Canadian Nurses Protective Society

infoLAW®

Privacy and Electronic Medical Records

Vol. 18, No. 1, December 2009

To protect the privacy of patients' personal information and decrease their legal risks, nurses should be aware of the unique privacy issues related to the use of electronic medical records (EMRs).

Privacy Risks

Access

Many EMR privacy breach cases involve inappropriate access. For example, a clerk in a plastic surgeon's office repeatedly accessed the health information of her lover's cancer-stricken wife through the provincial electronic health records system. The wife was not one of the plastic surgeon's patients. The clerk was charged with illegally accessing the wife's laboratory results, biopsy results and CT scans 17 times on six different days while she was working in the physician's office. The clerk pleaded guilty to the charge and was fined $10,000 for violation of the provisions in Alberta's *Health Information Act*.[1]

Accuracy

The inclusion of more than one patient's health information in an EMR can result in inappropriate disclosure of personal information. This happened when a patient requested a copy of his own medical record from a records management company and received a data CD containing his personal health information and the personal health information of two other patients. The investigation by the Alberta Information and Privacy Commissioner's Office revealed that, prior to closing his practice, the patient's physician sent two CDs to a company for conversion of the data into Portable Document Format (PDF). One of the CDs contained patients' charts and a backup copy of any files that had ever been misfiled or deleted from a chart. After the conversion, the company sent two DVDs to the records management company who used the DVDs to respond to patient requests.[2]

Theft

Theft or loss of computers and portable devices such as laptop computers, flash drives, and smartphones can result in the inappropriate disclosure of personal information. Recently, a physician left the hospital with a laptop computer loaded with the unencrypted personal health information of approximately 2,900 identifiable patients involved in research studies. The physician parked his minivan in a parking lot and placed the laptop computer under a blanket between the front seats. When he returned to the van the front passenger window was broken and the laptop computer was missing.[3]

Disposal

A lack of secure procedures for the disposal of records containing personal information can result in a privacy breach. The Ontario Information and Privacy Commissioner's first order under the *Personal Health Information Protection Act, 2004*[4] highlights the need for secure destruction practices for records in paper and electronic formats. In that case, records from a radiology clinic were strewn across a downtown Toronto street during a film shoot. The radiology clinic had provided

"For those who would consider violating the privacy of patients, I want them to think twice and ask themselves if it is worth it."

– Brian Beamish, Acting Information and Privacy Commissioner of Ontario

More than liability protection

patient records for shredding to a disposal company. Boxes that were marked recycling, not shredding, were sent to a recycling company and the recycling company sold the scrap paper to a film company for use as props on a film set. Some of the scrap paper contained patients' personal health information.[5]

Risk Management

Risk management strategies can decrease the likelihood of a privacy breach. Strategies should include:

- organizations having and enforcing policies and procedures related to the collection, use, access, disclosure, security and disposal of personal health information
- ongoing education for all employees, contracted staff, volunteers and students about privacy issues, the role of the organization's Privacy Officer, and the applicable privacy legislation
- having all employees, contracted staff, volunteers, students and agents (who have access to personal information) sign a confidentiality agreement
- having strong password protection on all computers
- limiting access to personal health information on a need to know basis for patient care or for purposes authorized in privacy legislation
- monitoring of use, access and disclosure of personal health information on an ongoing basis
- implementing a multi-layered approach including the use of strong passwords and encryption if personal health information is stored on mobile devices[6]
- custodians or trustees ensuring no other patient's personal health information is included in the EMR before use or disclosure[7]
- having permanent destruction or erasure of personal information in an irreversible manner as the goal of secure records destruction[8]

Resources

The following resources are available to assist you if you have questions relating to privacy issues: your organization's Chief Privacy Officer, federal/provincial/territorial Information and Privacy Commissioners' Offices, the Manitoba Ombudsman's Office, your professional nursing association or college, and the Canadian Nurses Protective Society.

1. *Health Information Act*, R.S.A. 2000, c. H-5; Alberta Court of Queen's Bench Docket number 061362778P1, 13 April 2007 (oral judgment).
2. Investigation Report H2008-IR-002, Office of the Information and Privacy Commissioner of Alberta, online: www.oipc.ab.ca.
3. Order HO-004, Office of the Information and Privacy Commissioner of Ontario, online: www.ipc.on.ca.
4. *Personal Health Information Protection Act*, *2004*, S.O. 2004, c. 3, Sch. A.
5. Order HO-001, Office of the Information and Privacy Commissioner of Ontario, online: www.ipc.on.ca.
6. Order HO-004, Office of the Information and Privacy Commissioner of Ontario; *Fact Sheet: Encrypting Personal Health Information on Mobile Devices*, 2007; *Safeguarding Privacy in a Mobile Workplace*, 2007; *BlackBerry® Cleaning: Tips on How to Wipe Your Device Clean of Personal Data*, 2008; online: www.ipc.on.ca.
7. Supra note 2.
8. Supra note 5; Fact Sheet: Secure Destruction of Personal Information, 2005, Office of the Information and Privacy Commissioner of Ontario; online: www.ipc.on.ca.

N.B. In this document, the feminine pronoun includes the masculine and vice versa except where referring to a participant in a legal proceeding.

THIS PUBLICATION IS FOR INFORMATION PURPOSES ONLY. NOTHING IN THIS PUBLICATION SHOULD BE CONSTRUED AS LEGAL ADVICE FROM ANY LAWYER, CONTRIBUTOR OR THE CNPS. READERS SHOULD CONSULT LEGAL COUNSEL FOR SPECIFIC ADVICE.