COMPLIANCE CONNECTION: Providing Relevant Issues and Hot Topics

IN THIS ISSUE

HIPAA Privacy Rule: Myths & Facts

Myth: HIPAA Privacy Rule Applies Only to Electronic Records

"As long as medical records are on good old paper, there is no need to comply with HIPAA privacy regulations that apply to electronically stored and transmitted electronic."

Fact: HIPAA covers all patient records, regardless of their nature.

Paper sign-in records and medical records do not make your healthcare facility exempt from adhering to the HIPAA Privacy Rule. HIPAA privacy requirements cover not only electronic health information.

As long as the information can be stored, handled, transmitted, breached or stolen, it needs to be protected by HIPAA. So even if you only have paper patient records, you must be compliant with the HIPAA Privacy Rule.

Also, it's the 21st century. Paper medical records are so last millennium.

Resource:
https://www.qminder.com/hipaa-myths-debunked/

PHI Compromised in CVS Pharmacy and Walgreens Break-ins

CVS Pharmacy is alerting certain patients that some of their personal and protected health information has been lost following several incidents at its pharmacies between May 27, 2020 and June 8, 2020. During that time frame, several of its pharmacies were affected by looting and vandalism incidents. Unauthorized individuals gained access to several of its stores and stole filled prescriptions from pharmacy waiting bins. Vaccine consent forms and paper prescriptions were also lost and potentially stolen in the incidents.

The types of information compromised include names, addresses, dates of birth, medication names, prescriber information, and primary care provider information. No reports have been received to date to indicate there has been any misuse of customer information.

CVS Pharmacy has reported the incidents to the HHS' Office for Civil Rights collectively as affecting 21,289 individuals.

Walgreens Reports Series of Break-ins and Theft of PHI

Walgreens Pharmacy has reported similar incidents at its pharmacies over the same period. According to the breach notification sent to the California Attorney General's office, various groups of individuals broke into Walgreens stores in several locations between May 26, 2020 and June 5, 2020. The individuals stole many items from the stores, some of which contained the personal and protected health information of its customers.

Read entire article:
https://www.hipaajournal.com/phi-compromised-in-cvs-pharmacy-and-walgreens-break-ins/

DID YOU KNOW...

Snooping on Healthcare Records

Accessing the health records of patients for reasons other than those permitted by the Privacy Rule – treatment, payment, and healthcare operations – is a violation of patient privacy. Snooping on healthcare records of family, friends, neighbors, co-workers, and celebrities is one of the most common HIPAA violations committed by employees. When discovered, these violations usually result in termination of employment but could also result in criminal charges for the employee concerned. Financial penalties for healthcare organizations that have failed to prevent snooping are relatively uncommon.

Resource: https://www.hipaajournal.com/common-hipaa-violations/

MIDLAND HEALTH

NEWS

IBM Security 2020 Cost of Data Breach Report Shows 10% Annual Increase in Healthcare Data Breach Costs

The 2020 Cost of Data Breach Report from IBM Security has been released and reveals there has been a slight reduction in global data breach costs, falling to $3.86 million per breach from $3.92 million in 2019 – A reduction of 1.5%.

There was considerable variation in data breach costs in different regions and industries. Organizations in the United States faced the highest data breach costs, with a typical breach costing $8.64 million, up 5.5% from 2019.

COVID-19 Expected to Increase Data Breach Costs

This is the 15th year that IBM Security has conducted the study. The research was conducted by the Ponemon Institute, and included data from 524 breached organizations, and 3,200 individuals were interviewed across 17 countries and regions and 17 industry sectors. Research for the report was conducted between August 2019 and April 2020.

The research was mostly conducted before the COVID-19 pandemic, which is likely to have an impact on data breach costs. To explore how COVID-19 is likely to affect the cost of a data breaches, the Ponemon Institute re-contacted study participants to ask their views. 76% of respondents believed the increase in remote working would increase the time taken to identify and contain a data breach and 70% said remote working would increase the cost of a data breach. The average cost increase due to COVID-19 was calculated to be $137,000.

Read entire article:
https://www.hipaajournal.com/ibm-security-2020-cost-of-data-breach-report-shows-10-annual-increase-in-healthcare-data-breach-costs/

NEWS

OCR Imposes $1 Million HIPAA Penalty on Lifespan for Lack of Encryption and Other HIPAA Failures

The HHS' Office for Civil Rights has imposed a $1,040,000 HIPAA penalty on Lifespan Health System Affiliated Covered Entity (Lifespan ACE) following the discovery of systemic noncompliance with the HIPAA Rules.

Lifespan is a not-for-profit health system based in Rhode Island that has many healthcare provider affiliates in the state. On April 21, 2017, a breach report was filed with OCR by Lifespan Corporation, the parent company and business associate of Lifespan ACE, about the theft of an unencrypted laptop computer on February 25, 2017.

The laptop had been left in the vehicle of an employee in a public parking lot and was broken into. A laptop was stolen that contained information such as patient names, medical record numbers, medication information, and demographic data of 20,431 patients of its healthcare provider affiliates.

Read entire article:
https://www.hipaajournal.com/ocr-1-million-hipaa-penalty-lifespan-lack-encryption/

HIPAAQuiz

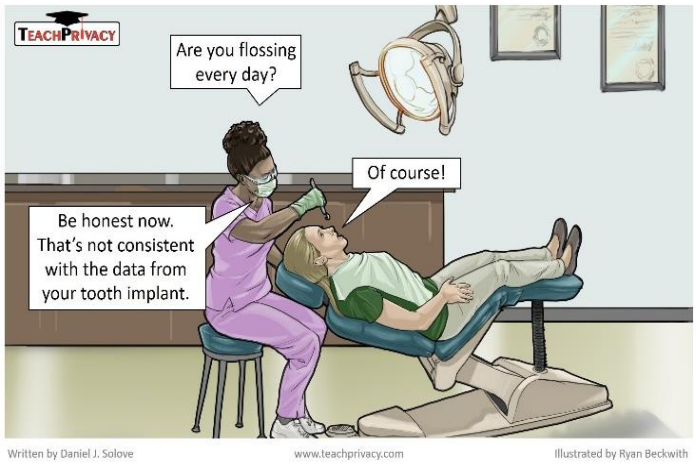
When discussing PHI try to:

a. lower your voice
b. use nongeneric terms
c. move to a more private area
d. both a and c

Answer: d

Reason: Even if your discussions of PHI are legitimate, acknowledge that others may be able to hear the conversation. When discussing patients, think to yourself, "Who else can hear?" and adjust your behavior based on the answer.

HIPAA Humor



IN OTHER COMPLIANCE NEWS

LINK 1

6,000 Patients Notified About Email Security Breach at Beaumont Health

https://www.hipaajournal.com/6000-patients-notified-about-email-security-breach-at-beaumont-health/

LINK 2

FBI Issues Flash Alert Warning of Increasing Netwalker Ransomware Attacks

https://www.hipaajournal.com/fbi-issues-flash-alert-due-to-increasing-netwalker-ransomware-attacks/

LINK 3

SURVEY: Have Emergency Preparedness Plans Changed Due to COVID-19?

https://www.hipaajournal.com/survey-have-emergency-preparedness-plans-changed-due-to-covid-19/

LINK 4

MarineXchange Confirmed as HIPAA Compliant

https://www.hipaajournal.com/marinexchange-confirmed-as-hipaa-compliant/

THUMBS UP!!!

Thumbs Up To ALL Departments For Implementing

MIDLAND HEALTH

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