



By Tom Troutman

“Closing the barn door after the horse is gone.”

“Pay me now, orpay me later.”

What’s your favorite phrase to help you comprehend that an ounce of prevention is worth a pound of cure? Have you noticed the “public notice” ads in the paper lately? Our Lady of Peace, Praxair, Medical Center Bowling Green, and many more have all gone through a “breach notification” process. This includes sending first class letters to everyone who may have had personal information placed at risk. They’ve had to run ads in the local newspapers, and arranged

The regulations are clear— if you have computer files that include PHI, the files must be encrypted. HITECH only recognizes two acceptable forms of PHI for electronic systems: either “encrypted” or “destroyed”.

for privacy alerts with all three credit bureaus. And it’s only the beginning of the expense—to say nothing of the impact to reputations.

Our Lady of Peace is going through all of this expense because a thumb drive can’t be found. The thumb drive had a copy of a file that included more than 500 patient’s names, room numbers, insurance company, and the admitted/discharged dates. The file did not include addresses, social security numbers, diagnosis or treatment. The thumb drive is just missing. While there’s no evidence to indicate the drive has been put to use by a “bad guy” under new federal privacy laws Our Lady of Peace must go through an expensive, laborious and painful process.

Addressable does not mean optional

If you’re not encrypting, you are at risk.

HIPAA Has Teeth

So what is going on? To put it simply, HIPAA has teeth. When the American Reinvestment and Recovery Act was approved last year, some very significant requirements were added, particularly the Health Information Technology for Economic and Clinical Health (HITECH) Act. The requirements are very much in force. If you are in healthcare, or your customers are in healthcare, they apply to you.

The new regulations require that the patient’s data be “at risk”. If you don’t protect PHI, the penalties are huge. Whereas before fines for violating a HIPAA regulation might be a maximum of \$25,000, now it is \$1.5 million.

You might think that implementing good physical access policies to protect computers from unauthorized access, and using “strong” passwords for all computers and laptops put you in compliance with the law. However, if your computer systems are not encrypting, then you are a “violatee”.

Limiting access and having “strong” passwords is good, but it’s not good enough. Medical Center Bowling Green recently had a laptop stolen, which included files with at least 500 patient names. A patient’s name alone is sufficient to qualify the data as “personally identifiable,” which makes it “Protected Health Information” (PHI). You might think a password of 12 upper and lowercase letters with numbers mixed in would be too difficult to crack. Perhaps. But that doesn’t mean the data on the laptop is protected. The laptop ran a Microsoft Operating System, and complete access to the laptop’s hard drive simply requires that you load a disk into the laptop’s CD drive and turn on the laptop. The laptop will boot up from that CD instead of the hard drive. Once finished booting, you can reset the administrator password and the hard drive and all of its files are wide open—since they weren’t encrypted.

The regulations are clear— if you have computer files that include PHI, the files must be encrypted. HITECH only recognizes two acceptable forms of PHI for electronic systems: either “encrypted” or “destroyed”.

So if it’s that straightforward, why isn’t every organization storing PHI in encrypted files? HITECH requirements for encryption are not mandated. They

are stated as “addressable”. Many organizations mistakenly interpret this as optional.

Easy Encryption Solutions

Encryption solutions are readily available. The upfront expense is reasonable. It would be hard to defend a decision not to encrypt. First, appoint a privacy and security officer. This individual should thoroughly understand HIPAA’s updated regulations and be well-versed in the privacy requirements imposed by the HITECH Act.

Second, your technology resource should deploy encryption software. Encryption of PHI is only considered secure provided that two conditions are met:

PHI is stored using encryption methodology to render the file unreadable without a unique password to view the file.

The password to that file is not compromised.

Training and supporting users is paramount. It’s not unusual for people to write passwords down on a sticky note and tape the note to their laptop or monitor. You must train users out of this behavior.

With secure PHI, you are not required to perform the “breach notification” if an event occurs where any of your PHI files are out of your control. Doesn’t that sound better than apologizing to all of your customers?

Remember, a byte of prevention is worth a grand of cure.

Tom Troutman is president of Network Advocates, Inc.

To see the entire list of violators dealing with breaches of 500 or more individuals, visit the Health & Human Services web site:

<http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/postedbreaches.html>