NOVEMBER 2018

COMPLIANCE CONNECTION

COMPLIANCE HOTLINE
877•780•9367

COMPLIANCE CONNECTION: Providing Relevant Issues and Hot Topics

IN THIS ISSUE

DID YOU KNOW...

HIPAA privacy rule: Myths & Facts

Myth:

“Providers must obtain consent for sharing PHI for purposes of treatment or billing.”

Fact:

For purposes of treatment, payment, or healthcare operations, providers are not required to obtain consent of the patient or his/her personal representative. (Healthcare operations include medical review, legal services, business management, and administrative activities that are necessary for the CE to run its business). However, some states require consent to use or disclose health information. The HIPAA Privacy Rule doesn’t prohibit providers from obtaining patient consent for use or disclosure of PHI. In fact, some states require consent for disclosure of PHI, which is completely permissible under HIPAA regulations.

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

Claxton-Hepburn Medical Center Fires Several Employees for Inappropriate PHI Access

Claxton-Hepburn Medical Center, a not-for-profit 115-bed community hospital in Ogdensburg, NY, has fired several employees for accessing patient health records without authorization.

The PHI breaches were discovered during an internal investigation. It is unclear whether that investigation was launched following a complaint that had been received or if the patient privacy violations were uncovered during a routine audit of PHI access logs – A requirement of HIPAA.

Claxton-Hepburn Medical Center has not publicly disclosed how many employees were terminated over the violations, only reporting that all employees who purposely committed the acts were terminated. It is also currently unclear exactly how many patients’ PHI was breached.

Claxton-Hepburn Medical Center has confirmed that training is given to all employees on the first day of employment detailing the requirements of HIPAA and the importance of protecting the privacy of patients. All employees are made aware that accessing patient health information is only permitted when PHI needs to be viewed to complete work duties or when patient records need to be updated, as per the requirements of the HIPAA Privacy Rule. Employees are also made aware that any unauthorized accessing of PHI will result in disciplinary action. It would have been clear to the employees concerned that their actions were in violation of HIPAA Rules.

The discovery of the privacy breaches has prompted the hospital to implement further safeguards to reduce the likelihood of future HIPAA violations of this nature occurring. Claxton-Hepburn Medical Center has also notified all patients by mail whose records were inappropriately accessed.

While it is possible for criminal charges to be filed against healthcare employees for HIPAA Privacy Rule violations, in this instance Claxton-Hepburn Medical Center has not involved the police.

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

DID YOU KNOW...

Common HIPAA Violation:

“Failure to Enter into a HIPAA-Compliant Business Associate Agreement”

The failure to enter into a HIPAA-compliant business associate agreement with all vendors that are provided with or given access to PHI is another of the most common HIPAA violations. Even when business associate agreements are held for all vendors, they may not be HIPAA compliant, especially if they have not been revised after the Omnibus Final Rule.

MIDLAND HEALTH

FDA Issues Medical Device Cybersecurity Regional Incident Preparedness and Response Playbook

On October 1, 2018, the U.S. Food and Drug Administration released a Medical Device Cybersecurity Regional Incident Preparedness and Response Playbook for healthcare delivery organizations to help them prepare for and respond to medical device cybersecurity incidents.

The playbook is intended to help healthcare delivery organizations develop a preparedness and response framework to ensure they are prepared for medical device security incidents, can detect and analyze security breaches quickly, contain incidents, and rapidly recover from attacks.

The playbook was developed by MITRE Corp., which worked closely with the FDA, healthcare delivery organizations, researchers, state health departments, medical device manufacturers and regional healthcare groups when developing the document.

The past 12 months have seen many vulnerabilities identified in medical devices which could potentially be exploited by hackers to gain access to healthcare networks, patient health information, or to cause harm to patients. While the FDA has not received any reports to suggest an attack has been conducted on medical devices to cause patients harm, the number of cyberattacks on healthcare organizations has increased significantly in recent years and concerns have been raised with the FDA about the potential for cybercriminals to attack patient medical devices.

"The playbook supplements existing HDO emergency management and/or incident response capabilities with regional preparedness and response recommendations for medical device cybersecurity incidents," said MITRE. "The playbook outlines how hospitals and other HDOs can develop a cybersecurity preparedness and response framework, which starts with conducting device inventory and developing a baseline of medical device cybersecurity information."

Read entire article:

https://www.hipaajournal.com/fda-issues-medical-device-cybersecurity-regional-incident-preparedness-and-response-playbook/

HIPAAQuiz

You have a board in the nurses' station where you can post the names of patients who are being treated. It faces the hall so that information is quickly available. Why is this a problem under the Privacy Rule?

Answer: PHI may be kept accessible to staff who need it to treat patients, but steps should be taken to keep others from seeing it. For example, place any sources containing PHI in a way that visitors or other patient cannot see it.

Remote Hacking of Medical Devices and Systems Tops ECRI's 2019 List of Health Technology Hazards

The ECRI Institute, a non-profit organization that researches new approaches to improve patient care, has published its annual list of the top ten health technology hazards for 2019.

The purpose of the list is to help healthcare organizations identify possible sources of danger or issues with technology that have potential to cause patients harm to allow them to take action to reduce the risk of adverse events occurring.

To create the list, ECRI Institute engineers, scientists, clinicians and patient safety analysts used expertise gained through testing of medical devices, investigating safety incidents, assessing hospital practices, reviewing literature and talking to healthcare professionals and medical device suppliers to identify the main threats to medical devices and systems that warrant immediate attention.

Weighting factors used to produce the final top 10 list includes the likelihood of hazards causing severe injury or death, the frequency of incidents, the number of individuals likely to be affected, insidiousness, effect on the healthcare organization, and the actions that could realistically be taken to reduce any impact on patient care.

Unsurprisingly, given the volume of cyberattacks on healthcare organizations, the high potential for harm, and the number of individuals that could be affected, the remote accessing of healthcare systems by hackers was rated as the number one hazard for 2019.

There is considerable potential for the remote access functionality of medical devices and systems to be exploited by hackers. A cyberattack could render medical devices and systems inoperative or could degrade their performance, which could have a major negative impact on patient care and could place patients' lives at risk. Cyberattacks could also result in the theft of health data, which could also have a negative effect on patients.

ECRI notes that while cyberattacks can have a negative impact on healthcare providers, resulting in reputation damage and significant fines, cybersecurity is also a critical patient safety issue.

Hackers can easily take advantage of unmaintained and vulnerable remote access systems to gain access to medical devices and healthcare systems. They can move laterally within the network and gain access to medical and nonmedical assets and connected devices and systems. Patient data can be stolen, malware installed, computing resources can be hijacked, and ransomware can be installed which could render systems inoperable. In the most part, these attacks are preventable.

"Safeguarding assets requires identifying, protecting, and monitoring all remote access points, as well as adhering to recommended cybersecurity practices, such as instituting a strong password policy, maintaining and patching systems, and logging system access," suggests ECRI.

Read entire article:

https://www.hipaajournal.com/ecri-2019-top-ten-health-technology-hazards/

IN OTHER COMPLIANCE NEWS

LINK 1

Michigan Medicine Notifies 3,600 Patients of PHI Disclosure Due to Mailing Error

https://www.hipaajournal.com/michigan-medicine-notifies-3600-patients-of-phi-disclosure-due-to-mailing-error/

LINK 2

Remote Hacking of Medical Devices and Systems Tops ECRI's 2019 List of Health Technology Hazards

https://www.hipaajournal.com/ecri-2019-top-ten-health-technology-hazards/

THUMBS UP!!!

Thumbs Up To ALL Departments For Implementing

Awareness of

HIPAA, PII, PHI, ePHI & Social Media

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.

Authorization is WRITTEN permission to use health information to include specific details about:

‣ ***what*** *information can be used*

Authorization is WRITTEN permission to use health information to include specific details about:

‣ ***how*** *the information can be used*

Authorization is WRITTEN permission to use health information to include specific details about:

‣ ***how long*** *the information can be used*

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