Privacy Practices in Health Records System

Yunan Chen
Department of Informatics
Institute of Clinical and Translational Sciences
University of California, Irvine
yunanc@ics.uci.edu

Introduction
Recent wide adoptions of information systems such as Electronic Medical Record (EMR) and Personal Health Record (PHR) systems move traditional medical practices into the eHealth era [1, 2, 3, 4]. The use of eHealth technologies allows easy access and sharing of health information among primary care physicians, specialists, patient, and caregivers. Nevertheless, the benefits of easy access are also accompanied by potential privacy issues [4]. In this position paper, drawn from a recent study on EMR and PHR use in a primary care clinic, I outline two types of tensions regarding privacy practices in health records systems, and provide suggestions for privacy practices in the eHealth systems.

The Study
Between February 2010 and July 2010, we conducted a research project in an outpatient clinic located in southern California. The clinic we studied is equipped with a networked EMR system that is connected with all other clinics and hospitals in the same healthcare organization. In addition, patients of this healthcare organization can access their medical records and communication with healthcare providers through an integrated PHR system.

Our study was intended to examine the use of EMR and PHR systems on information access and sharing among...
primary care physicians and patients. To do so we shadowed 140 patient visits in the exam-rooms and interviewed 16 patients after their medical visits. Below I detail two cases observed in this study regarding information sharing and privacy practices observed in this study.

**Case 1: Sharing among Providers**
The major role of primary care physicians is to monitor patients’ entire health status and be aware of patients other medical problems. Because of that, physicians always read other healthcare providers’ notes in the EMR system prior to seeing their patients. They also update patients’ medications in the EMR during the visit. The easy access to a patient’s entire medical documentations has greatly benefited primary care physicians’ work.

Nevertheless, not all patient information is accessible in the EMR. Frequently during our observations we saw primary care physicians frustrated about not being able to access psychiatrist’s notes in the EMR system prior to seeing their patients. They also update patients’ medications in the EMR during the visit. The easy access to a patient’s entire medical documentations has greatly benefited primary care physicians’ work.

**Case 2: Sharing among Patients**
The use of PHR allows patient to access their medical records and communicate with doctors through emails. By policy, the PHR system should only be accessed by patients themselves, since most information shared in the PHR system is protected personal health information. Nevertheless, during the study, we saw many family members or even friends attempted to communicate to doctors through the PHR system on behalf of the patients. Many times this is because caregivers have better computer or health literacy comparing with patients. Thus, it is often easier for caregivers to address questions more properly to physicians.

Most patients commented in the interviews that they simply shared their password for the PHR system with their spouses or children as a way to share their health information. This password sharing, however, brought in the dilemma for physicians who receive emails from
caregivers. As one physician complaint to us during the study:

This email is from my patient’s wife... and it’s sent from his account... I can’t answer her email. Now I have to call her husband to talk on the phone.

Patients could release their protected health information to their caregivers by signing an official medical information release form at the clinic. Noteworthy that once the form is signed, the designated caregivers can have complete access to the patients’ records and communicate to physicians on behalf of those patients, at any time and under any circumstance. However, the care giving relationships may change from time and time and whether the designated caregiver can or should have access to patients’ information have to be updated accordingly. This brought in the dilemma of releasing information to caregivers and protecting patients ever-change needs for privacy protection in medical practices.

Levels of Privacy Control in Health Records Systems

As what we have shown earlier in the two cases, various policies have been placed to protect patients’ privacy when using eHealth technologies: on the one hand, confidential documentations such as psychiatrist’s notes on mental illnesses are strictly protected from being viewed without any exception in the EMR system; on the other hand, patients’ records can be completely shared with caregivers after signing the official medical information release form. The organizational policies protect patients’ privacy in one mode regardless what the actual patient care situations. With respect to what has been shown in the two cases, there are certainly times when:

1. sharing mental diseases related information would avoid serious adverse effects and inaccurate diagnosis;
2. patients agreed to share health information with their spouses at one time, but not in the future when their relationship end or when patients develop other diseases which they may not be willing to share with their spouses any more.

These cases suggest that instead of strictly “sharing” or “not sharing” protected health information with others, privacy practices in health records systems should consider the timing and circumstances in each individual patient’s case. In other words, granting caregivers access to medical records would be under patients’ current medical conditions and the relationship status with caregivers only. And the new consent is needed when the circumstance under which the release form was signed is altered. The design of PHR system should allow different levels of information sharing for different caregivers and enable patient self-specified what information they are willing to share with whom. Such as for the most intimate caregivers, the patient may be willing to entire medical records. Patient may only share their diagnosis or schedules with other remote family members. Doing so would eliminate the strict “sharing/non-sharing” modes and provides user-friendly privacy control in system design.

Similarly, when the benefit of having psychiatrist’s note outweighs the privacy concerns, the EMR system should allow, when necessary, primary care physicians to access certain protected notes in order to plan the
optimal treatment for patients. In this case, the EMR system should provide exceptions in protecting patients’ confidential notes and specify under which conditions the notes can be shared with primary care physicians. These concerns call for design of health records system to consider flexibility in privacy controls and providing different levels of privacy protection mechanisms for different patients needs.

Last, what we observed in the study shows that the users of health records systems often workaround privacy policies, such as most patients share their PHR system password with family members. This observation suggests that most patients may not be aware of possible consequences of sharing medical records with others, indicating the needs for privacy educations when using healthcare records systems.

References: