Secure eMail for Clinical Communications

I've been using Google email (Gmail) for years without concern. Why am I now expected to use AHS email for clinical communication?

The need to use secure messaging (encrypted email) for communications containing identifiable patient information is not new. Regulatory (CPSA), legislative (Health Information Act), professional (AMA), liability (CMPA) and policy (AHS) direction has been clear for decades. The AHS Transmission of Information by Facsimile or Electronic Mail Policy dates back to AHS's formation. There have been many communications since about our responsibility to appropriately protect patient information, including:

- Transmission of Information by Facsimile or Electronic Mail Policy
- Emailing Personal Identifiable Health Information Procedure
- Emailing Personal Identifiable Health Information – User Guide to Email Encryption
- Mobile Wireless Devices and Services
- Guide: Clinical Email

Managing information in the electronic world can be confusing and complex. We all use email in our daily lives. However, when it comes to patient information, it is imperative that we adopt safe and secure practices. Nothing has changed but everyone needs to become more mindful about responsible behaviours in and around electronic devices and systems.

Why should I care about AHS email policies? I am an independent physician, looking to many organizations for health information management.

AHS policies apply whenever and wherever AHS holds responsibility for the record of care. This resonates with legislative, regulatory, professional and risk-management guidelines. It can be hard to know when a communication relates to the AHS context, or to some other organization. However, the risk of a breach, with very serious consequences, is everywhere, always. AHS and physicians share a common threat and interest. Moreover, the CPSA emphasizes physicians' responsibility to be aware of and heed organizational privacy protections.

AHS bears additional responsibility for information sharing in AHS facilities, health records and information systems. The organization needs to take reasonable steps to ensure that patient information is protected. To require use of secure email is reasonable, protective and helpful for AHS, physicians, patients and the health care team.

Policies are only as good as the people who follow them. It is critical that physicians understand the intent and practice of secure email communication.

What exactly is AHS secure email to be used for?

AHS email services enable secure communications. All email content is stored on protected servers in Alberta locations and all transmissions between AHS email accounts are encrypted. In addition, AHS email allows communications to non-AHS mail services to be encrypted, as long as "!Private" (exclamation mark immediately before capitalized word, Private, all-one-word) is added to the email subject line.

Popular public email services, including (but not limited to) all iCloud, Gmail, Hotmail, and Yahoo accounts, and any email accounts provider by internet providers such as Shaw or Telus and others, do not meet security standards and risk information exposure on unsecure and foreign servers. These services must not be used for clinical communications, either by physicians, their support staff or any AHS staff.

There are external secured clinical email and messaging services, including Alberta's Dr2Dr service. If in doubt, check with the AHS InfoCare team. In any case, AHS requires use of AHS email for clinical communications wherever and whenever AHS health records are used.

What makes AHS email any safer than any other email?

AHS email is held inside AHS's overall secured environment and is backed by comprehensive services that ensure the security of the entire network. It is encrypted in ways that prevent eavesdropping between sending and receiving. Known threats are screened and steady surveillance detects emerging threats.

No system is completely safe. Even the most robust security is defeated if a physician's username and password are (unwittingly) obtained by a hacker. Physicians must adopt an attitude of universal mistrust when it comes to information sharing. Yes, we must use appropriately secured systems. We must also protect logon credentials, take care when addressing emails, avoid email links and attachments, and be wary of possible emerging threats. AHS email helps by alerting us to communications coming from untrusted sources.

Again, why should I care? What happens if an inappropriate email service is used?

First you should care because no caring physician would put patients' information at risk. Second, any breach related to your choices also tarnishes our community, and Albertan's trust in physicians. We all share accountability for health information protection; as a matter of professionalism, social responsibility and good clinicianship.

Today's thieves are less interested in your possessions than your information. Cyber-attacks, phishing, viruses and worms target new vulnerabilities. We are under constant and growing threat. The consequences of information theft go way beyond inconvenience. Hackers harass, extort and damage relationships and reputations. Organizational penalties include fines, loss of privileges, disciplinary action and even license suspension.

How do I get an AHS email account?

During the AHS Medical Staff privileging approval process, all privileged physicians are provided with an AHS email address. This is usually firstname.surname@ahs.ca.

Visit the AHS Medical Staff website for instructions on how to access your login credentials.

Please consult with AHS Medical Affairs in your primary zone if you have questions or have never activated this AHS-issued account.