OCTOBER 2020

MIDLAND HEALTH
Compliance Hotline
877•780•9367

COMPLIANCE CONNECTION

This newsletter is prepared by the Midland Health Compliance Department and is intended to provide relevant HIPAA privacy issues and hot topics.

IN THIS ISSUE

HIPAA Privacy Rule: **Myths & Facts**

Myth: ***HIPAA Does Not Apply to Our Specific Healthcare Provider***

"HIPAA-Schmipaa, who cares! It's just another pointless set of regulations that doesn't concern our healthcare facility. It's a waste of money, is what it is."

Fact: HIPAA applies to any and all healthcare providers who transmit, store or handle protected health information.

HIPAA regulations apply to healthcare facilities of all sizes and purposes. Protected health information (PHI) *(which includes a patient's name, social security number, address, etc.)* is subject to the HIPAA privacy rule. As long as you handle PHI, you need to comply with HIPAA.

This also means any of your subcontractors who can also access your patient data. Any entity this data goes through *(e.g. a cloud database provider)* needs to be HIPAA-compliant as well. Otherwise, in case of a breach into a non-HIPAA-compliant database, expect to lose patients —and that's to say nothing about litigation costs.

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

Researchers Raise Concerns About Patient Safety and Privacy with COVID-19 Home Monitoring Technologies

A team of researchers at Harvard University has investigated COVID-19 home monitoring technologies, which have been developed to decrease interpersonal contacts and reduce the risk of exposure to the 2019 Novel Coronavirus, SARS-CoV-2.

A range of technologies have been developed to reduce the risk of exposure to SARS-CoV-2 and diagnose symptoms quickly to allow interventions that improve patient safety and limit the spread of COVID-19. The researchers define a home monitoring technology as "a product that is used for monitoring without (direct) supervision by a healthcare professional, such as in a patient's home, and that collects health-related data from a person." These technologies are being used to monitor patients in their homes for signs of COVID-19 and include smartwatches and mobile apps that connect to wireless networks and transmit health data. Algorithms are then applied to the data obtained by those technologies.

The study, recently published in Nature Medicine, raises several concerns about these home monitoring tools as they were found to increase the risks to patient safety and privacy. The technologies collect and transmit sensitive health data and, as such, they need to have appropriate security protections in place to ensure that information remains private and confidential. Many of these home monitoring tools were developed quickly to keep up with demand and to help limit the spread of COVID-19, and that has introduced risks that have not fully been addressed.

Their research confirmed that interventions were required to ensure patient safety and to comply with regulatory requirements, privacy laws, and Emergency Use Authorizations (EUAs). While there are privacy laws in the United States, they only somewhat address the privacy concerns with these platforms. There is a blind spot that could allow health data to be collected by a company and for that information to be freely shared with other companies. While there are valid reasons why information may need to be shared, for contact tracing for example, there are other potential uses that are a cause for concern, such as commercializing data gathered from patients.

Read entire article:
https://www.hipaajournal.com/harvard-researchers-raise-concerns-about-patient-safety-and-privacy-with-covid-19-home-monitoring-technologies/

DID YOU KNOW...

How are HIPAA Violations Discovered?

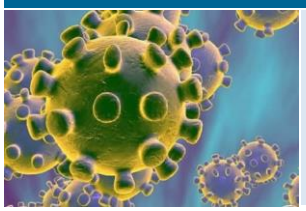
There are three main ways that HIPAA violations are discovered: (1) Investigations into a data breach by OCR or state attorneys general; (2) Investigations into complaints about covered entities and business associates; (3) HIPAA compliance audits.

Even when a data breach does not involve a HIPAA violation, or a complaint proves to be unfounded, OCR may uncover unrelated HIPAA violations that could warrant a financial penalty.

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

MIDLAND HEALTH

NEWS



Sharing PHI About COVID-19 Patients with First Responders

OCR has confirmed that HIPAA Rules permit the sharing of PHI with first responders such as law enforcement, paramedics, public safety agencies, and others under certain circumstances, without first obtaining a HIPAA authorization from a patient.

OCR confirmed that the HIPAA Privacy Rule permits disclosures of PHI for the provision of treatment (e.g. by a skilled nursing facility to medical transport personnel), when required to do so by law (such as to comply with state infectious disease reporting requirements), and to prevent or control disease, injury, or disability. That includes disclosures for public health surveillance, and to public health authorities to help prevent or control the spread of disease.

PHI can also be disclosed to first responders who may be at risk of infection and to help prevent or lessen a serious and imminent threat to the health and safety of a person or the public. OCR explained that it is permissible to "disclose PHI about individuals who have tested positive for COVID-19 to fire department personnel, child welfare workers, mental health crisis services personnel, or others charged with protecting the health or safety of the public if the covered entity believes in good faith that the disclosure of the information is necessary to prevent or minimize the threat of imminent exposure to such personnel in the discharge of their duties."

HIPAA also permits disclosures of PHI when responding to a request for PHI by a correctional institution or law enforcement official, that has lawful custody of an inmate or other individual. The disclosures are permitted when PHI is needed to provide healthcare to an individual, to ensure the health and safety of staff and other inmates, to law enforcement on the premises, and to help maintain safety, security, and good order in a correctional institution.

The minimum necessary standard applies in all cases and disclosures of PHI should be restricted to the minimum necessary amount to achieve the objective for which the information is disclosed.

Read entire article: https://www.hipaajournal.com/hipaa-compliance-checklist/

HIPAAQuiz

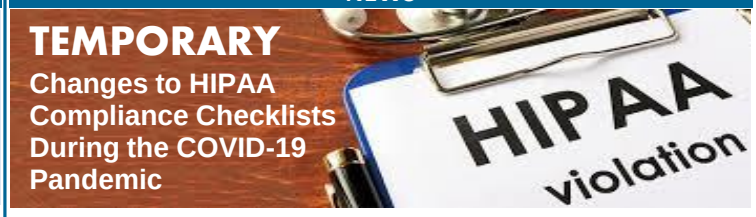
The most secure passwords are:

a. *names of sport teams*
b. *personal names or fictional characters*
c. *combinations of upper- and lowercase letters and numbers that are at least six characters long*
d. *dates of birth*

Answer: c

Reason: Using at least a six-character password of upper- and lowercase letters and numbers is more secure than using names or dates of birth. Consider using a word or subject that interests you and converting it into a character sequence meaningless to everyone but you.

NEWS



Healthcare organizations are having to deal with a nationwide public health crisis, the likes of which has never been seen. The 2019 Novel Coronavirus (SARS-CoV-2) that causes COVID-19 is forcing healthcare organizations to change normal operating procedures and workflows, reconfigure hospitals to properly segregate patients, open testing centers outside of their usual facilities, work with a host of new providers and vendors, and rapidly expand telehealth services and remote care.

This colossal extra burden makes HIPAA compliance even more difficult, yet even during public health emergencies such as the COVID-19 pandemic, health plans, healthcare providers, healthcare clearinghouses, and business associates and their subcontractors must still comply with the HIPAA Privacy, Security, Breach Notification, and Omnibus Rules.

HIPAA Rules have provisions covering healthcare operations during emergencies such as natural disasters and disease pandemics; however, the current COVID-19 nationwide public health emergency has called for the temporary introduction of unprecedented flexibilities with regards to HIPAA compliance.

The HHS' Office for Civil Rights appreciates that during such difficult times, HIPAA compliance becomes even more of a strain. In order to ensure the flow of essential healthcare information is not impeded by HIPAA regulations, and to help healthcare providers deliver high quality care, OCR has announced that penalties and sanctions for noncompliance with certain provisions of HIPAA Rules will not be imposed on healthcare providers and their business associates for good faith provision of healthcare services during the COVID-19 public health emergency.

Read entire article: https://www.hipaajournal.com/hipaa-compliance-checklist/

HIPAA Humor

Written by Daniel J. Solove www.teachprivacy.com Illustrated by Ryan Beckwith

IN OTHER COMPLIANCE NEWS

LINK 1

OCR Issues Guidance on Media and Film Crew Access to Healthcare Facilities

https://www.hipaajournal.com/ocr-issues-guidance-on-media-and-film-crew-access-to-healthcare-facilities/

LINK 2

Ashley County Medical Center Nurse Terminated for Improper Medical Record Access

https://www.hipaajournal.com/ashley-county-medical-center-nurse-terminated-for-improper-medical-record-access/

LINK 3

PHI Exposed in Phishing Attacks on FHN and Elkins Rehabilitation & Care Center

https://www.hipaajournal.com/phi-exposed-in-phishing-attacks-on-fhn-and-elkins-rehabilitation-care-center/

LINK 4

PHI of Customers Stolen in Looting Incidents at Cub Pharmacies

https://www.hipaajournal.com/phi-of-customers-stolen-in-looting-incidents-at-cub-pharmacies/

THUMBS UP to all MH Departments

for implementing awareness of...

MIDLAND HEALTH

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