
# COMPLIANCE CONNECTION: Providing Relevant Issues and Hot Topics

## IN THIS ISSUE



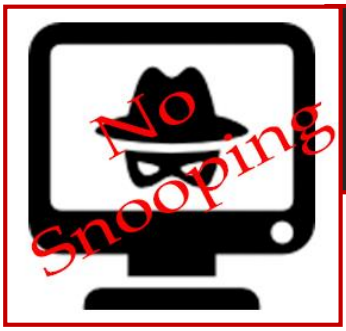

### HIPAA privacy rule: Myths & Facts

***Myth:*** *"Your Health and Medical Records Cannot Affect Your Credit Records."*

**Fact:**

Wrong! When services have been provided to you by a provider or facility, they are entitled to be paid. They are allowed to do whatever is legal under bill collecting statutes to collect that debt, including turning your files over to a collection agency. *[If you fall behind in paying your medical bills, that will be reported to credit agencies and your payment struggles will be recorded on your credit report.]* Your medical history and payment problems may also get reported to the Medical Information Bureau which services life insurance companies, among others, and ties together health and credit. Further, FICO, the organization that develops credit scores for use by lenders, began developing "medication adherence scores" in 2011. Many experts believe that eventually those scores will be put together with credit scores to draw conclusions about individual patients which will, in turn, affect their ability to access medical care or other types of health insurance (life, disability, others).

*Resource:*
*https://www.verywellhealth.com/hipaa-patients-and-medical-records-privacy-myths-2615514*




## EHR Snooping: *Best efforts to bust, punish and prevent it*

*By Jackie Drees*

Whether it's the result of sheer curiosity or motivated by an act of malice, EHR snooping is a serious employee offense that can occur at any hospital.

The Medical University of South Carolina in Charleston fired 13 employees in 2017 for viewing patient records without authorization. Earlier this year, Chicago-based Northwestern Memorial Hospital terminated approximately 50 staff members who inappropriately accessed actor Jussie Smollett's medical records. One employee told NBC Chicago she was fired on the spot.

"Simply put, it was morbid curiosity," the former employee said of viewing Mr. Smollett's health information. "I went into the charting system and started to search his name. I clicked just once. I never clicked into his chart."

Curiosity can also tempt employees to look at health records of patients they know personally, from family members to coworkers. Between 2016 and 2017, HHS reported that 1,309 records were inappropriately accessed by a single employee at a healthcare organization.

In March, a patient at Winfield, Ill.-based Northwestern Medicine Regional Medical Group sued the health system and a former employee for allegedly accessing her health records and posting them on social media. The lawsuit claimed the former employee viewed the patient's medical records before sending them to her ex-boyfriend, who posted the information on Twitter.

"In some instances, an employee believes they are helping a friend or loved one by looking at their chart and then providing guidance as to which provider to seek care from or how to assist with scheduling an appointment, " Penn Medicine CIO Michael Restuccia said. "In other situations, an employee is simply curious regarding a friend or loved one's health, reason for an appointment or perhaps changes in behavior. Regardless of the reason, without written consent, both situations represent inappropriate employee behavior."

*Read entire article:*
*https://www.beckershospitalreview.com/ehrs/ehr-snooping-best-efforts-to-bust-punish-and-prevent-it.html*

**DID YOU KNOW...**

***Scenarios that Violate HIPAA***

- *Allowing members of the media to interview a patient in a substance abuse facility.*
- *Releasing information about minors without the consent of a parent or guardian.*
- *Including private health information in an email sent over the Internet.*
- *Discussing private health information over the phone in a public area*
- *Telling friends or relatives about patients in the hospital.*

MIDLAND HEALTH

## NEWS

# UnityPoint Health Data Breach Lawsuit Partially Dismissed by Federal Judge

A class-action data breach lawsuit filed against UnityPoint Health has been partially dismissed by the US District Court for the Western District of Wisconsin.

The lawsuit stems from a phishing attack on UnityPoint Health in February 2018. As a result of employees falling for phishing emails, the attackers were able to gain access to email accounts containing the protected health information (PHI) of 16,429 patients.

The investigation into the breach showed access to patient data was first gained on November 1, 2017 and further email accounts were compromised up to February 7, 2018. The types of PHI in the compromised email accounts included names, contact information, diagnoses, medications, lab test results, and surgical information. Some patients also had their driver's license number and/or Social Security number exposed.

One month after the data breach was announced, four patients filed a lawsuit against UnityPoint Health claiming the company had mishandled the breach. The lawsuit also alleged UnityPoint Health had unnecessarily delayed the issuing of breach notification letters for two months, in violation of HIPAA Breach Notification Rule requirements.

*Read entire article:*
*https://www.hipaajournal.com/unitypoint-health-data-breach-lawsuit-partially-dismissed-by-federal-judge/*

# HIPAAQuiz

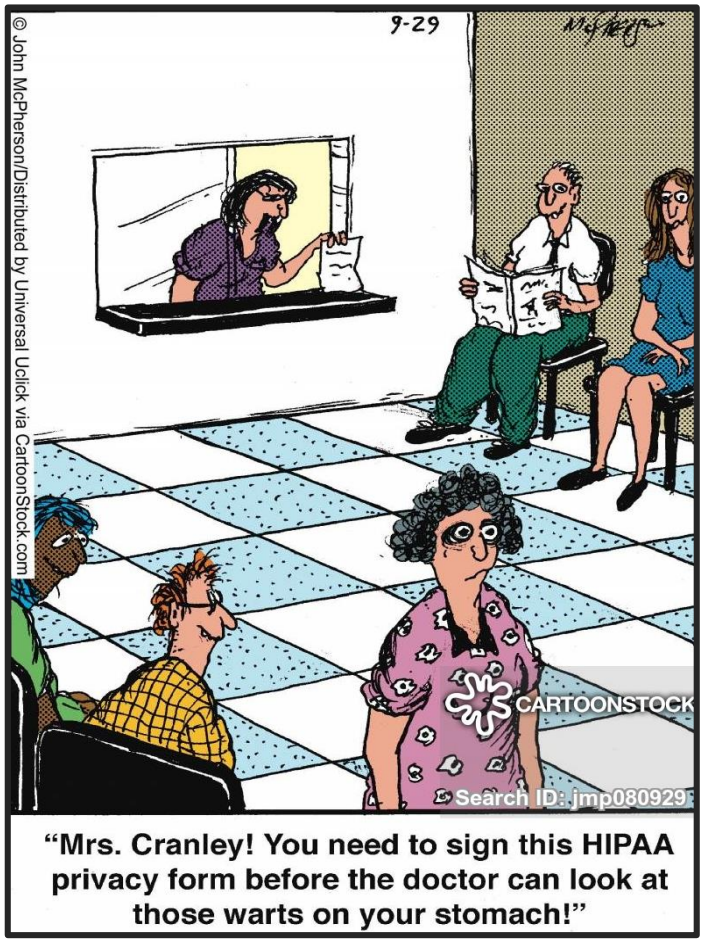
**What is Considered PHI Under HIPAA Rules?**

***Answer:*** *It is not only past and current health information that is considered PHI under HIPAA Rules, but also future information about medical conditions or physical and mental health related to the provision of care or payment for care. PHI is health information in any form, including physical records, electronic records, or spoken information. Therefore, PHI includes health records, health histories, lab test results, and medical bills. Essentially, all health information is considered PHI when it includes individual identifiers. Demographic information is also considered PHI under HIPAA Rules, as are many common identifiers such as patient names, Social Security numbers, Driver's license numbers, insurance details, and birth dates, when they are linked with health information.*


**Always**

- *use low conversational tones in clinical reception areas*
- *use encrypted email (work email) when transmitting PHI*
- *lock computer before leaving workstation*

## HIPAA Humor




"Mrs. Cranley! You need to sign this HIPAA privacy form before the doctor can look at those warts on your stomach!"

## IN OTHER COMPLIANCE NEWS

**LINK 1**

**Coffey Health System Agrees to $250,000 Settlement to Resolve Alleged Violations of False Claims and HITECH Acts**

https://www.hipaajournal.com/coffey-health-system-agrees-to-250000-settlement-to-resolve-alleged-violations-of-false-claims-and-hitech-acts/

**LINK 2**

**Repurposing a Text Alert System for Business as a HIPAA Compliance Helpline**

https://www.hipaajournal.com/text-alert-system-for-business/

**LINK 3**

**More than 10,000 FDNY EMS Patients Notified of PHI Exposure**

https://www.hipaajournal.com/more-than-10000-fdny-ems-patients-notified-of-phi-exposure/

**LINK 4**

**Allscripts Proposes $145 Million Settlement to Resolve DOJ HIPAA and HITECH Act Case**

https://www.hipaajournal.com/allscripts-proposes-145-million-settlement-to-resolve-doj-hipaa-and-hitech-act-case/

## THUMBS UP!!!

***Thumbs Up To ALL Departments For Implementing***


MIDLAND HEALTH

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