Health Information Compliance Alert

Health Information News

CHICAGO HOSPITAL HUSTLES TO PROTECT PATIENTS' IDs

Officials of the University of Chicago Hospitals are scrambling to alert about 85 of their patients after one or more hospital employees stole patient identity information, reports the Chicago Tribune.

A hospital employee attempted to apply for credit cards using the patients' identities, but officials don't know whether the employee was able to obtain the credit cards. The FBI has yet to name the worker responsible for the security breach.

The hospital has tried to contact all 85 patients, offering the patients free credit checks, said **John Easton**, spokesman for the University of Chicago Hospitals.

The Bottom Line: A tightening of data access safeguards is planned, along with an enhancement of the security of the university hospitals' record storage.

MOVE QUICKLY TO MITIGATE E-MAIL MISTAKES

A lightning-speed reaction to an e-mail faux pas in the Palm Beach County (FL) Health Department saved 6,500 AIDS and HIV-positive county residents from disclosures of their PHI to more than 800 health care workers, according to the Associated Press.

John Nolan e-mailed county employees a monthly statistics report, but accidentally attached a file with the names and addresses of the individuals with AIDS. The department immediately shut down the e-mail system when Nolan realized the mistake - which was only minutes after the e-mail was sent.

Technicians believe that only 10 people opened the e-mail, but they could not determine how many of the county health care workers opened or viewed the attachment, said **Tim O'Connor**, spokesman for the county health department.

The Bottom Line: If your employees are well-trained in HIPAA compliance, they'll be able to pounce on - and rectify - accidental errors.

WIRELESS INTERNET COULD WRECK YOUR COMPLIANCE

If you think strong passwords are enough to protect your patients' PHI when using a wireless Internet connection, you're in for a surprise that could be costing your patients millions of dollars.

"Evil-twin" attacks use a laptop and Internet freeware to broadcast a radio signal that takes over wireless access points, USA Today reports. Once the hijack is complete, thieves can view and monitor the activities of all wireless users within hundreds of feet of the site.

Medical centers are not safe from the scam. Columbus Regional Medical Center in Columbus, GA, monitored 480 wireless devices at its 110 access points. Their surveillance stopped 120 attempts to steal confidential information.

The Bottom Line: You can prevent an evil-twin attack by installing personal firewall and security patches and by using only hot spots for Web surfing, **Anil Khatod,** CEO of software- and sensor-maker AirDefence, tells USA Today.

YOUR ACCOUNTING LOAD MAY LIGHTEN

You might not need to account for many routine PHI disclosures anymore, if the Confidentiality Coalition gets its way.

In a letter to the Department of Health and Human Services, the Coalition urged Secretary **Michael Leavitt** to modify the privacy rule's requirement for an accounting of PHI disclosures.

The coalition, comprised of more than 100 health care organizations, wrote that the tracking and accounting of PHI disclosures is "extremely burdensome and costly," noting that some hospitals were forced to hire new employees just to process paperwork related to HIPAA.

The Bottom Line: The coalition points out that "while only a small percentage of patients will ask for a list of disclosure accountings after their care, the hospital must maintain a specific record of each disclosure."