Employee data thefts challenge hospital information security

Although warnings about medical data breaches often focus on how healthcare facilities should protect their computer systems from external hackers, insider threats remain the single most consistent vulnerability.

A former employee of Parkland Memorial Hospital in Dallas, Texas, pleaded guilty in November of stealing patient information to recruit patients for his home healthcare business. In April, two registration employees of Jamaica Hospital Medical Center in New York were charged selling emergency department patients' personal information to people who then solicited outpatient care and other services to those patients. In other examples, information stolen by employees has been used for medical identity theft activities such as accessing medical care and filing false insurance claims and tax returns. (Sources: Dallas Morning News, InformationWeek)

For the healthcare facilities where they occur, such incidents can result in Health Insurance Portability and Accountability Act (HIPAA) violation penalties and other fines. Other costs can be incurred from class-action lawsuits, lost staff time, provision of identity theft protection services to affected patients and potential damage to the organization’s reputation. (Source: InformationWeek) In one survey, 75 percent of healthcare organizations named employee negligence as their biggest security concern. In 2013, 12 percent of organizations said they had experienced a case in which a “malicious insider” had breached patient privacy. (Source: InformationWeek)
Routinely educate employees on HIPAA and other legal requirements and your facility's policies for the use and disclosure of patient information. (Source: Department of Health and Human Services)

Secure protected health information by making sure that employees only have access to the information required for their roles and responsibilities. (Source: Becker’s Health IT & CIO Review)

Change authorizations such as passwords immediately when an employee leaves or changes positions, and promptly cut off all access when an employee leaves an organization. (Source: InformationWeek)

UPCOMING EVENTS

MONDAY 12

No Mass Gatherings Scheduled

If you are not yet subscribed to this daily brief, click here to sign up.

MESH does not assume any liability for the content, materials, information, and opinions provided within this communication. Further, MESH disclaims any liability resulting from use of any content within this communication. Information contained in this communication is provided "as is," with all faults. Neither MESH, nor any person associated with MESH, makes any warranty or representation with respect to the quality, accuracy, or availability of this information.

MESH serves as the designated Medical Multi-Agency Coordination Center for Marion County, Indiana. The MESH Intelligence Program is a joint-effort between the City of Indianapolis, Division of Homeland Security, the Marion County Public Health Department and the Indiana Department of Homeland Security designed to provide real-time information and support to the healthcare sector in the Indianapolis area. Assistance with info or questions at: Office phone: 317.630.7363, Pager: 317.310.6762, Email: MESHintel@meshcoalition.org

This email was sent by: MESH 3930 Georgetown Road Indianapolis, Indiana, 46254, USA. Weather forecast information appears pursuant to a license from AccuWeather®GlobalTM by Telemet, Inc. It is unlawful to copy or redistribute such information. If you would like to update your profile please click: Update Profile
If you prefer not to receive any more emails from us Unsubscribe