Vol. 1 | Issue 2 | March 2013

mihealth
Secure Instant Access

Newsletter

Patient information security
The emerging concern over email and mobile device use

Among the threats to systems identified by the US Government Accountability Office in its February 2013 report to Congress are incidents affecting individuals. The GAO cites relatively recent breaches of security at a credit-transaction processor affecting 1.5 million accounts, at a State's Department of Health affecting almost 1 million people, and at the federal Retirement Thrift Investment Board affecting over 120,000 people. The December 2012 Ponemon Institute's research report on Patient Privacy & Data Security points out that, of the healthcare organizations surveyed by them:

- 81% of medical staff and employees are allowed to connect their own smartphones, tablets, etc. to the organization's systems
- 94% have had at least one data breach in the past two years and 45% have had more than five
- the primary causes of data breaches are: lost or stolen computers, smartphones, tablets, USB drives, etc. (46%); unintentional employee action (42%); and a third party problem (42%)
- 46% take no precautions to protect their networks and systems.

Half the time, the data that was lost or stolen involved a health record.

These examples highlight the need for extreme caution when dealing with patients' personal information. But this does not yet appear to be a significant concern for health professionals. An October 2012 survey by Rogers Connect Market Research Group concluded that only 5% of physicians and 1% of pharmacists surveyed saw privacy/confidentiality/security issues as a barrier to communicating digitally, i.e. by email, messaging, etc. This is in spite of the fact that the penalties for breach of patient confidentiality can be harsh. For example, penalties under Ontario's Personal Health Information Protection Act, 2004 can be as high as $50,000 for an individual and $250,000 for organizations. Under the federal Personal Information Protection and Electronic Documents Act (S.C. 2000, c. 5) penalties can range up to $100,000.

The introduction of e-codes means that there is an incentive to use electronic communications as an integral component of patient care. However, the dangers are very real. For example, Privacy Commissioners have cautioned about the use of emails. The Alberta Privacy Commissioner points out that in a health care environment the risks are:

- Interception -- you send an email to an address used by a patient and her family. A family member receives and reads the email.
- Misdirection -- two of your patients have similar email addresses. You send an email containing sensitive health information to the wrong patient.
- Alteration -- you send test results to a patient with a chronic condition via email. The patient alters the results and provides

them to another care provider as trusted health information
- Loss -- you save emails offsite with your "cloud" email service provider. The email provider goes out of business and you lose access to valuable health information or they refuse to provide you with your data when you want to change your service provider.
- Inference -- you send an appointment reminder to your patient. The name and nature of your practice reveal health information about your patient to family members with access to the patient's email account.

In addition, if you store patients' personal information unsecured on a mobile device such as a laptop, smartphone, tablet, or a USB drive, and the device is lost or stolen, you are risking a breach of confidentiality that could have serious repercussions for yourself and for the affected patients.

This is why the use of secure messaging systems is so important for physicians and other health care providers. It avoids these problems. On January 2nd, CBC's The National aired a feature on *Protecting your digital medical records*. Peter Mansbridge and health reporter Kim Brunhuber point out that

- there are some 17,000 health apps
- these apps are making paper medical records a thing of the past
- in the age of smart phones apps can help patients go digital
- they allow patients, for example, to get test results without a phone call or paper trail
- but there are hazards that need to be addressed if mobile devices are used to store personal health information, e.g. they could be stolen or hacked.

One of the two apps that the CBC selected to show in this segment was Mihealth, which offers the highest level of security available. How can you be assured? Mihealth was certified by Canada Health Infoway as a Consumer Health Application after an exhaustive review that included submission of a privacy impact assessment (PIA) and a threat/risk assessment (TRA). We use technology that meets the Federal Information Processing Standards (FIPS) 140-2 validation by the National Institute of Standards and Technology (NIST) for its mobile technology. We have recently had our PIA approved for Alberta physicians under that province's privacy legislation, and we meet the US Health Insurance Portability and Accountability Act (HIPAA) and UK privacy standards.

Also, on February 1st we were notified by Ontario's Information and Privacy Commissioner that Mihealth has been designated under the Privacy by Design (PbD) Ambassador program for following the Principles of *PbD*."

Mihealth takes the issue of personal health information security very seriously. Whether the information is being accessed through our secure servers, or is being sent between individuals, or is being downloaded by a client onto one of 280+ compatible smart phones, the information is secure. Mihealth uses encryption; password protection; two way authentication when transmitting data, i.e. recognition of the machine/device; synching between server and smart phone or other mobile device to keep the smart phone data up to date; and wiping and restoration (resyncing) of the data when unauthorized attempts have been made to log into a mobile device's Mihealth data.

Our experience to date shows that the use of Mihealth secure messaging by health care providers will improve their office's effectiveness and efficiency, can enhance revenue, leads to improved employee satisfaction, and improves patient satisfaction and loyalty. It also provides an audit trail that is stored securely for at least 20 years.

For more information about Mihealth, go to www.mihealth.com or contact us by email at info@mihealth.com. We are always pleased to arrange a demonstration for providers and their staff.