

THE SEMANTICS OF “TRUST” AND THE DISCONNECT WITH THE GENERAL PUBLIC

By Michael L. Nelson, DPM
Manager, Healthcare Policy and Strategy

February 2012



“ It’s not the tools you have faith in – tools are just tools. They work, or they don’t work. It’s people you have faith in or not. ”

– Steve Jobs

If you extrapolate Mr. Jobs’s quote to a healthcare-related extension, you’ll find that the general public’s fear of data breaches is rooted in the notion that systems aren’t foolproof – they’re hackable, too easily shared and age quickly. What the public is looking for is assurance that their personal and healthcare information is protected. Addressing these concerns directly with their physician or his office staff may make a patient feel less vulnerable, but oral communication about data protection can only go so far. What could seal the deal is written documentation that addresses the specific processes that have been put in place to protect the patient’s information.

GOVERNMENT PRIVACY INITIATIVES

As health information exchange technology, standards, and policies evolve, the privacy and security of protected health information (PHI), sensitive information (SI), and personally identifiable information (PII) is of the utmost concern. As a result, the HITRUST Common Security Framework, National Institute of Standards and Technology (NIST), and Data Use and Reciprocal Support Agreement (DURSA) all reference a “trust fabric” in order to comply with HIPAA privacy and security requirements. The “trust fabric” mandates that each constituent of a health information exchange is held accountable for HIPAA compliance – this includes both HIPAA covered entities and HIPAA business associates and their subcontractors.

Government regulators, standards organizations, and the healthcare industry all rely upon the “trust fabric” when they determine the necessary standards and policies to protect data, including: access management, identity authentication, and email encryption. However, the public often has a different perception of “trust”. This is a major stumbling block in adoption of electronic health records and health information exchange.

TRUST AS AN ISSUE

The healthcare industry must take into account the assumptions and experiences of the status quo. In order to do this, healthcare professionals may need to walk a mile in a patient’s shoes to understand his/her fear of sharing personal information and then figure out how to overcome it.

When patients hear the word “trust”, what they really want and need is “assurance”. Assurance can be a dicey proposition in our new-age world. Firstly, there’s no such thing as a simple one page contract. Most contracts resemble *War and Peace* and are written in arcane legalese. Secondly, our culture is rife with examples of lost trust, specifically with data privacy. Look no further than the scandals in Congress, the Catholic Church, or major league baseball to see why there’s a lack of public trust. Most people feel betrayed when seemingly respected organizations such as these are guilty of violations.

The trust issue swings both ways. Physicians fear lawsuits from patients and patients don’t trust doctor billing practices. Some patients even resort to withholding important details of their medical history such as age, medications, and sensitive information because they don’t trust the doctor to protect that information.

It’s naïve to assume that there’s sufficient trust between a doctor and patient to facilitate a patient giving carte blanche for the doctor to share his/her PHI with another doctor. A first visit, for example, may not establish the necessary trust. It’s also possible that not enough trust has been established even if the patient has been seeing the doctor for a longer period. Last but not least, people are wary of technology and “Big Brother” controlling their lives.

RAMIFICATIONS OF DATA BREACHES

If healthcare professionals stop to consider that patients are also customers, then it's not surprising that customers "want it in writing." A good start might be for the provider to offer each patient a clear and concise document, describing the safekeeping precautions taken to secure the patient's information. The document should specify how the patient's information is safeguarded as opposed to the HIPAA Notice of Privacy Practices document, which describes how the patient's data will be used and disseminated.

In light of the massive data breaches of patient records at Tricare, Sutter Healthcare and HealthNet, the ramifications of a data violation for facilities are severe from the patient's point of view.

The breach of personally identifiable information may lead to identify theft, which in turn can result in:

- Fraudulent financial activity such as drained bank accounts, damaged credit scores and loan denials
- Criminal arrests as a result of crimes committed in the patient's name
- Fraudulent benefit filings such as unemployment or tax refunds

In addition, the breach of protected health information or health plan information can lead to medical identify theft, which in turn can result in:

- Costly procedures and medical tests for a stolen identity
- Incorrect treatment or potentially life-threatening adverse drug reactions from mixed patient/stolen medical record information
- Getting turned down for life insurance because the insurance carrier believes that the applicant has a certain condition which in fact is not true
- Employment denials due to medical records checks

HIPAA Notice of Privacy Practices details the circumstances in which a patient's information may be shared with other entities. However, these notices don't give ample assurance that a patient's information is safe at the medical facility. Generic bromides such as "We take every precaution to make sure that your information is safe and secure" are condescending and simply not enough. Patients want written assurance that their data is secure from inappropriate access.

WRITTEN ASSURANCES BY FACILITY

Therefore, I propose that the medical facility distribute to each patient concise, easy-to-read patient education materials that address information safekeeping which could be entitled, "Assuring the Privacy and Security of Your Personal and Medical Information". This would describe how the facility prevents inappropriate access to the patient's information. It should include the following:

- Auditor's statement that certifies that a (named) 3rd party has performed an audit and that the medical facility uses appropriate privacy and security safeguards including:
 - Employee training on all state and federal regulations regarding the privacy and security of patient information.
 - Employee criminal background checks
 - Personnel Authentication and identity checks
 - Access control by assigning specific roles to personnel and patient data access levels
 - Ongoing audit trail of all access and/or attempts to access a patient's information
 - Encryption/encoding of patient information for all facility computers, flash drives and other electronic equipment
 - Disabling of stolen equipment
 - Supervised and proper disposal of drives, tapes and devices
 - Immediate patient notification in the event of a data breach

- Provider identity authentication performed for every provider to whom the patient's information will be sent
- Verification of the license, prescribing and sanctions status of every provider to whom the patient's information will be sent
- Encryption statement that documents all emails are encrypted to prevent unauthorized entities from opening
- A statement of remedy outlining the steps a facility will take should the patient suffer consequences as a result of a data breach

This document should be signed by a designated authority at the medical facility and HIE.

BELIEF VERSUS ASSURANCE - THE TRUE TEST

Regardless of a provider or facility adopting the written assurance approach or not, it's clear that each healthcare provider should ask, "Does the public want to *believe* that I'll do the right thing and protect their personal health information *or* do they want, need and deserve my *assurance*?" The starting point for getting a distrustful public to participate with electronic health records and health information exchange is to give them written assurance that their personal and medical information will be secure, and that all the necessary safeguards are in place to prevent inappropriate access to their information.