Codify
BY AAPC

Pain Management Coding Alert

Reader Question: Protect HIPAA From 'Social Engineering' Threat

Question: I recently heard about "social engineering" as a security threat related to the Health Insurance Portability and Accountability Act (HIPAA). What is it?

Delaware Subscriber

Answer: Social engineering is "an unauthorized attempt by someone masquerading as a legitimate party to elicit information from a staff member that may be used in attempts to compromise the security of systems or accounts," says **Jim Sheldon-Dean**, founder and director of compliance services for Lewis Creek Systems, LLC.

In other words: "Social engineering tactics are designed to obtain secure information (login, customer, patient, or corporate data) by conning a person into revealing the information," explains **Michael Whitcomb**, CEO of the IT security and regulatory compliance firm Loricca in Tampa, Fla. Social engineering exploits the overly trusting nature of most people.

Phishing is a type of social engineering, but phishing emails are becoming more and more sophisticated.

"Criminals have gotten smarter and their tactics have evolved," Whitcomb warns. "Train your employees to watch for emails that may contain tricks to access personal or professional information."

According to Sheldon-Dean, when you're investigating and evaluating security incidents, you should categorize them as one or more of the following:

- Denial of Service an event that prevents or impairs the authorized use of networks, systems, or applications;
- Malicious Code a virus, worm, Trojan horse, or other code-based malicious entity that infects a host;
- Unauthorized Access logical or physical access without permission to a network, system, application, data, or other resource;
- Inappropriate Usage a person violates acceptable computing policies; and/or
- Social Engineering.