Information Security and Assurance for Healthcare Applications

Gerald Masson (masson@jhu.edu)
Johns Hopkins University Information Security Institute
Baltimore, MD 21218

A primary goal of the research and educational programs at the Johns Hopkins University Information Security Institute (JHUISI) has been to develop information security and assurance professionals and programs with foundational exposure and involvement to the critical and emerging field of Healthcare Security from a wide range of perspectives.

JHUISI is an academic education and research center based in the JHU Whiting School of Engineering (WSE). JHUISI focuses on information security and assurance issues from the perspectives of education, research, and development.

JHUISI developed and has been offering a Master of Science in Security Informatics (MSSI) degree since 2002. Based on the MSSI program, in 2003, JHUISI was designated as a **Center of Academic Excellence in Information Assurance Education**. The CAE/IAE designation was renewed in 2006, and then again in 2008 until 2014. Additionally, the designation of a **National Center of Academic Excellence in Information Assurance Research** was made in 2008 for the academic years 2008-2013.

From the perspective of the JHUISI research and educational programs, the potential benefits from electronic medical records (EMRs), including lab tests, images, diagnoses, prescriptions, and medical histories are without precedent. Patients and insurers can avoid repeating studies that, for example, expose people to additional radiation and incur unnecessary costs. Providers can instantly access patient histories that are relevant to future care. And patients can take ownership of their medical records, with the potential for greater privacy, and better access to their records when they are needed.

However, while the promises of EMRs are seductive, moving from paper-based systems to electronic ones is not without risk. For example, it is a lot easier for an attacker to sneak out of a hospital (or data center) with a USB stick in their pocket containing 8,000 patient records, than with boxes containing the equivalent paper records. Moving electronic records online makes them particularly vulnerable to Internet- based attacks. These threats are getting worse, as attacks grow in sophistication, while defense mechanisms are not keeping up.

To meet the needs of the push towards EMRs, there are emerging XML- based standards, such as the Continuity of Care Record (CCR) and Continuity of Care Document (CCD). These standards call for protecting EMRs, but they do not provide enough guidance as to how such protection can be achieved. The "Standard Specification for Continuity of Care Record" states the following:

The CCR document instance must be self-protecting when possible, and carry sufficient data embedded in the document instance to permit access decisions to be made based upon confidentiality constraints or limitations specific to that instance.

Additionally, the Health Information Technology for Economic and Clinical Health (HITECH) Act puts an enormous burden on covered entities in the form of mandatory notification to the patient if unencrypted Personal Health Information (PHI) is disclosed. Clearly, encryption and authentication are needed, and these security mechanisms require key management protocols and policy management. To date, these remain largely unsolved problems for EMRs.

A primary goal of the JHUISI research and educational agenda is to develop new security technologies to enable deployment of secure EMRs.

EMRs have the potential to greatly improve healthcare and ultimately patient health in the US. However, electronic records introduce new threats to patient privacy, and so securing EMR systems is paramount. There are touted features in EMRs that require novel security solutions as well as non-trivial applications of existing technologies. For example, there is considerable effort by some major players, including Google, Microsoft, and Walmart, to provide Personally Controlled Health Records (PCHRs). These are systems that are intended to offer individuals access to, and control of, their health records. These systems can be described as "patient-centric"

There are also "provider-centric" solutions, such as that being implemented by the Children's National Medical Center in Washington DC that are designed to share EMRs among multiple providers through a centralized data center. Both of these models, patient and provider centric, come with scores of challenges and problems that must be addressed. On top of that, they operate in a highly constrained regulatory environment due to laws such as the Health Insurance Portability and Accountability Act (HIPAA).

An example is **Google Health** which is an opt-in centralized repository and service provider. It allows a subscriber to manually enter medical information such as physical characteristics, conditions, medications, and insurance; upload files of any type; share read-only access to her Google-Health profile with others; and link his/her profile with providers who have partnered with Google Health

These providers offer such services as creating medical cards, monitoring one's health and vitals, uploading lab/test results, converting paper records into electronic format, and checking for dangerous drug interactions. Subscribers can also use Google Health to search for medical programs and professionals. The data API offered by Google Health complies with a subset of the Continuity of Care Record (CCR) standard and provides software developers with an interface to the data in Google- Health profiles. Google Health recently began a pilot project that allowed some of its subscribers in Utah and Arizona who were Medicare Fee-for- Service beneficiaries to download the last 24 months of Medicare claims into their Google-Health profiles.

In addition to these systems, there are several web-based PCHR providers. They implement a cloud-based model where a subscriber's PCHR is universally accessible from any Web browser. Examples of other web-based PCHR providers include LifeOnKey.com, FollowMe.com, and MyMedicalRecords.com. Earlier this year, the Indiana University Health Center began to offer Indiana University students an online PCHR system via NoMoreClipboard.com. These providers often partner with medically-related organizations ({\em e.g.} clinics, labs, and pharmacies) to provide their subscribers with additional services such as record imports/exports, recordsharing, medical information and alerts based on the subscriber's PCHR, and monitoring of the subscriber's vitals. These systems interface with other PCHR systems via published APIs.
~