



# CHATROOM

## Electronic communication: secure systems are vital

**Without security, there is no infrastructure to grow upon.**

BY DR. ALAN BROOKSTONE

In the past, I have written about e-mail and electronic communication between providers, and also between providers and patients. For my own part, I have listed an e-mail address on my medical practice web site for the past four years, accompanied by a code of conduct describing the appropriate use of e-mail to communicate with a physician in my practice.

Despite initial concerns that I would be flooded with e-mail from patients who were unable to gain access to me regarding medical concerns, this has not been the case. Patients are generally respectful of the code of conduct and on average I receive one e-mail message per week.

These e-mails are sometimes clinical, but are more often administrative – for example, from a patient who is unable to reach the office by phone and would like to cancel or change an appointment time.

If I do receive medical related questions from patients, my policy is to copy the e-mail into the patient chart and either call the patient to discuss the condition or have my staff arrange an appointment for follow up, as this is regular unencrypted e-mail with all of its associated risks relating to privacy. We are, however, entering a new era of electronic communication in healthcare.

There is clearly a business driver for more efficient communication amongst all stakeholders in the system. Most components of the patient encounter have a communication element. Although it is necessary to have the correct technology and interoperability between

different systems, there is no infrastructure upon which to grow functionality and improve efficiencies without the ability to send secure messages.

In order to understand this in a practical sense, I believe it is useful to break communications into two broad categories:

- Those that are manually generated by patient or physician – for example, when a patient has a clinical question and needs to communicate with a provider, or;
- Those that take place automatically – such as the delivery of lab results or discharge summaries directly into the provider's EMR in-box, to be dealt with on a pre-determined workflow basis.

Both of these capabilities need to exist if the system as a whole is to function. One type of communication is delivered through a back door that is essentially invisible, and the other arrives through a highly visible front door and is linked to specific actions.

How does secure e-mail communication work and how should it be implemented to meet the needs of healthcare practitioners and their patients? Ease of use is

critical. That's where the well-known security architecture known as Public Key Infrastructure (PKI) architecture falls down.

PKI can deliver on the security challenge but it expects providers and patients to identify a public key in order to send or receive a secure communication. That's simply impractical in an environment in which a primary care physician has approximately 10 minutes for a patient encounter.

This is where an integrated portal becomes important. Companies such as Relay Health ([www.relayhealth.com](http://www.relayhealth.com)) and Zix Mail ([www.zixcorp.com](http://www.zixcorp.com)) have developed secure communication systems that provide much greater functionality than currently exists in the 'unprotected' world.

In addition to pure communication, they are beginning to facilitate payment of fee-for-service interactions (in the case of Relay Health) and electronic prescribing. A secure communication environment is one of the cornerstones of the e-physician project in Ontario. It is now known as Ontario MD and is working to provide secure messaging via its portal.

Without a secure communications network connecting all providers to one another, it is not possible to envision how the multitude of exchanges currently created would flow in an electronic environment.

Physical connectivity is just one of the core components. Making the system usable by providers in the course of regular workflow is an equally significant challenge.

Portals require a great deal of infrastructure and support and are costly investments. Understanding physician needs, business and clinical drivers are absolutely critical components in the vision and development of clinical portals.

**Alan Brookstone, MD, is a family practitioner based in Richmond, B.C. He is also a consultant and conference speaker on the topic of computerized solutions for physician practices. He can be reached at [alan-brookstone@shaw.ca](mailto:alan-brookstone@shaw.ca)**

