Codify
BY AAPC

Health Information Compliance Alert

Privacy: Are Your Employees Tempted to Pinch Medical IDs? Know The Risks

Watch for insider breach and human error advise experts.

Providers of healthcare -- be they practices or facilities -- need to be aware of the threat of medical identity theft and take suitable steps to prevent its occurrence.

Generally medical ID theft occurs two ways. Either it occurs from the inside where employees are involved or it occurs at point of care where patients are posing as someone else for the purpose of gaining expensive treatments or drugs without having to pay for them, **Ester Horowitz, CMC, CITRMS, CIISA** tells **Eli**. The bad news is that often "the very people we trust the most are actually the ones committing the fraud and it could have been going on for years," she warns.

Illicit cash: When medical ID theft is an inside job, "it means that someone who works for a covered entity is taking the IDs and passing them or using them for money," says Horowitz. "The street value of an ID is about $100 per name which can be sold repeatedly." If a patient steals a health insurance card or ID, it is generally for the purpose of getting services and prescriptions. Scripts have a tremendous street value because hard drugs can be sold underground for a lot more than the cost of selling them via the pharmacy, she warns.

Medical IDs do not usually include health information -- only name, address, social security number, date of birth, and health insurance ID number. You don't need an address to commit ID theft, but you do need a date of birth with a name, Horowitz adds. "When you can take someone's identity without permission, it is a crime even if nothing is done to use it in any way," she clarifies.

"Hospitals, and physicians' offices, are particularly vulnerable to viruses or attacks that are designed to steal information," **Kenneth Rashbaum, Esq.** of Rashbaum Associates, New York, N.Y. points out. "Phishing" attacks, in which a user is asked to click on an attachment or link that then loads malware that sends identifying information back to the malware authors, is a common and insidious method of identity theft, he adds.

Use a 2-Part Strategy to Thwart Security Threats

Taking a two-pronged approach to stopping both inside jobs and external theft of your PHI is the best way forward, experts insist. The first approach is apply the technical securities that will help prevent a threat to your information systems, "and the other is to require good authentication of individuals when providing services or supplying information," **Jim Sheldon-Dean,** Director of Compliance Services, Lewis Creek Systems, LLC in Charlotte, Vt. advises health providers and facilities.

Medical practices can be prone to "phishing" attacks, in which a user is asked to click on an attachment or link that then loads malware that sends identifying information back to the malware authors, which is a common and insidious method of identity theft, **Kenneth Rashbaum, Esq.** of Rashbaum Associates, New York, N.Y. points out.

Know flash drive risks: A virus can be introduced though use of a USB that had previously been used in an infected home computer, Rashbaum points out. "Clearly written policies and procedures can help in this regard, such as those that direct users not to open attachments or click on links from unknown or untrustworthy sources, and proscribing the use of USBs into facility computers after they have been used at home, unless they are checked out before being plugged into the facility system," he suggests.

Implement authorization controls such as password protocols, and access controls that limit access to patient

information limited to those who have a business need for that information, Rashbaum further advises.