medinet

Bringing you secure eHealth Solutions

November 2014

Email – is it secure? What are the risks?

Cybercrime

The 2013 Norton report issued by security expert Symantec showed that the cost of cybercrime in Canada doubled in just one year to $3 billion, and that 7 million Canadians have been victims. **That's about 20 percent of the population!** Norton defines cybercrime pretty broadly, and includes everything from attempted scams to identity theft. But if the crime were robbery, and one in five of us were robbed or had been attacked, something would be done.

The culture

The Atlantic magazine, recently surveyed 50 Silicon Valley industry leaders and in answer to the question "Which technology or tech company poses the greatest risk to our personal privacy?" The lead answer was **"It's not the tech companies—it's the unconcerned citizens and our complacent culture."** Second, third and fourth were Google, Facebook and the US Government.

November 2014 issue

New research

The New York Times on November 12, 2014 reported that a Pew Research Center study released the same day indicates a majority of adults feel that their privacy is being challenged along such core dimensions as the **security of their personal information** and their ability to retain confidentiality. Yet, even as Americans express concern about government access to their data, they feel as though government could do more to regulate what advertisers do with their personal information: 80% of adults "agree" or "strongly agree" that Americans should be concerned about the government's monitoring of phone calls and internet communications.

Across the board, there is a **universal lack of confidence** among adults in the security of everyday communications channels—particularly when it comes to the use of online tools. Across six different methods of mediated communication, there is not one mode through which a majority of the American public feels "very secure" when sharing private information with another trusted person or organization:

- 68% feel insecure using chat or instant messages to share private information
- 58% feel insecure sending private info via text messages
- **57% feel insecure sending private information via email**
- 46% feel "not very" or "not at all secure" calling on their cell phone when they want to share private information

When it comes to their own role in managing the personal information they feel is sensitive, most adults express a desire to take additional steps to protect their data online: When asked if they feel as though their own efforts to protect the privacy of their personal information online are sufficient, **61% say they feel they "would like to do more,"** while 37% say they "already do enough."

Social Security Numbers, health info and phone conversations are among the most sensitive data:

- 95% say their Social Insurance Number is very or somewhat sensitive
- 81% are concerned about privacy around the state of their health and medications
- **77% worry that their email messages are not private**
- 75% say their text messages are very or somewhat sensitive

www.pewinternet.org/2014/11/12/public-privacy-perceptions

How to Reduce the Risks

Email sent to another physician or hospital about urgent or significant patient issues should not be considered a substitute for effective and efficient communication as there is no assurance the recipient will access the account regularly.

The BC Physician Privacy toolkit contains recommendations for the use of email in the medical practice:

1. Before emailing personal information, take the following precautionary steps:
2. Confirm that you have the correct email address for the intended recipient. Verify email addresses regularly as they are not always intuitive, can be duplicated, and frequently change.
3. Where feasible, the recipient of the email should be contacted and informed that confidential information is being sent. Have the recipient call back to confirm receipt.
4. When emailing sensitive personal information **consider using unique identifiers** or codes to protect the identity of the individuals involved. Unsecured email messages **can be read during transmission.**
5. Ensure that **confidential and sensitive personal information sent by email is encrypted** with access provided only to authorized individuals who have the access code.
6. Add **a confidentiality disclaimer** to email messages that states that the content is confidential and only intended for the stated recipient. It should also state that anyone receiving the email in error must notify the sender, and return or destroy the email as per the request of the sender.
7. **Protect any attached documents with a strong password** and notify the recipient by phone of the password.
8. As sender, be aware of the **security of the receiving email account** and who has access to it.

". . . all emails and attachments should have adequate encryption."

9. Ensure that each email inbox used to send or receive messages has a secure password known only by the individual authorized to access that inbox.
10. Never use email distribution lists to send personal information.

Informed Consent

Patients at University of Washington, USA health services are bound by federal regulations which impose **a "duty to warn" patients of risks associated with unencrypted email.** UW Medicine must document in the medical record that patients have been advised that email communications could potentially be read by a third party. Upon receipt and documentation of this notification, the patient has the right to request communication via email.

Risk of using email include, but are not limited, to:

- Email may be forwarded, printed, and stored in numerous paper and electronic forms.
- Email may be sent to the wrong address by either party.

- Email may be **easier to forge** than handwritten or signed papers.
- Copies of email may exist even after the sender or the receiver has deleted his or her copy.
- Email service providers have a **right to archive and inspect** emails.
- Email may be **intercepted, altered**, or used without detection or authorization.
- Email may spread computer viruses.
- Email delivery is not guaranteed.

www.uwmedicine.org/about/compliance/email-risk

Privacy considerations

The Canadian Nurses Protective Society has this to say:

"Privacy and confidentiality are also important considerations if e-mail is being considered as a method of transferring patient health records or health information. Because the security and confidentiality of e-mail systems are not guaranteed, it is not the recommended method for transmission of health information. If this method of transmission is used, legal writers recommend that any **e-mail messages containing confidential health information be encrypted.**"

58% [of physicians] use email to contact professional colleagues."

"Additionally, the patient should be informed of the risks of disclosure and presented with alternative methods of communication; if the patient agrees to the transmission of the health information by e-mail, **it is prudent to obtain written consent from the patient for the transmission.** This requirement for informed consent also appears in some provincial health care legislation. In Alberta, for example, the new Health Information Act (Bill 40) requires that a custodian who "intends to disclose individually identifying diagnostic, treatment and care information about an individual by electronic means must obtain the individual's consent to the disclosure or ensure that the individual's consent has been previously obtained."

www.cnps.ca ->Publications->Articles->The Legal Risks of Email

Concerns around Email for Physicians

From the Canadian Medical Protective Association: "While email technology is almost two decades old, the medical community has been cautious in adopting it to interact with patients."

"According to the 2010 National Physicians Survey, only 16% of physicians use email with patients for clinical purposes. Meanwhile, 58% use email to contact professional colleagues."

"There are several potential risk areas in email communication including privacy and security, timeliness of responses, and clarity of communication. Before engaging in email communication, members should review any applicable statutory or regulatory authority (College) requirements that may impact the use of email for transmitting patient health information. Consent by the patient to this form of communications is also important. **As well, all emails and attachments should have adequate encryption.**"

Canadian Medical Protective Association: www.cmpa-acpm.ca -> Advice & publications -> Browse articles -> Safety of care -> Technology unleashed - The evolution of online communication

Legal concerns

The American Bar Association Standing Committee on Ethics and Professional Responsibility issued Formal Opinion 11-459 in August 2011, which discussed a lawyer's duty to protect the confidentiality of electronic communications with clients. The opinion is one which should be familiar to most lawyers, but unfortunately, based on my experience, it is not.

Briefly, the opinion warns that all lawyers should be having a frank discussion with their clients about the confidentiality of email and the attorney-client privilege. Risks arise

where clients are using an email address or a device owned and/or controlled by their employer, in which their employer might have access to their email and an ability to read their email messages (including messages from a 'personal' email account used on a business device). Many employers have a policy with regard to email and/or device use which allows the employer access. In these circumstances, there is significant risk of a breach of confidentiality or an erosion of the attorney-client privilege.

Similarly, where a client uses a home computer than can be accessed by third parties (such as a spouse, children or other family members), or a 'public' computer than can be accessed by others, the lawyer has a duty to warn the client of the potential risks and instruct the client accordingly. Additional concerns may arise when using public or unsecured wi-fi. **Lawyers should also consider the use of encryption**, or in some cases to cease sending email messages to clients completely if clients do not heed the lawyer's warnings.

Google uses electronic scanning of messages sent to its Gmail service to both filter spam and to send targeted advertising messages

Last week, news of a brief filed in June on behalf of Google supporting a motion to dismiss a class action lawsuit claiming that **Google's data-mining of email messages** through Google mail was a violation of privacy hit the airwaves. The Google brief cites a Supreme Court decision from 1979 (long before email became the communication medium of choice among lawyers) that users of web-based email should understand that the messages are being processed by the email provider, and therefore, that there is no expectation of privacy, since the messages were essentially being 'turned over to third parties.' Google uses **electronic scanning of messages sent to its Gmail service** to both filter spam and to send targeted advertising messages, but claims no human is reading those messages. Clearly, Google is not the only mail service to scan email messages to identify and filter spam messages, but what level of scanning and filtering is acceptable?

There has been much discussion over the past week about privacy concerns with email scanning, but what about client confidentiality and attorney-client privilege? **Does electronic scanning of messages breach confidentiality?** Should lawyers discontinue their own use of Google's mail service (or any other mail service that scans messages) and/or advise their clients to do so?

While regular users of email services can certainly consent to allow Google (or any other email provider) to scan their messages, is this an acceptable practice for attorney-client communications, where lawyers have an obligation to ensure that these communications remain confidential?

http://legalease.blogs.com/legal_ease_blog/2013/08/email-confidentiality-and-attorney-client-privilege.html