COMPLIANCE CONNECTION: Providing Relevant Issues and Hot Topics

IN THIS ISSUE

FEATURE ARTICLE

HIPAA Quiz

#1 – A billing clerk calls to verify information about a patient's treatment. Can you give this information?

#2 – A parent arrives in the emergency room demanding to know what is happening to his or her child. Can you answer?

DID YOU KNOW...

HIPAA privacy rule: Myths & Facts

Myth: *"Patients will sue health care providers for not complying with the HIPAA Privacy Regulation."*

Fact: ***The HIPAA Privacy Regulation does not give people the right to sue.***
Even if a person is the victim of an egregious violation of the HIPAA Privacy Regulation, the law does not give people the right to sue. Instead, the person must file a written complaint with the Secretary of Health and Human Services via the Office for Civil Rights. It is then within the Secretary's discretion to investigate the complaint.

Jail Terms for HIPAA Violations by Employees

The penalties for HIPAA violations by employees can be severe, especially those involving the theft of protected health information.

HIPAA violations by employees can attract a fine of up to $250,000 with a maximum jail term of 10 years and a 2-year jail term for aggravated identity theft.

This month there have been two notable cases of HIPAA violations by employees, one of which has resulted in a fine and imprisonment, with the other likely to result in a longer spell in prison when sentencing takes place in June.

Jail Term for Former Transformations Autism Treatment Center Employee

In February, a former behavioral analyst at the Transformations Autism Treatment Center (TACT) was discovered to have stolen the protected health information of patients following termination.

Jeffrey Luke, 29, of Collierville, TN gained access to a TACT Google Drive account containing the PHI of patients following termination and downloaded the PHI of 300 current and former patients onto his personal computer.

Approximately one month after Luke was terminated, TACT discovered patient information had been remotely accessed and downloaded. An investigation was launched and law enforcement was notified, with the latter alerting the FBI. Luke was identified as the perpetrator from his IP address, with the search of his residence uncovering a computer containing stolen electronic patient records and TACT forms and templates.

Luke's access rights to Google Drive had been terminated by TACT in accordance with HIPAA Rules; however, after termination, Luke had gained access to a shared Google Drive account and authorized access from his personal Gmail account.

It is unclear exactly how that was achieved after his access rights were terminated. Court documents say Luke hacked the account and law enforcement found evidence Luke had researched how to gain access to the data.

Law enforcement discovered this was not the first time Luke had stolen data from an employer. His computer also contained patient data from another former employer – Somerville, TN-based Behavioral and Counseling Services.

Read entire article:
https://www.hipaajournal.com/jail-terms-for-hipaa-violations-by-employees/

DID YOU KNOW...

Common HIPAA Violation:
INSIDER SNOOPING
This refers to family members or co-workers looking into a person's medical records without authorization. This can be avoided with password protection, tracking systems and clearance levels.

MIDLAND HEALTH

Theft of Unencrypted Laptop Sees Pathology Lab Patients' PHI Exposed

An unencrypted laptop computer issued to an employee of Clinical Pathology Laboratories Southeast, Inc., (CPLSE) has been stolen, exposing the protected health information of certain patients and their payment guarantors.

Prompt action was taken by CPLSE to prevent the laptop from being used to connect to its network and the theft was reported to law enforcement; however, it is possible that the protected health information stored on the laptop could have been viewed by unauthorized individuals.

An internal investigation was conducted to determine the types of information stored on the device which indicated the following PHI elements were potentially exposed: Names, addresses, driver's license numbers, Social Security numbers, government ID numbers, medical record numbers, and medical treatment information. Patients have now been notified of the breach and advised of the steps they can take to protect themselves against misuse of their data. Complimentary credit monitoring and identity theft protection services have been offered to affected individuals. Steps have also been taken to prevent similar incidents from occurring in the future, which include retraining staff on data security, updating appropriate policies and procedures, and using encryption technology on portable electronic devices used to store ePHI. The laptop was stolen on September 20, 2017 and the substitute breach notice uploaded to the CPLSE website on March 21, 2018. It is unclear why it took 6 months for the incident to be announced. HIPAA requires notifications to be issued within 60 days of the discovery of a breach.

Read entire article: https://www.hipaajournal.com/theft-of-unencrypted-laptop-sees-pathology-lab-patients-phi-exposed/

HIPAAQuiz

#1 – A billing clerk calls to verify information about a patient's treatment. Can you give this information?

Answer: In general, you may share patient information for the purpose of treating or billing a patient.

#2 – A parent arrives in the emergency room demanding to know what is happening to his or her child. Can you answer?

Answer: According to the Privacy Rule, PHI can generally be shared with the child's parents if they are the child's personal representatives. You must follow the organization's rules for disclosing this information. For example, you may need to refer the parents to another healthcare provider.

Example of HIPAA Violation Case in Healthcare

Nurse Faces Jail Time for HIPAA Violations

An employee at a midsize clinic was peripherally involved in a lawsuit when a car accident victim sued her husband. When the plaintiff became a patient at the clinic, the employee peeked at the patient's file and gave private info to her husband. The husband called the plaintiff and demanded that the lawsuit be dropped. The plaintiff quickly called the clinic and the Attorney General's office to complain. The employee faces a $250,000 fine and up to 10 years in prison if convicted. The clinic's head doctor fired the employee and immediately called a staff meeting on the importance of HIPAA.

Is UBER Health HIPAA Compliant?

This March, Uber officially launched Uber Health – A platform that makes arranging transport for patients more straightforward and cost effective. The service should benefit patients and providers alike, although questions have been raised about HIPAA and whether Uber Health is HIPAA compliant.

What is Uber Health? Uber Health consists of an online dashboard that healthcare providers can use to schedule transport for their patients in advance. Provided the patient has a mobile phone, he/she will receive a notification about the collection and drop off location via text message. In contrast to the standard Uber service, Uber Health does not require the use of a smartphone app.

By using Uber Health, healthcare providers can potentially reduce the number of no shows and ensure more patients turn up on time for their appointments. Rides can be scheduled when the patient is in a facility, ensuring they have transport arranged for follow up appointments. The service could also be used for caregivers and staff.

The official launch of the platform comes after a trial on around 100 healthcare organizations, with the platform now made available to healthcare organizations of all sizes.

Is Uber Health HIPAA Compliant? Any HIPAA-covered entity that signs up to use Uber Health would be required to enter patient names and appointment times into the system, so prior to using the service a business associate agreement would need to be obtained. Uber is happy to sign BAAs with all participating healthcare organizations.

Read entire article:
https://www.hipaajournal.com/uber-health-hipaa-compliant/

IN OTHER COMPLIANCE NEWS

LINK 1

Law Enforcement Notifies Cambridge Health Alliance About PHI Breach

https://www.hipaajournal.com/law-enforcement-notifies-cambridge-health-alliance-about-phi-breach/

LINK 2

Verizon PHI Breach Report Confirms Healthcare Has Major Problem with Insider Breaches

https://www.hipaajournal.com/verizon-phi-breach-report-healthcare-insider-breaches/

THUMBS UP!!!

Thumbs Up To ALL Departments For Implementing

MIDLAND HEALTH

- ***Main Campus***
- ***West Campus***
- ***Legends Park***
- ***501a Locations***

Take steps to keep information private when you talk to patients.

Balancing patient care and privacy can be a challenge.
Your efforts show you care about patients–and respect all patients' rights to privacy.

Limit what you say in public areas.
For example, if you'd like a patient in the waiting room to enter an exam room, only his or her name. Don't refer to the condition or reason for visit.

Use a private space.
Try to talk to patients in private places, such as an office or a private room.

Talk quietly.
When possible, lower your voice when talking to patients.

Do you have exciting or interesting Compliance News to report? Email an article or news link to:
Regenia Blackmon
Compliance Auditor
Regenia.Blackmon@midlandhealth.org