COMPLIANCE CONNECTION: Providing Relevant Issues and Hot Topics

IN THIS ISSUE

FEATURE ARTICLE

HIPAA Quiz

You're waiting in line in the cafeteria, chatting with a co-worker. You start telling her about a patient and difficulties she's having with her pregnancy. What's wrong with this situation?
(See answer on Page 2)

DID YOU KNOW...

HIPAA privacy rule: Myths & Facts

Myth: *"The HIPAA Privacy Rule imposes many new restrictions on hospitals' fundraising efforts so that fundraising becomes almost impossible."*

Fact: ***According to the Rule, a hospital may use, or disclose to its "business associate" or an institutionally related foundation, demographic information and the dates of health care provided to an individual "for the purpose of raising funds for its own benefit, without an authorization [from the patient]." Such use or disclosure is not permitted unless disclosed in the notice of privacy practices.*** Any fundraising materials that the covered entity sends to an individual must include a description of how the individual may opt out of future fundraising communications. Therefore, the Rule does not hinder fundraising in the first instance, and if a covered entity wants to target specific patients it must include this information in its notice of privacy practices.

What Happens if a Nurse Violates HIPAA?

What happens if a nurse violates HIPAA Rules? How are HIPAA violations dealt with and what are the penalties for individuals that accidentally or deliberately violate HIPAA and access, disclose, or share protected health information (PHI) without authorization? The Health Insurance Portability and Accountability Act (HIPAA) Privacy, Security, and Breach Notification Rules must be followed by all covered entities and their business associates. The failure to comply with HIPAA Rules can result in significant penalties for HIPAA covered entities. Business associates of covered entities can also be fined directly for HIPAA violations, but what about individual healthcare workers such as nurses? What happens if a nurse violates HIPAA Rules?

What are the Penalties if a Nurse Violates HIPAA? Accidental HIPAA violations by nurses happen, even when care is taken to follow HIPAA Rules. While all HIPAA violations can potentially result in disciplinary action, most employers would accept that accidental violations are bound to occur from time to time. In many cases, minor violations of HIPAA Rules may not have negative consequences and can be dealt with internally. Employers may decide to provide additional training in some cases to ensure the requirements of HIPAA are fully understood. If a nurse violates HIPAA by accident, it is vital that the incident is reported to the person responsible for HIPAA compliance in your organization – the Privacy Officer, if your organization has appointed one – or your supervisor. The failure to report a minor violation could have major consequences. You can read more about accidental HIPAA violations here. Serious violations of HIPAA Rules, even when committed without malicious intent, are likely to result in disciplinary action, including termination and punishment by the board of nursing. Termination for a HIPAA violation does not just mean loss of current employment and benefits. It can make it very hard for a nurse to find alternative employment. HIPAA-covered entities are unlikely to recruit a nurse that has previously been fired for violating HIPAA Rules. Willful violations of HIPAA Rules, including theft of PHI for personal gain or use of PHI with intent to cause harm, can result in criminal penalties for HIPAA violations. HIPAA-covered entities are likely to report such incidents to law enforcement and investigations will be launched. Complaints about HIPAA violations submitted to the Office for Civil Rights can be referred to the Department of Justice to pursue criminal penalties, including fines and imprisonment. Criminal prosecutions are rare, although theft of PHI for financial gain is likely to result in up to 10 years in jail. There is no private cause of action in HIPAA. If a nurse violates HIPAA, a patient cannot sue the nurse for a HIPAA violation. There may be a viable claim, in some cases, under state laws.
Examples of HIPAA Violations by Nurses: The list of possible HIPAA violations by nurses is long, here are a few: ***•Accessing the PHI*** *of patients you are not required to treat;* ***•Gossiping****–Talking about specific patients and disclosing their health information to family, friends & colleagues;* ***•Disclosing PHI*** *to anyone not authorized to receive the information;* ***•Taking PHI*** *to a new…*

Read entire article: https://www.hipaajournal.com/what-happens-nurse-violates-hipaa/

DID YOU KNOW...

Common HIPAA Violation:
IMPROPER DISPOSAL OF PATIENT RECORDS
Shredding is necessary before disposing of patient's records.

MIDLAND HEALTH

2 to 6 Year Jail Term for Receptionist Who Stole PHI from Dentist Office

A former receptionist at a New York dental practice has been sentenced to serve 2 to 6 years in state penitentiary for stealing the protected health information of hundreds of patients.

Annie Vuong, 31, was given access to the computer system and dental records of patients in order to complete her work duties. Vuong abused the access rights and stole the PHI of more than 650 patients. That information was passed to her co-defendants who used the data to steal identities and make fraudulent purchases of high value items. Vuong was arrested on February 2, 2015, following a two-and-a-half-year investigation into identity theft by the New York District Attorney's Office. The theft of data occurred between May and November 2012, when the PHI of 653 patients was taken from the dental office. The types of information stolen included names, birth dates, and Social Security numbers. That information was shared with co-defendant Devin Bazile in an email. Bazile used the information to obtain credit lines from Barclaycard in the victims' names. Credit ranged from $2,000 to $7,000 per individual. Bazile along with co-defendants Joshua Hamilton and Ahmeen Evans used the credit to purchase Apple gift cards that were used by buy tablets and laptop computers totaling more than $700,000. Bazile and Haughton had already been convicted and sentenced to lengthy jail terms for their role in the identity theft scheme. Bazile and Haughton were convicted of Grand Larceny in the Second Degree in 2015 and were sentenced to serve 3 to 9 years and 1 and 1/3 to 4 years in jail respectively. Evans was also convicted of Grand Larceny in the Second Degree and was sentenced to 5 years' probation. Vuong was found guilty of 189 counts against her including one count of Grand Larceny in the Second Degree, 49 counts of Grand Larceny in the Third Degree, 63 counts of Identity Theft in the First Degree, 45 counts of Grand Larceny in the Fourth Degree, 30 counts of Identity Theft in the Second Degree, and one count of Unlawful Possession of Personal Identification Information in the Second Degree.

Resource: https://www.hipaajournal.com/2-to-6-year-jail-term-for-receptionist-who-stole-phi-from-dentist-office/

HIPAAQuiz

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

Answer: You should never reveal PHI in a public place. You should always 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 a patient.

How to Defend Against Insider Threats in Healthcare

One of the biggest data security challenges is how to defend against insider threats in healthcare. Insiders are responsible for more healthcare data breaches than hackers, making the industry unique. Verizon's Protected Health Information Data Breach Report highlights the extent of the problem. The report shows 58% of all healthcare data breaches and security incidents are the result of insiders. Healthcare organizations also struggle to detect insider breaches, with many breaches going undetected for months or even years. One healthcare employee at a Massachusetts hospital was discovered to have been accessing healthcare records without authorization for 14 years before the privacy violations were detected, during which time the records of more than 1,000 patients had been viewed. Healthcare organizations must not only take steps to reduce the potential for insider breaches, they should also implement technological solutions, policies, and procedures that allow breaches to be detected rapidly when they do occur.

What are Insider Threats? Before explaining how healthcare organizations can protected against insider threats, it is worthwhile covering the main insider threats in healthcare. An insider threat is one that comes from within an organization. That means an individual who has authorization to access healthcare resources, which includes EMRs, healthcare networks, email accounts, or documents containing PHI. Resources can be accessed with malicious intent, but oftentimes mistakes are made that can equally result in harm being caused to the organization, its employees, or its patients. Insider threats are not limited to employees. Any individual who is given access to networks, email accounts, or sensitive information in order to complete certain tasks could deliberately or accidentally take actions that could negatively affect an organization. That includes business associates, subcontractors of business associates, researchers, volunteers, and former employees. The consequences of insider breaches can be severe. Healthcare organizations can receive heavy fines for breaches of HIPAA Rules and violations of patient privacy, insider breaches can damage an organization's reputation, cause a loss of patient confidence, and leave organizations open to lawsuits. According to the CERT Insider Threat Center, insider breaches are twice as costly and damaging as external threats. To make matters worse, 75% of insider threats go unnoticed. Insider threats in healthcare can be split into two main categories based on the intentions of the insider: Malicious and non-malicious.

Malicious Insider Threats in Healthcare Malicious insider threats in healthcare are those which involve deliberate attempts to cause harm, either to the organization, employees, patients, or other individuals. These include the theft of protected health information such as social security numbers/personal information for identity theft and fraud, the theft of data to take to new employers, theft of intellectual property, and sabotage. Research by Verizon indicates 48% of insider breaches are conducted for financial gain, and with healthcare data fetching a high price on the black market, employees can easily be tempted to steal data. ***A 2018 Accenture survey conducted on healthcare employees revealed one in five would be prepared to access and sell confidential data if the price was right. 18% of the 912 employees surveyed said they would steal data for between $500 and $1,000.***

Read entire article: https://www.hipaajournal.com/how-to-defend-against-insider-threats-in-healthcare/

IN OTHER COMPLIANCE NEWS

LINK 1

How to Defend Against Insider Threats in Healthcare

https://www.hipaajournal.com/how-to-defend-against-insider-threats-in-healthcare/

LINK 2

Study Reveals Healthcare Industry Employees Struggling to Understand Data Security Risks

https://www.hipaajournal.com/healthcare-industry-employees-struggling-to-understand-data-security-risks/

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.

Pay attention to information that gives details about who a person is: *(e.g., name; all or part of address; date of birth; admission/discharge date; etc.) When combined could be could be considered PHI.*

PHI takes many forms. *A medical record is an obvious example of PHI; a prescription label with patient name and name of drug; doctor's notes; X-ray; a letter giving patient test results.*

The Privacy Rule covers PHI in any format. *PHI must be kept private whether it is in written, spoken or electronic form.*

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