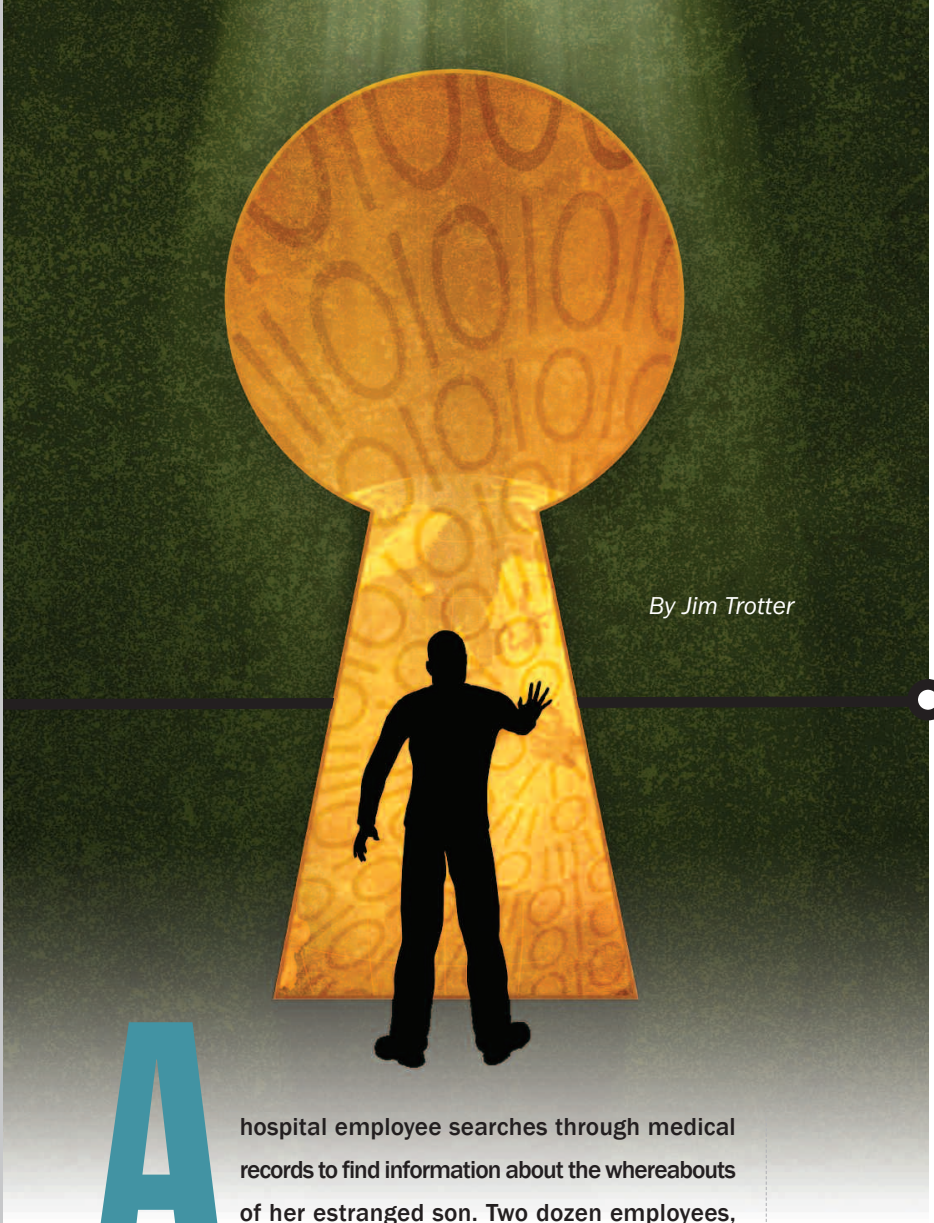

Safeguard Against Snooping

VIOLATIONS CAN RESULT IN HEFTY FINES OR WORSE

By Jim Trotter

A hospital employee searches through medical records to find information about the whereabouts of her estranged son. Two dozen employees, including doctors and nurses, are suspended for accessing George Clooney's medical records without authorization. And on April 30, 2010, a former researcher at UCLA is sentenced to four months in prison for accessing records of primarily well-recognized celebrities, the first person to be sentenced to prison for snooping through patients' medical records under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA").

"Snooping" is defined as "prying into the private affairs of others, especially by prowling about." Prior to the advent of HIPAA, snooping was probably more commonly known as a favorite activity of little sisters and big brothers. However, with the advent of the privacy regulations of HIPAA, there are specific safeguards that must be in place to protect access to private information by unauthorized individuals. There are no exceptions to the use and disclosure of protected health information for purposes other than treatment, payment and healthcare operations without express written authorization. Organizations and individuals who fail to implement the appropriate safeguards are beginning to now face very stiff penalties. Organizations are beginning to see that while they may have expended much effort to close gaping holes in protecting their patients' private information, many loopholes still exist.

How to Prevent "Snooping" in Your Organization

While no system or process is guaranteed to be 100% foolproof, there are steps organizations can take to mitigate the risk of a patient's private information being accessed and/or released without the proper authorization.

The HIPAA Privacy Rule provides federal protections for personal health information without interfering in the use of this information for patient care and other treatment purposes. Likewise, the standards for the security of electronic health information are designed to ensure confidentiality of electronic protected health information.

Perhaps one of the most important steps a covered entity can take in ensuring compliance with these laws and regulations is to educate its workforce. Employee training about why protecting private information is important and how it is done within an organization is critical. Important topics to include

are email encryption, changing passwords frequently, and reporting suspected privacy violations.

Organizations should have written policies and procedures and should ensure that they are up-to-date. Policies that define how PHI may be used and disclosed need to be understood by employees. Training should encompass the minimum necessary rule and when it is restricted, patients' rights with respect to their PHI, patient authorization requirements for disclosure of PHI, and organizational safeguards. Employees should be asked to sign attestations about their understanding of the policies and procedures and their agreement to cooperate and abide by them. It is especially important for all employees to understand that if they report a suspected compliance violation, there will be no retaliation from the organization.

Employees are not the only ones who need to commit to protecting a company's PHI. Business Associates must also attest to their commitment by signing a Business Associate Agreement. A Business Associate is defined by HIPAA as "an individual or corporate person who performs on behalf of the covered entity any function or activity involving the use or disclosure of protected health information (PHI) and is *not* a member of the covered entity's workforce."

Business Associates are contracted to perform functions on behalf of an organization and have access to PHI in performing these services. Common examples include accountants, attorneys, consulting personnel, and collection agencies.

Some organizations are getting creative in their approach to catching "snoopers" by setting up "honeypots" or "honeynuts." These are fictitious medical records that are closely monitored to determine if someone is attempting to access them inappropriately.

What to Do if You Find Someone "Snooping" in Your Organization

Snooping may be a reportable offense under the Health Information Technology for Economic and Clinical Health Act or the "HITECH Act" and should not be taken lightly by covered entities. Ensuring the proper policies and procedures are in place with mechanisms for reporting suspected offenses and continually educating employees will go a long way towards discouraging potential "snoopers" within your organization.

The HITECH Act imposes data breach notification requirements for unauthorized uses and disclosures of unsecured PHI. The Department of Health & Human Services ("HHS") has defined "secured PHI" as information that has been encrypted or destroyed. Under the HITECH Act "unsecured PHI" essentially means "unencrypted PHI."

> "Snooping" is defined as "prying into the private affairs of others, especially by prowling about."

HITECH requires that patients be notified of any unsecured breaches. A breach is defined as any unauthorized use or access to PHI where there is a significant risk of financial, reputational, or other harm to the individual. If the PHI accessed contains a) the type of services the individual received, such as oncology services, b) information that the individual received services from a specialized facility, such as a substance abuse treatment program, or c) information that increases the risk of identity theft, such as a social security number or an account number, it is considered a reportable breach.

Patient notification must include:

- A brief description of the breach, including the date of the breach and the date it was discovered
- A description of the type of PHI involved in the breach
- Steps the patient should take to protect himself/herself from potential harm resulting from the breach
- A brief description of any actions taken to investigate and mitigate losses from the breach and prevent further breaches
- Contact information in case there are additional questions

Additionally, all reportable breaches must be reported to the Secretary of Health & Human Services at the end of the year under the new HITECH law, unless there are over 500 breaches, in which case they must be reported within 60 days of identification of the breach. For more information, visit the HHS website at www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brinstruction.html. ■