

Case Report

Patient safety and privacy in the electronic health information era: Medical and beyond

A. Cahid Civelek

Department of Radiology, Division of Nuclear Medicine, University of Louisville, Kentucky, USA

Received 18 April 2008; accepted 11 September 2008

Keywords: Patient safety; Privacy; Electronic health information; Nuclear medicine

Computers are now being used for a wide range of applications. Using the power of computers is common in many physician practices. Billing is usually the first application to be automated. Many physician practices connect electronically to hospitals and laboratories for access to results and other clinical messaging services. Electronic prescribing tools are also becoming popular.

Many initiatives point to the fact that this is the era of the electronic health record (EHR). The federal government in the U.S.A. is promising the use of health information technology (HIT) for patient safety and enhanced quality of care. Payers have started pay-for-performance efforts that virtually require an EHR for physicians to meet data reporting needs.

Electronic health records impact the patient care:

A patient's paper chart can only be in one place at one time, which impinges on the level of patient care that a physician can provide.

When physicians, nurses, and staff can access charts anytime from anywhere, patient care increases, as patient issues can be dealt with instantaneously rather than waiting hours or days to get the paper chart in the hands of providers (IMWR Vol. 22; 2: 7, 2007).

However, patient medical records contain all the information a thief needs to steal someone's identity and may include Social Security numbers, driver's license numbers, phone numbers, addresses, even checking account and credit card information. Yet providers are generally more concerned about protecting clinical information than they are about protecting their patients' identity information. Clinical data have layers of protection,

such as computer passwords and other security features, to prevent leaks, but providers just don't think about protecting identity information. It's not a natural thought process for them.

Medical identity theft is a disturbing and growing trend, however, and practices that fail to protect their patients' financial information risk their reputations, possible huge legal damages, and the expense of victim credit monitoring and counseling. Fines under the Health Insurance Portability and Accountability Act (HIPAA) for unlawfully disclosing patient data can be as high as \$250,000 and, if convicted, a person could face 10 years in prison.

Typically, physicians and other providers must notify each person whose identity information was lost or stolen, set up a call center for victims, pay legal fees of about \$1000 per victim, and pay fines and penalties for each incidence.

The US Federal Trade Commission (FTC) defines medical identity theft as the use of a person's name or insurance information without permission to obtain medical care or file false claims for medical care. The FTC reported almost 18,000 such cases in 2005. This trend affects medical practices of every size; physicians aren't doing enough to prevent HIPAA violations. The security segment of HIPAA went into effect in 2004, but compliance rates for security measures are declining. Physicians' HIPAA compliance rates are at only 38% for security. (C.P. Options February 2007).

Medical identity theft is a fast-growing crime in the USA, largely because Personal Health Information (PHI) is a valuable commodity. Some estimate that the black market value of a name attached to medical and insurance information is as high as \$60, compared with just 7 cents for a resume (Radiology Today Vol. 7 (23); 43, 2006).

There are cases in which computers were stolen and the clinical information could not be accessed because of the protection.

E-mail address: accivelek@gmail.com.

However, the business software, was on the hard drive and there was plenty of financial information easily obtainable on the computers and more savvy crooks use these financial information.

Good security is done in layers. The goal is to make access difficult enough to deter thieves, but not so difficult that personnel must take shortcuts around security safeguards. (Example: a front office worker from the Cleveland Clinic in Florida stole names, birth dates, Social Security numbers, Medicare numbers, and addresses from more than 1000 patients in the clinic's database. The worker used the information to make fraudulent Medicare claims worth more than \$2.8 million. He also sold the information to others who filed false Medicare claims as well).

Steps should be taken to improve practice security and many of these steps used to protect patient personal and financial information are common sense.

Electronic Health Record also provides means of tracking patient information on diagnostic tests that involves radiation, such as CT scans.

Since the radiation doses of CT are accumulative over time. The radiation dose that a patient accumulates over his/her life is important. The first 100 or so units of radiation are added to the

new 100 units of radiation, and the patient gets a cumulative effect.

Dose should be adapted to the size of the patient, the number of prior CT studies and to the clinical indications, which EHR help to track such information.

There are other techniques for lowering dose in children and adults. These include using a lower tube current, and that would be applicable to any protocol. For example, using a lower tube current, using automated exposure control, using a lower tube potential or kvp, using a higher pitch or using a better detector profile or geometry.

For example, a 4-slice scanner has higher dose than 64-slice scanners. The efficiency of a 4-slice scanner is around 70–80%. The efficiency of a 64-slice scanner is around 90–95%.

Although the use of EHR provides numerous advantages to patient care, there is information security concerns related to their utilization, which can be addressed with a diligent effort.

Security policies and efforts tend to break down over time. As Wayne Markert said: "Security is a journey, not a destination."

(Mackert, iTM Healthcare — 2007).