FEBRUARY 2021

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 prohibits the use of sign-in sheets."

Fact

Your practice can use sign-in sheets as long as the information collected is appropriately limited.
For example, sign-in sheets can include the patient name, check-in time, and provider name if necessary but should omit medical information such as the reason for the visit.
This reduces incidental disclosure of patients' health information to others.

Resource:
https://www.aafp.org/journals/fpm/blogs/inpractice/entry/hipaa_myths.html

U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES
OFFICE FOR CIVIL RIGHTS

OCR Issues Guidance on Disclosures of PHI to Health Information Exchanges under HIPAA

The Department of Health and Human Services' Office for Civil Rights has published new guidance on the Health Insurance Portability and Accountability Act (HIPAA) Rules covering disclosures of protected health information (PHI) to health information exchanges (HIEs) for the public health activities of a public health authority (PHA).

An HIE is an organization that enables the sharing of electronic PHI (ePHI) between more than two unaffiliated entities such as healthcare providers, health plans, and their business associates. HIEs' share ePHI for treatment, payment, or healthcare operations, for public health reporting to PHAs, and for providing other functions and services such as patient record location and data aggregation and analysis.

HIPAA supports the use of HIEs and the sharing of health data to improve public health, which has been especially important during the COVID-19 public health emergency. The HIPAA Privacy Rule permits HIPAA-covered entities and their business associates to disclose protected health information to an HIE for reporting to a PHA that is engaged in public health, without requiring prior individual authorization.

Such disclosures are permitted under the following circumstances:

- *When disclosures are required by federal, state, local, or other laws that are enforceable in court*
- *When the HIE is acting under a grant of authority or contract with a PHA for a public health activity*
- *When the HIE is a business associate of the covered entity or another business associate, and wishes to provide ePHI to a PHA for public health purposes**

**The HIPAA Privacy Rule only permits an HIE which is a business associate of the covered entity or another business associate to disclose ePHI to a PHA for public health purposes if it is expressly stated that they can do so in the business associate agreement (BAA) with the covered entity. However, earlier this year in response to the COVID-19 public health emergency, OCR issued a notice of enforcement discretion stating no action will be taken against a business associate for good faith disclosures of ePHI to a PHA for public health purposes if they are not expressly permitted to disclose ePHI to a PHA in their BAA. In such cases, the business associate must inform the covered entity within 10 calendar days of the disclosure. The notice of enforcement discretion is only valid for the duration of the COVID-19 public health emergency. When the Secretary of the HHS declares the COVID-19 public health emergency over, such disclosures will no longer be permitted unless expressly permitted in the BAA.*

Read entire article:
https://www.hipaajournal.com/ocr-issues-guidance-on-disclosures-of-phi-to-health-information-exchanges-under-hipaa/

DID YOU KNOW...

HIPAA Mandates Physical Controls

Apart from technical safeguards that restrict access of electronic personal health information, audit stipulations, and disaster recovery protocols, HIPAA mandates having in place physical safeguards, which encompasses restricted access to the facility, controls on removing, transferring, disposing or re-using electronic media, and more.

Resource:
https://lifelinedatacenters.com/colocation/five-things-probably-know-hippa-compliance/

MIDLAND HEALTH

NEWS

OCR HIPAA Audits Industry Report Identifies Common Areas of Noncompliance with the HIPAA Rules

The Department of Health and Human Services' Office for Civil Rights has published its 2016-2017 HIPAA Audits Industry Report, highlighting areas where HIPAA-covered entities and their business associates are complying or failing to comply with the requirements of the Health Insurance Portability and Accountability Act.

The Health Information Technology for Economic and Clinical Health (HITECH) Act requires the HHS to conduct periodic audits of HIPAA covered entities and business associates to assess compliance with the HIPAA Rules. Between 2016 and 2017, the HHS conducted its second phase of compliance audits on 166 covered entities and 41 business associates to assess compliance with certain provisions of the HIPAA Privacy, Security, and Breach Notification Rules.

The 2016/2017 HIPAA compliance audits were conducted on a geographically representative, broad cross-section of covered entities and business associates and consisted of desk audits – remote reviews of HIPAA documentation – rather than on-site audits. All entities have since been notified of the findings of their individual audits.

The 2016-2017 HIPAA Audits Industry Report details the overall findings of the audits, including key aspects of HIPAA compliance that are proving problematic for covered entities and business associates.

In the report, OCR gives each audited entity a rating based on their level of compliance with each specific provision of the HIPAA Rules under assessment. A rating of 1 indicates the covered entity or business associate was fully compliant with the goals and objectives of the selected standards and implementation specifications. A rating of 2 means the entity substantially met the criteria and maintained adequate policies and procedures and could supply documentation or other evidence of compliance.

Read entire article:
https://www.hipaajournal.com/ocr-hipaa-audits-industry-report/

HIPAAQuiz

What should you tell an individual who asks for information about HIPAA or his or her privacy rights?

a. *Explain the organization's HIPAA privacy policies.*
b. *Give copies of the organization's notice of privacy practices and tell the individual to direct further questions to the privacy officer.*
c. *Ask whether the individual is a current patient. For current patients only, supply a copy of the notice of privacy practices.*
d. *None of the above.*

Answer: b

HIPAA's privacy rule requires healthcare organizations to provide patients with a notice explaining their rights and how the provider may use their PHI. Anyone—even people who are not currently patients—may receive a copy of this notice.

NEWS

NIST National Institute of Standards and Technology U.S. Department of Commerce
NCCoE NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

NIST Releases Final Guidance on Securing the Picture Archiving and Communication System (PACS) Ecosystem

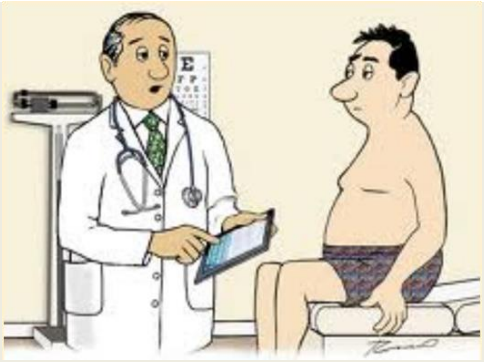
The National Cybersecurity Center of Excellence (NCCoE) at the National Institute of Standards and Technology (NIST) has released final guidance for healthcare delivery organizations on securing the Picture Archiving and Communication System (PACS) ecosystem.

PACS is a medical imaging technology that is used to securely store and digitally transmit medical images such as MRIs, CT scans, and X-rays and associated clinical reports and is ubiquitous in healthcare. These systems eliminate the need to store, send, and receive medical images manually, and assist healthcare delivery organizations by allowing the images to be securely and cheaply stored offsite in the cloud. PACS allows medical images to be easily retrieved using PACS software from any location.

PACS is a system that by design cannot operate in isolation. In healthcare delivery organizations, PACS is usually integrated into highly complex environments and interfaces with many interconnected systems. The complexity of those environments means securing the PACS ecosystem can be a major challenge and it is easy for cybersecurity risks to be introduced that could easily compromise the confidentiality, integrity, and availability of the PACS ecosystem, protected health information (PHI), and any systems to which PACS connects.

Read entire article:
https://www.hipaajournal.com/nist-final-guidance-securing-the-picture-archiving-and-communication-system-pacs-ecosystem/

HIPAA Humor



"According to your HIPAA release form I can't share anything with you."

IN OTHER COMPLIANCE NEWS

LINK 1

Former GenRx Pharmacy Patients' PHI Potentially Compromised in Ransomware Attack

https://www.hipaajournal.com/former-genrx-pharmacy-patients-phi-potentially-compromised-in-ransomware-attack/

LINK 2

OCR HIPAA Audits Industry Report Identifies Common Areas of Noncompliance with the HIPAA Rules

https://www.hipaajournal.com/ocr-hipaa-audits-industry-report/

LINK 3

Xavier Becerra Named Secretary of the Department of Health and Human Services

https://www.hipaajournal.com/xavier-becerra-secretary-department-health-human-services/

LINK 4

Largest Healthcare Data Breaches in 2020

https://www.hipaajournal.com/largest-healthcare-data-breaches-in-2020/

THUMBS UP to all MH Departments for implementing awareness of...

MIDLAND HEALTH

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