United States Senate

Committee on the Judiciary

Testimony before the Subcommittee on Privacy, Technology and the Law

Implementation and Enforcement of Privacy Rules

and the Electronic Health Record

November 9, 2011

Kari L. S. Myrold
Privacy Officer
Hennepin Healthcare System, Inc.
d/b/a Hennepin County Medical Center
Minneapolis, Minnesota

Introduction

Mr. Chairman, Ranking Member Coburn, distinguished members of the Subcommittee, thank you for this opportunity to testify on behalf of a hospital that has implemented an electronic health record and information privacy and security rules for that record. My name is Kari Myrold and I am here on behalf of Hennepin County Medical Center in Minneapolis as their Privacy Officer.

Organizational Overview

Hennepin County Medical Center (HCMC) is operated by the Hennepin Healthcare System, Inc., a public subsidiary corporation owned by Hennepin County. HCMC is a 477 bed safety net teaching hospital with numerous in-house and specialty clinics and six primary care clinics located throughout the metro area. HCMC has been recognized for 15 straight years on the *US News and World Report* list of top hospitals. HCMC is:

- Minnesota's premier Level 1 Adult Trauma Center and Level 1 Pediatric Trauma Center with many nationally recognized programs and specialties and approximately 100,000 Emergency Services visits annually;
- The third largest hospital in Minnesota, based on operating revenue;
- An essential teaching hospital for numerous students of many professions including doctors and over 1000 medical residents each year;
- A safety net hospital providing care for low-income, the uninsured and vulnerable populations; and
- A major employer and economic engine in Hennepin County.

Electronic Health Record History

In late 2002 HCMC embarked on a journey toward an electronic health record (EHR). HCMC chose to replace a number of "best of breed" applications that had been implemented throughout the

organization. These individual models did not interface with one another. HCMC wanted a fully integrated clinical and revenue cycle system for its hospital and clinics. This $68M capital investment was supported by a return on investment analysis demonstrating a seven year payback which is on schedule to deliver. HCMC was driven in this endeavor by a vision that included enhancing the experience of its patients, improving patient quality and safety, supporting research and education, and sustaining the financial viability of the organization.

Principles that guided HCMC along the way included designing an EHR that would support standardized workflow, creating an environment to enhance the patient and provider experience, and improving clinical and financial performance. Design also included an environment that would be patient-focused and actively engage patients in their care. It was also a desire of HCMC to standardize processes and tools throughout the enterprise and capture current data for measurement and continuous improvement. More importantly, HCMC wanted to be able to facilitate communication between caregivers for coordinated interdisciplinary care.

EHR vendor selection involved over one hundred full-time and temporary staff from interdisciplinary teams who drafted the design criteria; it took two years to go from design phase to a signed contract. HCMC used a phased approach for implementation, with six waves occurring from 2005 - 2007. Since that time, HCMC has continued to add functionality for specialties as well as becoming an early adopter of Epic's Care Everywhere® (health information exchange application), MyChart® (electronic patient chart access application), and most recently, Care Link® (a web-based application for community users). The addition of these modules allows for record sharing among providers and with our patients. The hardware and software upgrades along with regular maintenance are continuous.

HCMC has representatives on all of the major e-Health Committees in Minnesota, including HIE, Privacy and Security, and Standards. Through active involvement, HCMC is able to influence direction at the state level and collaborate with our peer organizations. HCMC is also active in the Minnesota Epic User Group and has numerous staff qualified to present at Epic conferences. The working relationship we have with our vendor has been very instrumental to our success.

Through performance and improvements in our EHR, HCMC has achieved Stage 6 (of 7) of the HIMSS Analytics EMR Adoption model; only 4% of hospitals nationwide have achieved this standing. We hope to achieve Stage 7 in 2012. In addition, and as testament to our EHR being able to capture data for measurement purposes, HCMC was an early attester to Stage 1 of Meaningful Use; only 10% of hospitals nationwide have achieved this so far.

Implementation of Privacy and Security Protections

One of the first examples to not only test the viability of HCMC's EHR, but also the privacy regulations, involved the collapse of the 35W bridge in Minneapolis on August 1, 2007. EHR was a critical help in treating our patients in a very difficult, mass casualty situation. This is what Marsha Zimmerman, HCMC's EHR Clinical Director, said about our use of the EHR after the collapse:

"The initial direction from some of the ED and ICU docs was to go back to paper, but they quickly determined that it was faster and easier to actually do their work on Epic. It also allowed us to do some first time access auditing of staff. "[1]

For a public entity, complying with federal data privacy requirements was an expansion of what Minnesota already had in place. As a public hospital, HCMC had to comply with the Minnesota Government Data Practices Act[2] already. For non-profit and other privately operated organizations federal privacy and security regulations posed a greater challenge. Minnesota also had in place the Minnesota Medical Records Act which provided protections for information privacy as well as patient's rights. [3]

When compliance with federal mandates in the Health Insurance Portability and Accountability Act (HIPAA)[4] became a reality for many organizations (April 14, 2003 for the Privacy Rule, and April 20, 2005 for the Security Rule), the way healthcare was transacted changed for the better. Although it will be a continuous climb to perfect the regulations for patients, providers and third parties, it was necessary.

Addressing Improvements to Privacy Issues Surrounding an EHR

1. Policies and Procedures for Privacy and Security Compliance

The time and effort that continues to be put into policy and procedure development by organizations is extraordinary, not to mention the amount of inconsistencies found when comparing one organization to another. When responding to an Office of Civil Rights (OCR) investigation, one of the items they review consistently is policies. They are quick to point out where a policy is lacking for compliance or enforcement purposes, but will also make helpful suggestions to improve upon an organizations effort. An initial effort to set forth model policies defining expectations would have been very helpful.

2. Business Associates

Because we are still awaiting the final rule on this topic from HHS, there is no shortage of parties still confused as to whether they are engaging in a business associate relationship. Once a determination is made that such a relationship exists, negotiating the terms of a "Business Associate Agreement" begins: Who determines if there is a breach? By what standards? Who notifies who? What

[1] Marsha Zimmerman, RN, MA, EHR Clinical Director HCMC (November, 2011)

[2] Minn. Stat. Chap.13

[3] Now known as the Minnesota Health Records Act, Minn.Stat.§144.291 - 298

[4] 42 C.F.R. 160, 162 & 164

recourse does any party have, including the multitude of patients that have had their privacy breached by a contracted party? Where do subcontractors fit in?

HCMC has stiff requirements for contracting parties that include: signing business associate agreements that limit the amount of information accessed, actually requesting the business associate to define what type of PHI they will be accessing or using and how they will be using it; requiring privacy training for EHR users; and, compliance with security requirements, including having a recent security assessment available for review.

A final rule containing additional guidance is necessary in order for all parties to better understand their roles, responsibilities and consequences.

3. Data Breach Notification

One of the key functions of having an EHR is the ability to be able to run audits for determining inappropriate uses or accesses of patient information. An EHR allows you to run reports by patient, provider, department, etc. The regulations and this new tool presented a culture change for caregivers in that they no longer were able to follow their patients due to the lack of a continuous caregiver relationship.

> "HCMC had a Security/Compliance/Legal workgroup during the implementation. We, early on, determined that we couldn't fight the rules/regulations since we weren't in charge of them, but we could design and implement a system that supported the rules and provided access to information for the staff that needed to have this information. I grew up in the Emergency Department as a nurse, and had, as did my medical and nursing peers, a concern about what happened to my patients when they left the ED. It was hard to transition to a new reality where we could no longer access a patient's to follow their care. HCMC also decided to have a balance between the EHR restricting and/or controlling access to functionality and an expectation that staff needed to only access the information they needed to do their job."[5]

While awaiting publication of a final rule on data breach notification by HHS, organizations have established independent harm analysis criteria for notification ranging from no analysis, to lengthy "objective" checklists, to holding breach team meetings in a multidisciplinary fashion in hopes of achieving consensus, to including peers of those whose privacy was breached on decision-making groups. Without guidance, there is inconsistency in application of the rules for notification.

In addition to the large breach postings it would be helpful to have a generic (non-identifying) publication of breaches that are below the 500 patient threshold indicating the types of breaches received, the process in evaluating such breaches, and how they are resolved.

---

[5] Marsha Zimmerman, RN, MA, EHR Clinical Director HCMC (November, 2011)

4. Organizational Costs of an EHR and Privacy & Security Rules:

While some organizations were adding Compliance and Information Professionals earlier, many in health care did not get started until the EHR movement picked up and enforcement of the Privacy and Security Rules became a reality. Since then, the C-Suite positions have expanded as have other related professional positions (Ex: CCO, CIO, CMIO, C/PO, C/ISO, EHR staff).

Selection of an EHR is only the beginning – annual maintenance fees, interfacing applications, upgrades, certifications for employees, training and continuing education, and infrastructure support and IT security are but a few of the added and ongoing expenses.

Breach costs – including insurance, investigations, remediation (credit monitoring), auditing and legal expenses are also of concern to providers.

5. Expansion of the definition of "covered entity"

With the expansion of EHR, there is an increasing ease of using "de-identified" data for quality, safety, research, and treatment improvements. HIPAA de-identified data is protected health information that has 18 specified identifiers removed, including demographic information as well as other unique identifiers. This is certainly known by those who are not now considered covered entities or business associates. Expanding the definition to include these future users, or those who sell or share such data without exception or consent, would further protect the privacy of patient data.

6. Encryption

Although designated as the one safety net for the protection of health information, there are far too many organizations still not finding it critical to implement encrypted systems. Cost, lack of IT resources to implement, maintain and control assets, and the perceived distant risk of a breach or lack of enforcement are perhaps some reasons why.

Closing

On behalf of HCMC, I thank you for providing us with this opportunity to share our story with regard to the use of an EHR in today's ever-challenging environment of information privacy and security. If we can be of further assistance in this or related areas please do not hesitate to call on us.