OCTOBER 2019

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: *"Since it's your healthcare information, it only makes sense that you should have unlimited access to it, right? You should be able to obtain it as you please, no questions asked."*

Fact:
It's a bit more complicated than that. You absolutely have the right to request medical records, but this doesn't guarantee you getting all, if any, of your records. Some records may be deemed too harmful for you — for example, mental health records — and as such, you may be denied the access to them. Then again, there needs to be a reasonable assumption that exposing you to this information may prompt you to harm yourself.

Otherwise, as long as you follow all of the required steps, you're more than likely to get copies of your medical records. And if you don't, healthcare providers are obligated to notify you in writing.

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

HHS Proposes Rule Easing Restrictions on Substance Use Disorder Treatment Records

The Substance Abuse and Mental Health Services Administration (SAMHSA) has proposed a new rule that loosens restrictions on substance use disorder (SUD) treatment records, aligning Part 2 regulations more closely with HIPAA.

The new rule, proposed on August 22, is the first element of the HHS's Regulatory Sprint to Coordinated Care initiative, which will also see changes made to HIPAA, the Anti-Kickback Statute, and Stark Law.

SUD treatment records are covered by Confidentiality of Substance Use Disorder Patient Records regulations – 42 CFR Part 2 (Part 2). Part 2 pre-dates HIPAA by two decades and was introduced at a time when there were no broader privacy and security standards for health data. Part 2 regulations were required to protect the privacy of patients by severely restricting the allowable uses and disclosures of SUD treatment records. When Part 2 was introduced, there was a stigma associated with SUD and without privacy protections, many individuals suffering from the disorder may have avoided seeking treatment.

Since 1975, further privacy and security laws have been introduced. The HIPAA Security Rule requires all HIPAA-covered entities to implement safeguards to ensure the confidentiality, integrity, and availability of electronic protected health information (ePHI) and the HIPAA Privacy Rule restricts uses and disclosures of that information. However, Part 2 requires additional protections for SUD records than those for PHI and ePHI.

It is important to protect the privacy of patients and ensure that SUD information is safeguarded against unauthorized access as the information could be misused, but it is also essential for SUD treatment information to be made available to healthcare providers to better support care coordination. The proposed rule does not change the privacy framework of Part 2, it just eases restrictions on SUD treatment records and removes some of the complexity of Part 2 regulations. While there is closer alignment with HIPAA, the proposed changes fall short of full harmonization with HIPAA Rules.

Read entire article:
https://www.hipaajournal.com/hhs-proposes-rule-easing-restrictions-on-substance-use-disorder-treatment-records/

DID YOU KNOW...

The settlements pursued by the Department of Health and Human Services' Office for Civil Rights (OCR) are for egregious violations of HIPAA Rules. Settlements are also pursued to highlight common HIPAA violations to raise awareness of the need to comply with specific aspects of HIPAA Rules.

MIDLAND HEALTH

NEWS

82% of Healthcare Organizations Have Experienced a Cyberattack on Their IoT Devices

82% of healthcare providers that have implemented Internet-of-Things (IoT) devices have experienced a cyberattack on at least one of those devices over the course of the past 12 months, according to the Global Connected Industries Cybersecurity Survey from Swedish software company Irdeto. For the report, Irdeto surveyed 700 security leaders from healthcare organizations and firms in the transportation, manufacturing, and IT industries in the United States, United Kingdom, Germany, China, and Japan. Attacks on IoT devices were common across all those industry sectors, but healthcare organizations experienced the most cyberattacks out of all industries under study. The biggest threat from these IoT cyberattacks is theft of patient data. The attacks also have potential to compromise end user safety, result in the loss of intellectual property, operational downtime and damage to the organization's reputation. The failure to effectively secure the devices could also potentially result in a regulatory fine. When asked about the consequences of a cyberattack on IoT devices, the biggest concern was theft of patient data, which was rated as the main threat by 39% of healthcare respondents. Attacks on IoT devices can also threaten patient safety. 20% of respondents considered patient safety a major risk and 30% of healthcare providers that experienced an IoT cyberattack said patient safety was actually put at risk as a direct result of the attack. 12% of respondents said theft of intellectual property was a major risk, and healthcare security professionals were also concerned about downtime and damage to their organization's reputation.

Read entire article:
https://www.hipaajournal.com/82-of-healthcare-organizations-have-experienced-a-cyberattack-on-their-iot-devices/

10 Common HIPAA Violations

1. Employees disclosing information *(Employees gossiping about patients to friends or coworkers.)*
2. Medical records mishandling *(A physician or nurse may accidentally leave a chart in the patient's exam room available for another patient to see.)*
3. Lost or Stolen Devices *(Mobile devices are the most vulnerable to theft because of their size.)*
4. Texting patient information *(There are new encryption programs that allow confidential information to be safely texted, but both parties must have it installed on their wireless device.)*
5. Social Media *(Posting patient photos on social media is a HIPAA violation.)*
6. Employees illegally accessing patient files *(Whether it is out of curiosity, spite, or as a favor for a relative or friend, this is illegal and can cost a practice substantially.*
7. Social breaches *(It is best to have an appropriate response planned well in advance to reduce the potential of accidentally releasing private patient information*
8. Authorization Requirements *(If an employee is not sure, it is always best to get prior authorization before releasing any information.)*
9. Accessing patient information on home computers *(Keep all mobile devices out of sight to reduce the risk of patient information being accessed or stolen.)*
10. Lack of training *(Compliance training is one of the most proactive and easiest ways to avoid a violation.)*

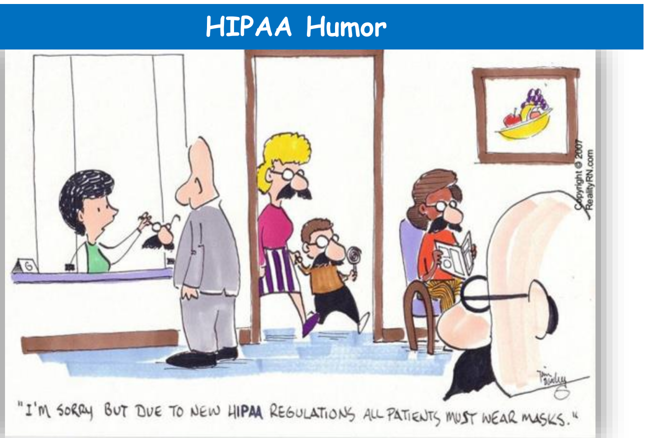
Resource:
https://www.beckershospitalreview.com/healthcare-information-technology/10-common-hipaa-violations-and-preventative-measures-to-keep-your-practice-in-compliance.html

HIPAAQuiz

Isn't consent the same as *"patient authorization?"*

Answer: *No. Patient authorization is at odds with patient consent in that it is required by the Privacy Rule for uses and disclosures of PHI not otherwise allowed by the rule. Where the Privacy Rule requires patient authorization, voluntary consent is not sufficient to permit a use of disclosure of PHI unless it also satisfies the requirements of a valid authorization. An authorization is usually a detailed document that gives the Covered Entity permission to use PHI for specific purposes which typically are other than those sanctioned by the TPO standard or to disclose PHI to a third party specified by the patient. A proper authorization specifies a number of elements, including a description of the PHI to be used and discussed, the person authorized to make the use or disclosure, the person to whom the Covered Entity may make the disclosure, an expiration date, and – in some cases – the purpose for which the PHI may be used or disclosed. With some limited exceptions, Covered Entities may not condition patient treatment or coverage upon providing an authorization.*

HIPAA Humor



"I'M SORRY BUT DUE TO NEW HIPAA REGULATIONS ALL PATIENTS MUST WEAR MASKS."

IN OTHER COMPLIANCE NEWS

LINK 1

Georgia Court of Appeals to Decide Whether Athens Orthopedic Data Breach Victims Are Entitled to Damages

https://www.hipaajournal.com/georgia-court-of-appeals-to-decide-whether-athens-orthopedic-data-breach-victims-are-entitled-to-damages/

LINK 2

73 Email Accounts Compromised in Major Phishing Attack on NCH Healthcare System

https://www.hipaajournal.com/73-email-accounts-compromised-in-major-phishing-attack-on-nch-healthcare-system/

LINK 3

Ransomware Attack Impacts More Than 400 U.S. Dental Practices

https://www.hipaajournal.com/ransomware-attack-impacts-more-than-400-u-s-dental-practices/

LINK 4

33,370 Mount Sinai Hospital Patients Impacted by AMCA Breach

https://www.hipaajournal.com/33370-mount-sinai-hospital-patients-impacted-by-amca-breach/

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***

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