Codify
BY AAPC

Health Information Compliance Alert

The Third Degree: Reader Questions Answered

TODAY IS YOUR LUCKY DAY

Question: Our facility likes to distribute a newsletter that includes a birthday section. Would it be okay to publish patients' special days (i.e., births, deaths, anniversaries, etc.), or does this violate HIPAA?

-- Ohio subscriber

Answer: It is a violation without patients' authorizations, says attorney **Kerry Kearney** of Pittsburgh's Reed Smith. However, it might also be considered marketing. "You're trying to prove what a nice place this is by showing that people stay for 50 years," Kearney explains.

If the disclosure is not intended to market the hospital as a trusted caregiver, then publishing that information "is not for treatment, payment or healthcare operations, so should be made only upon receipt of the individual's written authorization," cautions **William Hubbartt**, president of Hubbartt & Associates in St. Charles, IL.

Tip: Even if the disclosure is for marketing, it's good practice to allow patients to refuse the acknowledgement, asserts **C. Jon Burke**, a data security specialist for California's Toshiba American MRI and Toshiba American Medical Systems.

"It seems like innocent information, but it's not necessarily," he contends. Asking patients for an authorization will allow them some control over their information, he adds.

The Bottom Line: An authorization is your best bet for ensuring your patients are not upset by your use of their information, experts agree. Even if you think you can get away with publishing individually identifiable health information, "get authorizations and let your patients know what you're doing with their information," Burke says.

THIEF IN THE NIGHT

Question: One of our lab employees took PHI-laden patient files home with her. That night her home was burglarized and a few of those files were stolen. What is our responsibility? Would we be violating HIPAA if we did not contact those patients?

-- Texas subscriber

Answer: "This is a full-on disclosure," Burke says. Though policies and procedures should be in place to keep patient files from leaving secure areas, it is reality that they often do wind up in someone's car or home office, he explains.

"Entities are obligated to investigate the incident and take action to mitigate, to the extent practicable, any harmful effect of a use or disclosure of PHI," Hubbartt states. And they must sanction that employee if any of her actions went against the company's HIPAA policies and procedures.

This brings up the hardest question: "Must you tell the patient?" Kearney discusses. The general consensus is that the covered entity is responsible for notifying those patients whose files were stolen, she says.

The Bottom Line: When there is a privacy or security incident, entities "must account for it," Kearney states. Remember: In the case of medical records removed from the office and then stolen, the CE must take steps to prevent

this from happening again. "Reasonable safeguards must be established to protect against unauthorized disclosures," Hubbartt notes. The first step in mitigating this situation is to contact the patients. After that, analyze your risks and make policy changes, Burke insists.

EMAIL ME?

Question: We like to send e-mail reminders to employees who need to update their immunizations for MMR and Hepatitis, among others. Can we do this or do we need an authorization?

- Montana subscriber

Answer: If your employees must be properly immunized as condition of their employment, then sending them an e-mail is okay, experts agree.

However, because "e-mail is inherently insecure ... document that the employee was asked if e-mail was a permitted method of communication," counsels attorney **Marc Goldstone** of Hoagland & Longo in New Brunswick, NJ.

If your e-mail system is secure, your office is clear to send the reminders, says senior partner **Kathy LePar** of Beacon Partners in Norwell, MA. Remember: "Don't put them on your office bulletin board or in the employee lunch room where everyone can see," says **Kirk Nahra**, an attorney in the Washington, DC office of Wiley Rein & Fielding.

The Bottom Line: As always, keep in mind the vulnerabilities attached to any method of communication, but don't shrink away from e-mail. Tip: Get your employees' written consent to communicate with them via e-mail and you're safe, Goldstone assures.