



Going HITECH? Be prepared for breaches

B. Janelle Jordan, CIC, CLCS | MSV Insurance Agency

The use of electronic health records (EHR) to support the practice of medicine is increasing rapidly. This surge in interest may be due in-part to the efficiency gains seen by health care providers, but for many it is certainly due to the Health Information Technology for Economic and Clinical Health (HITECH) Act, which was signed into law as part of the American Recovery and Reinvestment Act on Feb. 17, 2009. The HITECH Act brings with it many changes aimed at reducing cost and improving the quality of health care through the use of certified EHR. However, for those who are embracing the use of EHRs, it is important to become familiar with the new liabilities created by the use of health information technology (health I.T.).

One of the fastest growing risks to businesses and consumers relates to privacy of electronic information. With the vast amount of personal information that providers hold, it is no surprise that the HITECH Act prescribes regulations to control protected health information (PHI) and give patients greater protection from the disclosure of PHI. A number of new guidelines on how disclosures are to be permitted, tracked, and recorded have been enacted. In particular, there is the requirement of providers to notify patients of breaches or possible breaches of patients' PHI.

Effective Sept. 23, 2009, the Interim Final Rule for Breach Notification for Unsecure Protected Health Information was issued pursuant to the HITECH act. While this rule was specifically created to bring transparency to breaches and to initiate a quick response to a possible breach, the notification requirements associate with this act can interrupt operations and bring significant financial loss. However, for those providers who are properly prepared for a breach response and the cost associated with it, the risk of disturbances in operations and revenue flow can be significantly reduced if not eliminated.

What is a PHI breach?

A breach is defined as the acquisition, access, use or disclosure of unsecured PHI which is not permitted by the Health Insurance Portability and Accountability Act (HIPAA) and compromises the security or privacy of the PHI. A breach to your patients' PHI can occur while in your care, custody or control, but now, according to the HITECH Act, a provider will be liable for a breach occurring to patients' PHI while in the care, custody and control of a business associate in certain circumstances. Breaches are not just caused by hackers. In fact, breaches occur more often from lost or stolen laptops, malicious insiders, and off-site data storage issues. In one reported case, boxes with patient records ended up in a trash dump and were accessed, in another an office burglary resulted in a breach.

Required responses to a breach

You must send written notification via first class mail to each person whose information was breached within 60 days of the discovery of the breach. In cases where the addresses are unknown for more than 10 individuals, the notice is to be posted on a Web site, in major print media or over broadcast media. If the breach affects 500 or more individuals, then the notice must also be sent via prominent media outlets that serve the state or jurisdiction and you must notify the U.S. Department of Health and Human Services (HHS). Compliance with the breach notification rules may also trigger mitigation of harm to the affected individuals which often requires credit monitoring services for each affected individual.

What are the real risks?

As of July 4, the Office for Civil Rights (OCR) updated its findings of the number of breaches effecting over 500 individuals and reported that since Sept. 22, 2009, 107 breaches of this type have affected over four million individuals. With the increase in the usage of EHRs, the number of breaches is expected to increase. Sanctions and financial penalties (ranging from \$100 to \$50,000 per violation) are at the discretion of HHS under the interim final rule, however it is expected that such fines will be put into force in the final rule. It doesn't stop there. Breaches may also bring on litigation costs due to HIPAA privacy and security standards, or the Federal Trade Commission's Disposal Rule.

How much could a breach cost?

There are a number of expenses that may be involved in order to remedy a breach, therefore projecting the costs are difficult. However, a 2008 – 2009 benchmarking study performed by the Ponemon Institute reported that the average notification costs for health care institutions are \$282 per patient. The Institute's notification cost estimates include communication expenses for notification, lost business, and credit monitoring. Other fees that may also apply that are not in this finding include costs for internal investigations, attorney's fees, crisis management services, regulatory investigations, and civil/regulatory fines. For example, the loss of a laptop holding 500 patient records could result in breach expenses totaling \$140,000; one with 1,500 records over \$400,000.

How can the Medical Society of Virginia Insurance Agency (MSVIA) help prepare providers?

As privacy security becomes a growing area of exposure, MSVIA has worked with liability insurance carriers to provide broader products and services for cyber risks. These coverages can be offered under a malpractice policy or may be purchased as a separate policy. Cyber liability policies can offer services such as crisis management, specialized legal defense, and computer forensics to mitigate losses. Cyber liability coverage may also provide financial protection expenses related to network security, notification expenses, credit monitoring, regulatory fines, data recovery, and public relations efforts. A breach can cause a storm of issues for your organization. If prepared, however, the impact to your patients, your employees and your community can be significantly minimized. More than simply providing insurance products, MSVIA aims to protect what is most valuable to you – your reputation.

MSV is now offering a webinar on this topic. Check the Practice Services course listing at www.msv.org/classes for more information.