entities. A covered entity may utilize a BA to perform services such as claims processing, data analysis, utilization review, quality assurance, billing, benefit management, or practice management (2). Other activities performed by business associates for covered entities may be legal, actuarial, accounting, or consulting (2). Some examples of business associates may include electronic medical records vendors, companies sponsoring research, companies involved in innovation, product development and testing, or companies providing hosted video teleconferencing services for telemedicine.

HIPAA requires that a covered entity have a business associate agreement in place with companies who are BAs to ensure defined limits as to how the BA is allowed to disclose PHI. The BA agreement should also describe the process for the BA to report to the covered entity any violations of the disclosure limitations (4).

Special Topics

Public Health

For the protection of the public health, HIPAA regulation may allow CEs to disclose PHI. The objective of these disclosures include preventing or controlling disease outbreaks, risk of injury, or disability to organizations such as the Center for Disease Control and Prevention (CDC) or state or local health departments. These disclosures may be necessary for controlling the spread of sexually transmitted diseases or in cases of child or elderly abuse or neglect. They may also help the Food and Drug Administration (FDA) determine risk from pharmaceuticals or medical devices. Work place disease surveillance also falls under disclosure related to public health (5).

Research

Medical research requires the approval of the Institutional Review Board (IRB). Studies with minimal risk and no PHI may be granted as expedited or waived studies, but most studies do require the study participants to grant informed consent. The informed consent document outlines the objectives of the study, what is entailed in the subjects participation, any anticipated risks of participation, and details around how patient's confidential information will be protected. Investigators should ensure privacy and security of any records that have identifiable information. Research generally falls under the minimum necessary principle (6).

Emergency Preparedness

HIPAA regulations are designed to allow for access to information required to treat patients, as well as billing and operations, during a disaster. In fact, the Secretary of HHS can order a suspension of certain rules for specific entities during a national disaster declaration (7). For example, a master patient index of all patients in multiple hospitals within a geographic location may be kept secure and unavailable to each other hospital in a network. When a disaster meeting the requirements of establish policy occurs, the designated individual can allow the master index to become available to all hospitals in the network to help separated family members determine if they should look for a loved one at a another networked hospital.

Genetic Information

Genetic Information Nondiscrimination Act (GINA) is design to prohibit discrimination based on genetic information in health coverage as well as in employment. In general, genetic information is to be treated at PHI (8). This area is in its infancy and is yet to be fully defined.

Mobile Health

Mobile health refers to mobility in health care. This includes both mobile phone base application as well as wireless devices in the hospital, clinic, or home. Increasing mobility in health care, especially the use of laptops, smart phones, and tablets, is associated with increase security risk. Management of portable devices provides challenges to the enterprise to manage data during loss or theft. Mobile data must also be encrypted on the device, during transmission, and in use. A challenge in the area of wireless devices includes the correct association of wireless devices with the correct patient. Health care organizations should make sure that the use of mobile devices occurs in the appropriate business case and with a well thought out risk assessment.

Personal Health Records (PHRs)

A Personal Health Record (PHR) is an individually controlled health record that allows the patient to manage and track their health as well as share their data with whom they want. Unfortunately, adoption of PHRs has been very slow, with less than 10% of patients reported using a PHR. Interestingly, HIPAA does not apply to PHRs that are not offered by covered entities. These PHRs are governed by the privacy policies of the entity that offers them and

potentially other state or local regulations. However, HIPAA regulations do apply to how PHI held by a covered entity enters the PHR. This is probably why there are often multiple steps required by your provider to release records directly to populate a self standing PHR like Google Health or Microsoft Health Vault (9).

Breach

Breach is the impermissible disclosure of information by a covered entity or business associate which compromises the privacy and security of PHI. Breaches may be subject to notification requirements or financial penalties based on the type and extent of the breach (4).

The North Carolina Healthcare Information and Communications Alliance, Inc. (NCHICA) has developed a Risk Assessment tool to determine if notification of a breach is required. A reportable breach is a disclosure of unsecured PHI that violates HIPAA privacy regulations. However, there are criteria that exempt a covered entity from having to report the breach. The first exemption is an unauthorized access of PHI by an employee of the covered entity that is performed in good faith and within the scope of their organizational role. The second exemption is the inadvertent disclosure of PHI to another authorized person in the covered entity that is not disclosed further. The third exemption pertains to unauthorized disclosure of PHI which realistically cannot be retained by the unauthorized person (10).

Breaches must be reported to individuals whose PHI has been disclosed and in some cases to the Office or Civil Rights and the Secretary of HHS. Breaches involving more than 500 individuals must be reported to the media. The CE has the obligation to report breaches in a timely manner and cooperate with any investigations initiated by HHS (4).

Unauthorized disclosures of PHI are a significant problem for health care organizations. Between September 2009 and September 2010 there were 166 data breach incidents involving over 500 individuals (11). The total number of individuals involved with those breaches was 4,905,768 (11). The largest incident exposed 1,220,000 individuals (11).

The average organization cost for a breach increases almost ten percent from 2008 to 2010 to over $7.2 million. Similarly the average cost of breach per individual record costs health care organizations over $200, also about a ten percent increase from 2008 to 2010. The elements that are included in these costs are the lost business associated with loss of credibility, the post breach response, the notifications expenses such as mailings, and the investment for detection and escalation (11).

Case Studies

Controlling access to online PHI through Medical Staff Portal

Challenge: A busy academic hospital that grows rapidly often acquires multiple clinical information systems that are forced to interface with each other. Physicians and other

practitioners require access to each system and may have workflows that require access to multiple systems at the same time. In addition, practitioner responsibilities often require them to complete documentation or access clinical information at home and at off hours.

Solutions: The Hospital deployed for all providers a portal that houses all clinical applications. The portal uses a Citrix client to provide access to registered providers. The Hospital also implemented a single sign on program to limit loss of multiple passwords associated with numerous clinical information systems. The portal has allowed the Hospital to better control access to clinical systems outside of the hospital as well as improve the ability to audit use of remote access.

Controlling access to PHI in clinical area, specifically for research study recruitment

Challenge: An increase in the number of clinical research studies and the use of undergraduate students as research assistants for subject recruitment was perceived as risk for a medium sized academic hospital. Student were enrolled at the affiliated University but still required a credentialing process to be able to be in the clinical area of the hospital and access clinical systems. The Hospital wants to meet IRB, HIPAA research regulations, and follow the minimum necessary principle.

Solutions: The Hospital developed tighter controls to manage research assistants and their association with specific research projects. Each provider conducting research is now tied directly to specific IRB number. Each research assistant must meet certain HR requirements (ie. Vaccinations, drug screening) as well as go through HIPAA training at the Hospital. However, access to the EMR has been eliminated for the time being for all research assistants. The Hospital is exploring possibilities to create a server with a copy of the EMR data that is de-identified and updated in real time for research assistants to scan for possible study subjects.

Securing Mobile and Portable devices

Challenge: As a large multi-specialty academic medical practice, providers are often utilizing laptop computers and mobile devices in patient care and research related activities. Tracking, securing, and managing the numerous devices to mitigate loss, theft or other breach is important to the enterprise.

Solution: The medical practice has taken a number up steps to mitigate risk related to the increased use of portable and mobile devices. First, an email filter that automatically selects outgoing email that may contain PHI and sends it through a secure portal. Second, the IT department has moved the EMR to be hosted on a Citrix thin client. Finally, IT has increased accountability and enforcement of laptop registration and remote controllers. Additionally, new policies have been implemented to scrub devices that have been used overseas for viruses and malware.

Health care trends and Risk Mitigation

Numerous factors are driving health care towards an increase in digitization of both data and workflows. Health care providers at all levels and in all roles are becoming more mobile. Electronic health information exchange, new care models, and changes in health policy are creating new challenge in maintain privacy and security of health care information. It is clear that there is increased risk and increased costs associated with that risk, both with large business impacts (3).

Health care organizations are prioritizing risk mitigation efforts. Some areas of focus include ensuring that encryption of PHI occurs at rest, in transit, and in use. Administrators are enhancing efforts to improve compliance with privacy and security policy and procedure. IT departments are examining various hardware and software solutions to mitigate risk from theft and loss of portable and mobile devices such as virtualization, full disk encryption, and processor controls (3). Close collaboration with clinical information system vendors and third party technical solutions can lead to improvements in authentication procedures to access PHI. The near future will see the increased use of biometrics, RFID and other similar technologies.

Health care is rapidly changing. Many aspects of clinical practice, new business models, and evolving policy and regulation make the environment somewhat unpredictable. However, what is clear is the movement to digitization and mobility. These changes are sure to expose new vulnerabilities. Mitigating privacy and security risks requires a pro-active approach driven by high stake consequences associated with breach that can hurt patients, be expensive, and damage reputations.

References

1. http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/privacysummary.pdf Accessed March 21, 2011
2. http://www.hhs.gov/ocr/privacy/hipaa/understanding/srsummary.html Accessed March 20, 2011
3. Houlding, D. "Healthcare Security and Privacy", presentation shared March 2011. Intel Corporation.
4. Heide, C. "Breach Notification for Unsecured Protected Health Information" presentation May 11, 2010. Accessed online March 17, 2011 at http://csrc.nist.gov/news_events/HIPAA-May2010_workshop/presentations/1-3a-breach-notification-heide-ocr.pdf Office of Civil Rights, Department of Health and Human Services.
5. http://www.hhs.gov/ocr/privacy/hipaa/understanding/special/publichealth/index.html Accessed March 21, 2011
6. http://www.hhs.gov/ocr/privacy/hipaa/understanding/special/research/index.html Accessed March 21, 2011
7. http://www.hhs.gov/ocr/privacy/hipaa/understanding/special/emergency/index.html Accessed March 21, 2011
8. http://www.hhs.gov/ocr/privacy/hipaa/understanding/special/genetic/index.html Accessed March 21, 2011
9. http://www.hhs.gov/ocr/privacy/hipaa/understanding/special/healthit/phrs.pdf Accessed March 22, 2011
10. *Preventing a Data Breach and Protecting Health Records*, Kaufman, Rossin & Co. White Paper 2011
11. *2010 Annual Study: U.S. Cost of a Data Breach* , The Ponemon Institute, March 2011

Dr. Neal Sikka, M.D.

The George Washington University School of Medicine and Health Sciences

The Department of Emergency Medicine

Dr. Sikka is a Board Certified Emergency Physician at The George Washington University Hospital and Director of the Section of Innovative Practice at the GW Medical Faculty Associates. He serves as the Co-Director for both OnSite Medical Access and Global Health Services. He also oversees the GW Medical Transport Service and is the ED Information System Physician Application Manager.

Dr. Sikka has been a faculty member of the Department of Emergency Medicine since 2003 and is a Fellow of the American College of Emergency Physicians. His interests liein medical informatics, telemedicine, mobile health, travel and tourism medicine, and innovative medical practice and design.