Electronic Prescriptions and Information Risks

Understanding risks of exposure as use of e-prescriptions increases

By Joseph E. Kelly, CISA, Security+, HIT

April 2013

White Paper

essextec
GETTING IT DONE TOGETHER

INTRODUCTION

I was recently at my doctor's office when he prescribed a medication for me. But instead of handing me the prescription scribbled on a prescription pad, the doctor typed it on his laptop, asked me what pharmacy I used and, "Presto!", my prescription was electronically sent to the pharmacy. For a moment, I thought to myself how neat and efficient that was. Then it struck me. How did my information get to the pharmacy? After all, what is a pharmacy but a retailer. We have all heard of many security and data breaches from retailers, but most of those involved credit card numbers. Now, the retailer could potentially have much more information - *personal information*.

So, what information is being sent to my pharmacy with the simple keystroke? Much more than a credit card number - which comes with the complete backing of my FDIC insured bank and the seemingly unlimited availability of TARP funds to make sure I have no out of pocket loss. Should I be concerned?

Maybe I should be concerned for the information on my medication, medical history, allergies, insurance plan and benefits, name, address, date of birth and possibly my social security (Health Plan ID) number. In fact, with all the electronic interchanges involved in such a simple transaction, my information was instantly shared with numerous intermediaries before it reached my pharmacy.

SO WHAT DOES THIS MEAN FOR US?

The Center for Medicare and Medicaid Services (CMS.gov) is offering up to a 1% bonus in 2012 to physicians who use electronic prescribing. According to the National Progress Report on E Prescribing for 2011, 570 million prescriptions were routed electronically; a 75% increase from 2010. This represents an estimated 36% of total electronic prescriptions in 2011- an increase of 22% from 2010. The adoption is expected to increase in 2013 as the proposed penalties for not using electronic prescribing will be enforced.

WHAT IS THE RISK OF EXPOSURE?

Are the prescriber's devices (desktop, laptop, tablet, phone, etc.) secure to protect patient information? Are the wired or wireless networks on which the information travels protected? Are the intermediaries for data transfer which communicate the prescription information between the software system in the physician's office to the systems in the pharmacies and to the pharmacy benefit manager (PBM) and health plans safe and secure? Are there proper controls and procedures in place to ensure personal information is not lost or stolen?

Are proper controls and procedures in place to ensure personal information is not lost or stolen?

WHAT ARE THE VULNERABILITIES?

What are the risks to the patient information? It would seem that this would be a gold mine of exploitable information that could be sold on the open market if unauthorized access were obtained. You might ask, “How could this possibly happen? Why would the computer systems not be safe?” Unfortunately, there are many reasons. Computer systems must be patched often with security and software updates. Proper processes must be implemented that keep track of the physical location of devices and access to these devices. Security awareness education alone is ineffective. The users of the systems are also required to comply with information security standards. You can have all the updated system patches and firewalls operating but if an authorized user clicks on that suspicious link in an email or website and releases the malicious code, an unauthorized person could potentially have access to personal data.

CONCLUSION

As the market tries to catch up with the security demands, our systems will remain vulnerable. The days of being able to keep our heads in the sand and say that we did not know - have gone away. There will be severe penalties if regulators, courts, stockholders, and customers determine that an organization did not perform due diligence or keep up with industry standards. Non-adherence to best practices to could lead to the loss of a practitioner’s license or suspension during an investigation. The costs associated with a data breach can be staggering. According to a recent study by the Ponemon Institute, data breaches have cost the healthcare industry an estimated $12 billion in the past two years alone.

In order to protect yourself and your organization, a risk assessment should be conducted that specifically looks at the technology that you are utilizing and vulnerabilities based on the threats to your environment. The assessments should occur on a regular basis in order to check for new vulnerabilities and threats as well as to look at how well any remediations are working.

There is a careful balance of making systems secure, operating the business, and the human element. Risk must be mitigated through implementing controls, diverting to a third party, accepting the risk, or insuring against loss. Being risk intelligent will help keep you and your organization from becoming the next data breach story.

According to a recent study by the Ponemon Institute, data breaches have cost the healthcare industry an estimated $12 billion in the past two years alone.

> Dynamic Infrastructure > Data Management / Analytics > Business Risk Services

Essex Technology Group, Inc.
> 201 West Passaic Street
Suite 303
Rochelle Park, NJ 07662
> exceed@essextec.com
> 1-888-519-1518
> essextec.com

essextec
GETTING IT DONE TOGETHER