Canadian Nurses Protective Society

infoLAW®

Legal Risks of Email - Part 1
Privacy Concerns

Vol. 22, No. 2,
November 2014

Privacy Concerns

Health care organizations and health care professionals use email extensively because of its speed, reliability and convenience. However, the same characteristics that make email use advantageous are also the source of legal risks, including potential privacy breaches. Being aware of the risks inherent in the use of email can help nurses manage those risks and decrease their potential liability.

Network Security and Safeguards

Personal health information (PHI) contained in email communications is governed by the same health information management legislation as PHI contained in health records. As a result, confidentiality and privacy are important considerations if email is being used to communicate PHI to recipients who are not part of a secure internal network. Internet-based email systems generally do not provide a level of security appropriate for transmitting sensitive information. Even within a secure internal network, depending on the system in use, special software overlays may be necessary to protect the server and all endpoint devices connected to the network (e.g. desktop computers, laptops, smartphones, etc.). Nurses would be prudent to seek confirmation from their employer, or, when acting as custodians of PHI, from a qualified IT professional, that the necessary safeguards are in place before transmitting PHI via email.

In addition, privacy commissioners have published guidelines and rendered decisions regarding the use of email for transmitting PHI to email addresses that are not part of a secure network. In circumstances where email is determined to be the preferred method of transmission, privacy commissioners strongly recommend that proper safeguards, such as strong encryption, be used to prevent interception by unauthorized parties.[1]

Additional Privacy Considerations

Additional factors to consider before sending PHI by email include: whether the recipient is authorized to receive the information; whether the email address provided is accurate; whether it was accurately transcribed or selected from a menu; and whether the intended recipient is the only one with access to the email address. Further, nurses may consider whether the recipient has or would be required by law to have in place the necessary safeguards to protect the information from improper access, use and disclosure.

Nurses who consider communicating PHI by email beyond a secure internal network may wish to inform patients of the risks inherent in email use and discuss the potential benefits and drawbacks over alternative methods of communication. It would be prudent to obtain the patient's written consent before transmitting PHI or, alternatively, document the patient's verbal consent. The responsibility for ensuring reasonable safeguards are in place does not shift to the patient, nor is it diminished, even when the patient has provided an informed consent to communicate by email.[2] The Information and Privacy Commissioner of Ontario has advised that even where patients are willing to accept the risk of unauthorized access or disclosure of their PHI in exchange for the

Health care providers have a duty to take reasonable steps to safeguard PHI in their custody and control.

convenience of communication via email, health care providers still have a duty to take steps that are reasonable in the circumstances to safeguard personal health information in their custody and control.[3]

Given the inherent risks of email communication, where time permits, nurses may consider whether more traditional and safer methods of information exchange (e.g. registered mail) are more appropriate.

Statutory and Regulatory Considerations

Nurses should consider any statutory (e.g. privacy legislation) or regulatory body requirements in their jurisdiction that may govern the use of email for clinical purposes. For example, the Alberta *Health Information Act* requires health care organizations considering changes to the manner by which they collect, use or disclose PHI (e.g. transmitting PHI by email) to submit their proposals, along with privacy impact assessments, to the Privacy Commissioner for approval.[4]

Employer Policies

The foregoing discussion applies to all nurses; however, nurses who are employees should also consider that employers may have implemented workplace policies on the use of email for clinical purposes. The employer is typically the custodian of the PHI and generally mandated by law to determine compliance with the PHI legislation. Where there are no or insufficient policies on this issue, it would be prudent to seek further guidance from the employer or the appropriate designate prior to communicating PHI by email.

Risk Management Considerations

To limit the potential legal risks related to email communications, consider implementing the following risk management strategies:

- Confirm the correct email address for the intended recipient before transmitting PHI;
- Use encryption when sending to an external email recipient;
- Obtain signed consent forms from patients who wish to communicate by email indicating that they have reviewed and accepted the risks associated with communicating PHI via email;
- If no consent form is used, document the patient's express consent to email communication in the patient's record;
- If responsible for IT services, obtain written assurances from reputable IT professionals as to the security of any email system that may be used to transmit PHI; and
- If responsible for entering into IT contracts, ensure the agreement meets any regulatory requirements and that it clearly states that the system will be used to transmit PHI and that certain security assurances were provided.

---

1. Ann Cavoukian and Peter G. Rossos, "Personal Health Information: A Practical Tool for Physicians Transitioning from Paper-Based Records to Electronic Health Records," Information and Privacy Commissioner of Ontario, May 21, 2009. Ann Cavoukian and Ross Fraser, "Fact Sheet: Health-Care Requirement for Strong Encryption," Information and Privacy Commissioner of Ontario, July 2010; Canadian Nurses Protective Society, "Mobile Devices in the Workplace," *infoLAW* 21(1), November 2013.
2. Office of the Information and Privacy Commissioner of Alberta, "Email Communication FAQs," Edmonton, AB: Office of the Information and Privacy Commissioner of Alberta, August 2012.
3. Cavoukian and Rossos, *op. cit.*
4. *Health Information Act*, RSA 2000, c H-5, s 64.

Related infoLAWs of interest: Mobile Devices in the Workplace and the Legal Risks of Email – Part 2. Available at **www.cnps.ca**