Security Concerns In E-Prescribing

Sam Nataraj, Morehead State University, USA

ABSTRACT

There has been significant growth in electronic prescriptions in the last three years. E-prescribing volume has exceeded 250 million and the number of prescribers routing prescriptions has exceeded 75,000. There has been a push from the federal government to increase e-prescriptions. There are many advantages to e-prescriptions. But, with these advantages there is also a concern regarding privacy and security of patient information. The purpose of this research is to develop an understanding of the e-prescribing processes, point out security risks, and develop ideas to reduce or eliminate those security risks.

Keywords: Electronic prescriptions; e-prescribing; security of medical records

INTRODUCTION

As defined by the National Association of the Boards of Pharmacy (NABP), e-prescribing is more than just filling a prescription. It is getting the right medication, to the right patient, at the right time.

Providers of healthcare have been writing paper prescriptions to patients for decades. "Writing prescriptions is a fundamental part of every physician's day," says David Ailard, M.D. (Blair, 2006). Doctors are accustomed to writing paper prescriptions and giving them to the patient. The patient can then take those prescriptions to any pharmacy to have it filled.

The process seems simple enough and has worked for many years; however, there are various risks involved with paper prescriptions. Some of those risks include: 1) provider errors in handwriting interpretation by pharmacists, 2) risk of fraud duplicating paper prescriptions, and 3) the inability to keep track of a patient's medication list. Healthcare providers have no way of easily tracking a patient's prescription history without thumbing through a medical chart that is likely to be inaccurate. "Physician practices spend hours every day managing prescriptions long after the original prescription has been written" (Blair, 2006). When a patient needs a refill before it was time to see the doctor again, the patient would have to call the provider. In turn, the provider would have to call the prescription renewal to the pharmacy of the patient's choice.

E-prescribing is a process of digitally sending prescriptions to pharmacies straight from the provider to the pharmacist. "Electronic prescribing (e-prescribing) has the potential to improve the safety and efficiency of medication use, but uptake of e-prescribing in community-based settings has been limited to date"(Fischer, 2008). "It has been estimated that e-prescribing systems, providing automated warnings and updated patient information at the time of prescribing, could reduce outpatient adverse drug events by 25% per year"(Fischer, 2007).

THE PLAYERS INVOLVED

The first step to understanding e-prescribing is to know who the players are in the process and what they do. The electronic prescription creator, the traffic director, and the receiver of the e-prescription are the main players. Of course, the patient is in the middle of the mix.

The patient visits the provider through normal procedures. The provider makes a medical decision based on criteria and chooses to send a prescription electronically. E-prescribing systems are different depending on the system, but all have similar functionality. The provider uses an electronic device, such as a desktop computer, tablet

PC, laptop, or personal digital assistant, to access the system. The provider will find the patient in the system, look at the medication list in the system for the patient, and search the drug database built into the system for medications being prescribed.

The provider often has many capabilities in E-prescribing systems, such as drug information, drug-to-drug interactions, and insurance coverage. After the provider digitally creates the prescriptions for the patient, the provider will have the capability of choosing any pharmacy at any location, based on the patient's choice, to send the electronic prescription. All of these actions are recorded in the e-prescribing system for future reference. The electronic prescriptions go directly to the assigned pharmacy without physically being touched.

The electronic prescriptions are transmitted through digital networks. It starts at the local area network at the location of the provider and then traverses wide area networks across the globe. In the wide area network awaits a traffic cop that houses a national database of pharmacies and their information. The largest company called SureScripts is one of these traffic cops. SureScripts receives the prescription and routes it to the correct pharmacy either via fax or completely electronically, depending on the pharmacy's capabilities.

The receiver (Pharmacist) will either receive the fax or be notified on their pharmacy system of an incoming prescription/s for the patient. The pharmacist will make sure there are no errors and will then fill the prescription. The provider back at the medical facility then tells the patient they can pick up their medicine at the designated pharmacy. By the time the patient travels to the pharmacy, the prescription is likely to be filled and awaiting the patient.

Prescription renewals are another procedure that is more streamlined with e-prescribing. A patient calls or goes to his/her pharmacist and requests medication. If there is no prescription or an outdated prescription on file, the pharmacist can send a request from their pharmacy computer system to the provider's e-prescribing system to ask the provider to renew a prescription electronically. The provider has the option to deny or approve the renewal. E-prescribing allows these actions to take place with less dependency on the phone.

SECURITY CONCERNS

E-prescribing, though useful, raises concerns of security . According to the Asia-Pacific Review, "a person's life and reputation can be greatly affected if important personal information, such as his medical records or financial information, falls into the hands of unauthorized individuals"(Asia-Pacific Review, 2003). As the power and efficiency of the technology revolution heightens, so does the security risks involved. "An underlying condition of success in electronic prescribing is the role and necessary use of standards" (Hammond, 2004). E-prescribing takes advantage of technical services, such as databases, local area networks, wide area networks, the Internet, and many technical standards to allow communication between systems. "Security is a continuous, living process for ensuring that people, networks, and information have the necessary protection required by businesses for secure, reliable day-to-day operations"(Gupta, 2007).

The first point of access is the healthcare facility. There, the e-prescribing system will be housed (a PDA, tablet, laptop, or desktop). These devices must be connected to a network either though wired or wireless network. All of these services have security risks if vulnerabilities are not patched, appropriate firewalls in place, up-to-date software, policies enforced, standards followed, and end-users trained properly. Hackers can access systems in a variety of ways if local technologies are not monitored and properly secured.

When using E-prescribing, local technical services must communicate with the external service, such as SureScripts (traffic director). External services must provide the same types of security for their technologies. Another external entity would be the pharmacy. "Following the introduction of EP, there was a significant reduction in both pharmacists' interventions and prescribing errors. Interventions reduced from 73 (3.0% of all medication orders) to 45 (1.9%) (95% confidence interval (CI) for the absolute reduction 0.2, 2.0%), and errors from 94 (3.8%) to 48 (2.0%) (95% CI 0.9, 2.7%)" (Parastou, 2007). They also have their own technology systems that communicate with the traffic director and the provider e-prescribing system.

A summary of the risk areas include the local healthcare provider's IT environment, the traffic director (example SureScripts), and their IT environment - the receiver (pharmacy) IT environment. The task seems daunting to have some type of security and conformity with so many entities and variables in the mix. The key to technology security is development, implementation, and enforcement of technology standards and policies. According to Building Secure Products and Solutions, "The inclusion of many security add-ons, such as firewalls, antivirus software, intrusion detection systems (IDSs), and intrusion prevention systems (IPSs), may imply that the security objectives were an after-thought, not adequately defined initially, or that the required security objectives were never met by the individual system components" (Gupta, 2007).

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule was one of the largest set of standards protecting patient privacy passed by Congress. A large part of the ruling deals with securing public health information and setting standards for health information technology. The International Standards Organization is another organization that develops standards for industries. These types of standards organizations need to fine tune standards that deal with E-prescribing to create a more standard and secure process. Organizations must abide by standards and promote health information security as the highest priority to ensure security for the patient and for the provider.

Organization training is another major milestone to preventing security breaches. "INFORMATION security is about people as much as procedures"(Mann, 2008).

Most breaches to technology systems occur by internal organizational employees. Prevention is the best medicine when dealing with security. Training employees to follow organizational security policies and raise their security awareness is essential. Ongoing training must continue throughout the organization with new hires and existing employees. Proper training creates an organizational culture of security and privacy. Creating standards and policies is not the problem; the most difficult part is enforcing them.

CONCLUSION

The goal of this article has been to increase the understanding of e-prescribing, promote awareness of some of e-prescribing processes that are possible security vulnerabilities, and provide some general managerial ideas on promoting a more health information security focused organization to increase e-prescribing security. The information wherein is very general and could act as a preface to a book on e-prescribing. The technology is new and there will surely be many changes and standards developed in the future. The technology is a grand step forward for the healthcare community and writing prescriptions in a safer and more legible, traceable manner.

AUTHOR INFORMATION

Sam Nataraj is an associate professor of Information Systems at Morehead State University. His research interests are: Healthcare Information Systems, Health Informatics, Computer Security and Database Security. His teaching interests are: Database Systems, Object Oriented Programming, Health Information Systems.

REFERENCES

1. AHRQ Publication No. 07-0047-EF. (April 2007). Findings from the evaluation of e-prescribing pilot sites. http://healthit.ahrq.gov/images/apr07norcerxreport/erxinterimevaluationreport.html
2. Blair, R. (2006, October). And the Winner Is…Everyone.. *Health Management Technology*, *27*(10), 46-52. Retrieved April 23, 2009, from Health Source - Consumer Edition database.
3. Donyai,P. (2007). The effects of electronic prescribing on the quality of prescribing. *British Journal of Clinical Pharmacology*. 65(2) 230-237. Lexis-Nexis
4. Fischer, M. (2007, April). The National e-Prescribing Patient Safety Initiative: Removing One Hurdle, Confronting Others. *Drug Safety*, *30*(6), 461-464. Retrieved April 10, 2009, from Academic Search Premier database.

5. Fischer, M., Vogeli, C., Stedman, M., Ferris, T., & Weissman, J. (2008, April). Uptake of Electronic Prescribing in Community-Based Practices. *JGIM: Journal of General Internal Medicine*, *23*(4), 358-363. Retrieved April 10, 2009, doi:10.1007/s11606-007-0383-1
6. Gupta, A., Chandrashekhar, U., Sabnis, S., & Bastry, F. (2007, Fall2007). Building secure products and solutions. *Bell Labs Technical Journal*, *12*(3), 21-38. Retrieved April 6, 2009, doi:10.1002/bltj.20247
7. Hammond, W. (2004). The role of standards in electronic prescribing. *Health affairs*. W4 325-327. Lexis-Nexis
8. Hong-Sun, K. (2003). Information security—now and beyond. *Asia-Pacific Review*, 10(2) 89-119. Lexis-Nexis.
9. Mann, I. (2008, January 26). Hacking the human [IT security]. *Engineering & Technology (17509637)*, *3*(1), 62-63. Retrieved April 10, 2009, doi:10.1049/et:20080119

