COMPLIANCE CONNECTION: Providing Relevant Issues and Hot Topics

IN THIS ISSUE

FEATURE ARTICLE

• Facebook Sharing of PHI Sees ER Doc Fired

HIPAA Quiz

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? How could it be fixed?
(See answer on Page 2)

DID YOU KNOW...

HIPAA privacy rule: Myths & Facts

Myth: *"The Privacy Regulation mandates all sorts of new disclosures of patient information."*

Fact: As HHS states, disclosure is mandated in only two situations: to the individual patient upon request, or to the Secretary of the Department of Health and Human Services for use in oversight investigations. Disclosure is permitted, not mandated, for other uses under certain limits and standards, such as to carry out treatment, payment, or health care operations, or under other applicable laws. Disclosure of protected health information has always been permitted for purposes such as national security, public health monitoring, and law enforcement, as well as many others. The Privacy Rule requires that patients be informed, through the notice of privacy practices, of these uses and disclosures. Nearly all of these uses and disclosures are permissive, so health care plans and providers may choose not to use or disclose medical information.

Facebook Sharing of Patient Info Sees ER Doc Fired

A doctor has recently been fined $500 by the State medical board after posting personally identifiable information about a patient on Facebook, a number of months after the incident caused her to lose her employment. This is a HIPAA violation that all healthcare professionals should take note of.

The doctor, Alexandra Thran, did not post the patient's name in her post, which would be an immediate violation of HIPAA Rules, but she did post sufficient information to enable the person to be identified. Another individual who visited Thran's Facebook page was able to determine the identity of the patient from the information she wrote on the page, even in the absence of the patient's name.

The disclosure of Protected Health Information, which includes references to medical treatments as well as health records, along with Personally Identifiable Information (PII) can result in civil penalties being brought against the covered entity and any individual responsible for the HIPAA breach. The penalties can involve time in jail.

This is not the first incident of its kind. Nurses and doctors have been fired by their employers in California and Wisconsin for having social media discussions about patients via social media.

One problem is that users of social media are encouraged to share all manner of information with friends and relatives, yet in a work setting the potential for HIPAA violations means extreme caution should be taken. In this case the incident involved an ER doctor, and the conversation was not had with the patient. Some doctors may be choosing social media channels to interact with patients but there is considerable potential for a HIPAA violation.

With social media it is too easy to write something and regret it after it has been sent, but by that time it is too late and control of information released has been lost. To tackle the issue, it is essential that healthcare providers start to develop policies covering the use of social media, the sharing of PHI and communicating with patients through secure channels.

Social media use is only likely to grow, and with it so will the risk of causing HIPAA violations. It is better to train the staff on Privacy Rules and to set strict policies covering the use of Facebook and other platforms. Many hospitals have identified the risk and have taken action and put together policies for staff to make it clear on what is allowed and what is strictly forbidden. Children's Hospital Boston, for example, has just developed a 6-page document detailing allowable uses of social media and do's and don'ts, with many other hospitals now electing to do the same.

Resource: https://www.hipaajournal.com/facebook-sharing-of-patient-info-sees-er-doc-fired/

DID YOU KNOW...

Common HIPAA Violation:

Failure to Properly Release Information to Patients

According to HIPAA, a patient has the right to receive electronic copies of medical records on demand.

MIDLAND HEALTH

What is the Relationship Between HITECH, HIPAA, and Electronic Health and Medical Records?

The Health Insurance Portability and Accountability Act (HIPAA) was signed into law in August 1996, and was updated by the HIPAA Privacy Rule in 2003 and the HIPAA Security Rule in 2005, but how did the Health Information Technology for Economic and Clinical Health (HITECH) Act change HIPAA and what is the relationship between HITECH, HIPAA, and electronic health and medical records?

What is the Relationship Between HITECH and HIPAA and Medical Records? *Title I of HIPAA is concerned with the portability of health insurance and protecting the rights of workers between jobs to ensure health insurance coverage is maintained, which have nothing to do with the HITECH Act. However, there is a strong relationship between HITECH and HIPAA Title II. Title II of HIPAA includes the administrative provisions, patient privacy protections, and security controls for health and medical records and other forms of protected health information (PHI). One of the main aims of the HITECH Act was to encourage the adoption of electronic health and medical records by creating financial incentives for making the transition from paper to digital records. The HITECH Act also strengthened the HIPAA Privacy and Security Rules with respect to electronic health and medical records. The HITECH Act required the Secretary of the HHS to ensure guidance was issued annually to covered entities and business associates to help them implement appropriate technical safeguards to ensure the confidentiality, integrity, and availability of PHI. The technologically neutral nature of HIPAA had led to confusion about how best to protect PHI.*

How did the HITECH Act Change HIPAA? *The HITECH Act, which was published on January 25, 2013, made several changes to HIPAA and introduced new requirements for HIPAA-covered entities with notable changes for business associates.*

Read entire article: https://www.hipaajournal.com/category/hitech-act-news/

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? How could it be fixed?

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 patients cannot see it.

More than 90% of Hospitals and Physicians Say Mobile Technology is Improving Patient Safety and Outcomes

90% of hospitals and 94% of physicians have adopted mobile technology and say it is helping to improve patient safety and outcomes, according to a recent survey conducted by Black Book Research.

The survey was conduced on 770 hospital-based users and 1,279 physician practices between Q4, 2017 and Q1, 2018.

The survey revealed 96% of hospitals are planning on investing in a new clinical communications platform this year or have already adopted a new, comprehensive communications platform.

85% of surveyed hospitals and 83% of physician practices have already adopted a secure communication platform to improve communications between care teams, patients, and their families. Secure text messaging platform are fast becoming the number one choice due to the convenience of text messages, the security offered by the platforms, and the improvements they make to productivity and profitability.

98% of hospitals and 77% of physician practices said they have implemented secure, encrypted email and are using intrusion detection systems to ensure breaches are detected rapidly.

Many providers of secure text messaging solutions have developed their platforms specifically for the healthcare industry. The platforms incorporate all the necessary safeguards to meet HIPAA requirements and ensure PHI can be transmitted safely and securely. Text messaging is familiar to almost all employees who are provided access to the platforms and they make communication quick and easy.

However, 63% of respondents to the survey said they are still facing ongoing challenges with buy-in of general mobile adoption strategies and related enterprise technology execution.

30% of respondents said that even though secure methods of communication have been implemented such as encrypted text messaging platforms and secure email, they are still receiving communications on a daily basis from unsecured sources that contain personally identifiable information such as patients' names and birthdates.

Part of the study involved an assessment of cybersecurity and privacy software and services, allowing the company to identify the vendors that are most highly regarded by customers. TigerText, the market leading provider of secure text messaging solutions for the healthcare industry, was rated highly across the board, as were Vocera, Spok, Doc Halo, and Imprivata. Doc Halo was the highest rated secure communications platform provider among physician organizations, with Perfect Serve, Patient Safe Solutions, OnPage, Telemediq, and Voalte also scoring highly. Spok ranked highest among hospital systems and inpatient organizations, with Qlik and Cerner also receiving high marks.

Read entire article:
https://www.hipaajournal.com/more-than-90-of-hospitals-and-physicians-say-mobile-technology-is-improving-patient-safety-and-outcomes/

IN OTHER COMPLIANCE NEWS

LINK 1

OCR Reminds Covered Entities Not to Overlook Physical Security Controls

https://www.hipaajournal.com/ocr-reminds-covered-entities-not-to-overlook-physical-security-controls/

LINK 2

Warnings Issued Over Vulnerable Medical Devices

https://www.hipaajournal.com/warnings-issued-over-vulnerable-medical-devices/

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.

Remember the minimum necessary information rule.
Do not *access information that you do not need for your job.* ***Do not*** *share information unless another needs it to do his or her job..*

Take care when talking to or about a patient.
This includes speaking quietly, choosing a private location and not revealing unnecessary information.

Be aware of what information is protected.
Remember, PHI includes any information that could identify a person.

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