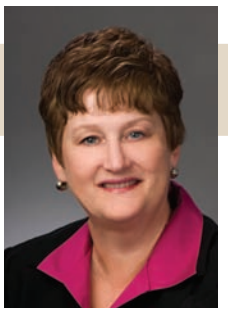
Legal issues



By Janet K. Feldkamp, JD, RN, LNHA

A Matter of Trust: The Cost of HIPAA Non-Compliance

Health care providers protect patient information through daily actions, but failures resulting in breaches of compliance with the Health Insurance Portability and Accountability Act (HIPAA) are increasingly costly. Initially passed into law in 2003, HIPAA has been updated several times with a number of amendments and updates. Most recently, 2013 modifications added requirements for HIPAA-covered entities and business associates that required both types of entities to directly comply with the updated privacy and security standards.

Health care providers, including physicians and acute and PA care providers, have long understood the importance of protecting patient information. However, since the enactment of the HIPAA standards, health care providers have been required to implement detailed HIPAA compliance plans that include, among other things, employee training, authorization for release of health care information, and assessment of the inherent risks related to privacy and security of patients' protected health information. When a loss of protected health information occurs, the Office for Civil Rights (OCR) reviews the provider's investigation materials and may take enforcement action that can include issuance of sanctions. OCR's website provides useful information for the health care provider, both large and small, as well as for business associates that also must comply with all HIPAA requirements by virtue of handling protected health information generated by the health care provider. OCR's website provides a wealth of information on HIPAA requirements, enforcement actions, settlements, news archives, and useful answers to frequently asked questions. (www.hhs.gov/ocr/privacy).

Information Breach

Protected health information (PHI) broadly includes health information that relates to past, present, or future health care or payment information for individual patients; this PHI is maintained or transmitted in any form or medium by a covered entity. The covered entity definition includes any provider that electronically transmits health information in transactions covered by HIPAA, including submission of claims or benefit eligibility inquiries. When an individual's PHI is compromised, a potential breach of HIPAA requirements occurs, and the individual may be notified of the breach. If more than 500 individuals' PHI is breached through release or unauthorized access, the covered entity must immediately notify OCR and notify a media outlet to inform the public that a significant breach of individuals' health care information has occurred. The covered entity also must notify each individual within 60 calendar days of the breach.

Upon notification of a breach, OCR conducts an investigation of the covered entity's actions and may levy fines, request more information for review and analysis, and require additional action to be undertaken by the covered entity. Fines for breaches and noncompliance with HIPAA requirements range from $100 per violation to $1,500,000, depending upon the severity of the violation. Also, criminal penalties can be levied upon individuals who knowingly obtain or disclose PHI.

Understanding the most likely situations to occur with a breach of protected health information can help providers focus on areas that may need ongoing review and monitoring. OCR lists the five most investigated issues regarding HIPAA:

1. Impermissible uses and disclosures of PHI
2. Lack of safeguards of PHI
3. Lack of individuals' access to their own PHI
4. Lack of administrative safeguards of electronic PHI
5. Use or disclosure of more than minimum necessary PHI

Cost of Carelessness

Two recent enforcement settlement actions highlight current OCR expectations regarding breaches. Cancer Care Group PC, a 13-physician group, agreed to pay $750,000 and implement a corrective action plan following the theft of an unencrypted laptop from an employee's car. The laptop included names, addresses, birth dates, Social Security numbers, and other insurance and clinical information for approximately 55,000 former and current patients of the physician group. OCR investigation revealed noncompliance with the HIPAA security rule requiring safeguards on electronic PHI, such as encryption of electronic devices. Encryption renders the information inaccessible without proper access codes even if the hard drives are removed from the electronic device. OCR also noted that the physician group had failed to conduct a comprehensive risk assessment and lacked written policies on the receipt and removal of hardware and electronic media containing electronic PHI. OCR maintained the group's inactions contributed to the breach, and had the physician group proactively implemented the required protections, the breach could have been totally prevented.

In another recent settlement, St. Elizabeth's Medical Center, Boston, resolved its breach situation with OCR regarding workforce members using Internet-based document sharing to store 498 patients' Information. The settlement amount of $218,400 is listed on OCR's website as are most of its actions and settlements. A complaint filed with OCR alleged that the hospital failed to investigate and identify a known security incident, and to reduce the potential effects of the incident through prompt action. OCR determined that the security incident and outcome were not documented as required by the hospital's HIPAA program and HIPAA requirements. In a separate breach report, St. Elizabeth's reported that a former workforce member's personal laptop and flash drive were lost or stolen. This breach affected 595 patients. The St. Elizabeth's settlement also included a number of corrective actions to enhance the hospital's HIPAA program.

Fines for breaches and noncompliance with HIPAA requirements may range from $100 per violation to more than $1 million.

Health care providers should be vigilant in protecting patient information. Some key considerations include:

- Business associates (individuals or companies under contract with the health care provider that utilize PHI) also are required to follow all HIPAA requirements. Monitoring the business associates' compliance can help ensure that the provider's patients' PHI is protected. In 2011 and 2012, according to the OCR, about 25% of all breaches—including 50% of all affected individuals—were related to business associates.
- Thefts continue to be a leading cause of breaches. Providers should strengthen security and train employees to be careful and watchful regarding medical equipment and access to information.
- Laptop theft or loss is a frequent type of breach report. With laptop encryption, a breach will be avoided as the data is inaccessible without the appropriate codes required to access the information. OCR makes it clear that providers are expected to encrypt electronic media devices, such as laptops and flash drives. These portable media devices are easily lost and/or stolen, and without encryption the information is readily accessed in violation of the law.
- Hacking of health care organizations' websites and other electronic access portals continues to increase. A security review of the health care provider's electronic systems can be a proactive step to avoid successful hacking.

These recent settlements and other enforcement actions remind covered entities and business associates that proactive compliance with security and privacy requirements are a necessity of daily health care business. If actions are not taken to review the entity's risk analysis documentation and to ensure that preventive and reactive processes are in place, the provider has failed to address significant risks that could potentially cost the entity significant fines. If a breach occurs, this information may be publically posted on the OCR website. Review and update the required HIPAA policies and procedures, train your work force, monitor business associates, conduct regular compliance monitoring, and thoroughly investigate potential breaches. With these actions, the health care provider's risk of HIPAA noncompliance is reduced. Start the new year with a updated and strengthened HIPAA program.

This column is not to be substituted for legal advice. Ms. 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, OH. Read this and other columns at* www.caringfortheages.com *under "Columns."*