COMPLIANCE CONNECTION: Providing Relevant Issues and Hot Topics

IN THIS ISSUE

HIPAA privacy rule: Myths & Facts

Myth: *"Because I password-protect my smartphone, I can use it for receiving, storing, or transmitting patient PHI."*

Fact: Electronic PHI must be protected in compliance with the HIPAA administrative, physical, and technical safeguards, which prevent unauthorized disclosure, destruction, or loss of PHI. Loss or theft of mobile devices are one of the most frequently occurring reasons for breach of PHI, though in many instances the use of smartphones can enhance patient treatment. HIPAA safeguards must be in place for any mobile device used in treatment, payment, or healthcare operations. In addition to password protection, providers will want to encrypt PHI stored or sent on their mobile devices, activate remote wiping should the device be lost or stolen, install security and firewall software, keep software up-to-date, be careful downloading files or apps, and maintain physical control of one's phone.
Required measures should also be documented in the organization or practice's policies and procedures manual. For example, if staff members use their smartphones, is there a documented procedure for removal of PHI on the device if their employment is terminated or they leave the organization?

Resource:
https://www.todayswoundclinic.com/blog/hipaa-privacy-security-compliance-dispelling-common-myths

Healthcare Organizations Reminded of Importance of Securing Electronic Media and Devices Containing ePHI

In its August 2018 cybersecurity newsletter, the Department of Health and Human Services' Office for Civil Rights has reminded HIPAA-covered entities of the importance of implementing physical, technical, and administrative safeguards to ensure the confidentiality, integrity, and availability of electronic protected health information (ePHI) that is processed, transmitted, or stored on electronic media and devices.

Electronic devices such as desktop computers, laptops, servers, smartphones, and tablets play a vital role in the healthcare, as do electronic media such as hard drives, zip drives, tapes, memory cards, and CDs/DVDs. However, the portability of many of those devices/media means they can easily be misplaced, lost, or stolen. Physical controls are therefore essential. Anyone with physical access to electronic devices or media, whether healthcare employees or malicious actors, potentially have the ability to view, change, or delete data. Device configurations could be altered or malicious software such as ransomware or malware could be installed. All of these actions jeopardize the confidentiality, integrity, or availability of ePHI.

HIPAA – 45 CFR § 164.310(a)(1) – requires covered entities and their business associates to implement policies and procedures to restrict access to electronic devices and media and the facilities in which they are housed. 45 CFR § 164.310(d)(1) of the HIPAA Security Rule requires policies and procedures to be implemented to govern the receipt and removal of those devices into and out of an organization's facility, as well as movement within the facility. Robust policies and procedures must be developed to ensure ePHI is appropriately protected at all times.

When developing policies and procedures covering portable electronic devices and media, OCR recommends that HIPAA covered entities and their business associates consider the following questions:

- *Are records tracking the location, movements, alterations, repairs, and disposition of devices and media in place covering the entire life cycle of the devices/media?*
- *Does the organization's record of device and media movement include the individual(s) responsible for such devices and media?*
- *Have members of the workforce (including management) received training on the correct handling of devices/media to ensure ePHI is safeguarded at all times?*

Read entire article:
https://www.hipaajournal.com/healthcare-organizations-reminded-of-importance-of-securing-electronic-media-and-devices-containing-ephi/

DID YOU KNOW...

Common HIPAA Violation:
"Exceeding the 60-Day Deadline for Issuing Breach Notifications"

The HIPAA Breach Notification Rule requires covered entities to issue notifications of breaches without unnecessary delay, and certainly no later than 60 days following the discovery of a data breach. Exceeding that time frame is one of the most common HIPAA violations.

MIDLAND HEALTH

Couple Sues McAlester Hospital Over Alleged Snooping and Impermissible Disclosure

Following the accidental drowning of their adopted son, Denise and Wayne Russell were contacted by the child's birth mother who made threats against their family.

The phone call from the birth mother came shortly after their son was admitted to McAlester Regional Health Center following a tragic swimming pool accident. Their 2-year old child had fallen into the pool after the gate to the pool area had been accidentally left open. The parents administered CPR at the scene until the paramedics arrived and the child was rushed to hospital where he was later confirmed to have died.

Shortly after their son died, the Russells received the telephone call from the birth mother. When asked how she knew about the accident and death of the child, she confirmed that she had been informed by the hospital. The birth month screamed at the Russells and made multiple threats, according to Denise Russell, including a threat to kill their other son. The situation became so bad that a protective order was filed against their son's birth mother. The Russells had taken care of their adopted son Keon since he was two weeks old and finalized the adoption in July 2015. Under the terms of the adoption, the birth mother terminated all of her parental rights. Even so, an employee at the hospital contacted the birth mother to alert her to the death of her son.

In the lawsuit the Russells claim that as a result of the impermissible disclosure of their son's health information they have experienced "extreme emotional distress" from having to deal with the birth mother. The couple are seeking $150,000 in damages.

The call to the birth mother was made by an employee of the hospital, although according to the lawsuit that was not the only privacy violation and HIPAA violation that occurred. The lawsuit alleges multiple hospital workers accessed Keon's medical records without authorization, including workers in the hospital cafeteria.

Read entire article:
https://www.hipaajournal.com/couple-sues-mcalester-hospital-over-alleged-snooping-and-impermissible-disclosure/

HIPAAQuiz

You're waiting in line at the cafeteria, chatting with a coworker. You start telling her about a patient and the difficulties she's having with her pregnancy. What is wrong with this situation?

Answer: You should never reveal PHI in a public place. You should only discuss PHI with authorized staff who need to know the information to treat the patient or to carry out other acceptable tasks, such as billing the patient.

EMTALA — Emergency Medical Treatment and Active Labor Act

EMTALA Review:

- Under EMTALA, Medicare hospitals must provide a Medical Screening Exam (MSE) to:
  - All patients who come to a dedicated emergency department and request medical services
  - All patients who come to any location on the hospital campus and within a 250 yard sphere, and ask for treatment for a possible emergency condition
  - All patients who come to any location on the hospital campus and within a 250 yard sphere, and appear to have an emergency medical condition
  - All patients transported to the hospital via an ambulance
- Patients must receive an MSE whether or not they are able to pay.
- To comply with EMTALA, do not talk about payment until AFTER the patient has been screened and stabilized.
- Triage is not an acceptable MSE under EMTALA.
- The MSE must be comprehensive enough to determine whether a patient has an Emergency Medical Condition (EMC).
- In general, determining or excluding an EMC may require:
  - A complete medical history
  - Taking vital signs at regular intervals
  - Performing a physical examination
  - Performing any necessary lab or imaging studies
- If a complete MSE does not find an EMC, the hospital has no further EMTALA obligation to the patient.
- However, if the MSE finds an EMC, the hospital must do one or both of the following;
  - Stabilize the patient
  - Transfer the patient to another facility if medically necessary
- On-Call physicians must respond promptly when called and provide care at the hospital.
  - Physicians must be prepared to leave non-emergent patients to respond to call
  - Physicians must respond to call by going to the patient's current location
- A transfer is not appropriate for financial reasons or physician/hospital convenience.
- Under EMTALA a Medicare hospital must accept a request for incoming transfer if the hospital has the necessary resources needed to treat the patient and the transferring hospital is less able to treat the patient.
- The purpose of EMTALA is to prevent discrimination in the treatment of patients with emergency medical conditions. Under EMTALA, all patients have the same rights to emergency care, regardless of ability to pay.
- The Centers for Medicare and Medicaid Services (CMS) review all EMTALA complaints and investigate if the complaint seems legitimate.
- If the EMTALA violation is proven, CMS informs the hospital of its two options:
- The hospital must submit a plan of corrective action to CMS
- The hospital will lose its status as a Medicare provider in 23 days
- CMS informs the OIG of findings. If the OIG can prove an EMTALA violation, it can impose fines.
- Fines are:
  - Up to $50,000 per violation for hospitals with 100 beds or more
  - Up to $25,000 per violation for hospitals with less than 100 beds
  - Up to $50,000 per violation for individual physicians
  - These fines are not covered by malpractice insurance.

Submitted by:
Robyn Kedzie, Executive Director Quality Management
Midland Health

IN OTHER COMPLIANCE NEWS

LINK 1

Plaintiffs in Class Action Claim Premera Blue Cross Destroyed Key Evidence

https://www.hipaajournal.com/plaintiffs-in-class-action-claim-premera-blue-cross-destroyed-key-evidence/

LINK 2

Phishing Attack on Legacy Health Results In Exposure of 38,000 Patients' PHI

https://www.hipaajournal.com/phishing-attack-legacy-health/

THUMBS UP!!!

Thumbs Up To ALL Departments For Implementing

MIDLAND HEALTH

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

A closer look at Protected Health Information (PHI)….

Remember, PHI is any health information an organization has or gets from another organization that could be used to identify a specific individual.

Limit the PHI you give or take.
For example, if you:

- *call out a person's name in a pharmacy, don't say what medication the person is picking up*

Limit the PHI you give or take.
For example, if you:

- *call out a patient's name in a waiting room, don't reveal any other any information about the patient's condition or reason for the visit*

Limit the PHI you give or take.
For example, if you:

- *ask patients to use a sign-in sheet, ask only for their name, not the reason for their visit*

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