Legal Issues

By Janet K. Feldkamp, JD, RN, LNHA

The Importance of Taking Privacy Seriously

Confidentiality has a leading role in today's health care environment. Now more than ever, providers of all types must carefully follow federal privacy requirements because the Office of Civil Rights within the Department of Health and Human Services is taking an aggressive stance against any breach of protected health information.

The office recently issued press releases regarding several significant monetary settlements with health care providers who had failed to protect clients' health care information as required by the Health Care Health Insurance Portability and Accountability Act (HIPAA).

The federal law mandates definitive action by health care providers, including nursing homes, to prevent the information from being released without the client's specific permission. If such information is lost or stolen, the provider must promptly report the breach to the Office of Civil Rights.

The office takes its duties seriously. In 2012, it reported the resolution of 8,370 breaches. Of that number, 3,898 were investigated and found "significant."

Typical cases involve thousands of patient records that had been compromised. But recently, the Office of Civil Rights issued a press release touting its first settlement of a HIPAA breach involving fewer than 500 patients.

On Jan. 2, the office announced that the Hospice of North Idaho entered into an agreement to pay $50,000 to settle violations involving the breach of unprotected and unencrypted electronic health information on 441 patients when a laptop computer was stolen. In the press release, office Director Leon Rodriguez indicated that the action was intended to send a strong message to the health care industry that the government will take HIPAA action against careless providers, regardless of their size.

Earlier in 2012, the office announced two other significant settlements of $1.5 million and $1.7 million with the Massachusetts Eye and Ear Infirmary and the Alaska Department of Health and Human Services, respectively. Each of these cases also stemmed from the loss of an electronic device containing unencrypted health information.

The office's listing of breaches is enlightening. Breached material has resided on network servers, paper, laptops, desktop computers, and in e-mails, paper mailings, and portable devices. Losses of the information have been via improper mailings and thefts.

In other words, a breach of information can take many forms and occur in a variety of ways, stressing the importance of comprehensive policies and procedures to protect confidentiality.

Policies should prohibit employees from phone texting information, as well as posting patient information on social media sites. Protected information, including pictures of patients, appearing on an employee's social media pages violates HIPAA.

The Office of Civil Rights website, www.hhs.gov/ocr/privacy, provides much useful information for the health care provider, both large and small. It discusses HIPAA requirements, enforcement actions, directions for filing a complaint, a news archive, and very useful answers to frequently asked questions.

The "FAQs" tab allows searching by category to provide specifics, such as how "minimum necessary" is defined as the acceptable level of health care employee access to patient information.

Even though not all enforcement actions and settlements are necessarily reported by the Office of Civil Rights on its website and almost all postings concern large settlements, what's there can help smaller providers avoid violations. Some examples:

- A breach was reported when an employee left a message containing patient information on a home answering machine rather than contacting the patient at a work number, as designated.
- A hospital operating room employee e-mailed information about upcoming surgery to a work e-mail that the patient's supervisor had access to.
- An insurer sent explanations of benefits to a family member's address rather than that provided by the patient.
- Several unencrypted computer hard drives containing protected information were stolen from the off-site storage facility of a health care provider.
- A flaw in a health plan's computer system put the information of several thousand families at risk of disclosure.

The $1.5 million settlement agreement mentioned above details other breach issues and reveals where information-handling weaknesses at the Massachusetts Eye and Ear Infirmary allowed protected information to be released in violation of patients' rights:

- The facility failed to conduct a thorough analysis of the ongoing risk to confidentiality of electronic information.
- Security measures were not sufficient.
- The organization did not adequately develop, adopt, or implement policies and procedures to identify, respond to, and report breaches.

Even state agencies, such the Alaska Department of Health and Human Services, can have breaches and be the object of HIPAA enforcement. Last June, the state acceded to its $1.7 million settlement because an unencrypted hard drive had been stolen from an agency employee. Again, the federal Office of Civil Rights reinforced the importance of organizations reviewing their policies and procedures to ensure the security of both paper and electronic information.

HIPAA concepts and the office's requirements are no longer new, and the expectation is that health care providers, large and small, are knowledgeable of the requirements and will comply. The federal government will continue and probably step up its enforcement of patient privacy by investigating information breaches that are filed by patients and, as required by law, by health care providers themselves.

The proactive nursing home leader should review current HIPAA and state requirements for patient-privacy protection. If your facility has not undertaken encryption of its electronic devices, such as laptops and desktop computer hard drives, it should seriously consider doing so now. Risk assessment, policy implementation, and ongoing education will be important to continuing compliance and minimizing sanctions should a breach of protected information occur.

This column is not to be substituted for legal advice. The writer, Janet K. Feldkamp, practices in various aspects of health care, including long-term care survey and certification, certificate of need, health care acquisitions, physician and nurse practice, managed care and nursing related issues, and fraud and abuse. She is affiliated with Benesch Friedlander Coplan & Aronoff LLP of Columbus, Ohio.