
# COMPLIANCE CONNECTION: Providing Relevant Issues and Hot Topics

## IN THIS ISSUE




### HIPAA privacy rule: Myths & Facts

***Myth:*** *"Providers are not allowed to share information about patients with others."*

**Fact:** Providers may share information with family or friends if they are involved in the patient's treatment, or payment for healthcare, or if the patient tells the provider they may share healthcare information with a particular individual. The only exception to this is if the patient specifically objects to the provider sharing the information. If a patient is incapacitated, providers may use their professional judgment to decide to share healthcare information. *(For example, if it's in the patient's best interest, or if providers have good reason to believe the patient would not object to the sharing of their healthcare information.)* Providers may divulge health information to family or friends who are caregivers or with a family member who pays the medical bill. Providers may also give health information to clergy, unless the patient objects. The HIPAA Privacy Rule does not require providers to share information with family and friends, unless certain individuals have been designated as a patient's personal representative. For example, if a patient has a healthcare power of attorney, that person is considered a "personal representative" *(state law may differ)*. In most states, with some exceptions, parents are considered their children's personal representatives. In the case of divorced parents, the parent or parents who are authorized to make healthcare decisions in the divorce decree are considered the personal representative.

*Resource:*
*https://www.todayswoundclinic.com/blog/hipaa-privacy-security-compliance-dispelling-common-myths*

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

## OCR Fines Florida Contractor Physicians' Group $500,000 for Multiple HIPAA Compliance Failures

An HHS Office for Civil Rights (OCR) investigation into an impermissible disclosure of PHI by a business associate of a HIPAA-covered entity revealed serious HIPAA compliance failures.

Advanced Care Hospitalists (ACH) is a Lakeland, FL-based contractor physicians' group that provides internal medicine physicians to nursing homes and hospitals in West Florida. ACH falls under the definition of a HIPAA-covered entity and is required to comply with the HIPAA Privacy, Security, and Breach Notification Rules. ACH serves approximately 20,000 patients a year and employed between 39 and 46 staff members per year during the time frame under investigation.

Between November 2011 and June 2012, ACH engaged the services of an individual who claimed to be a representative of Doctor's First Choice Billings Inc., a Florida-based provider of medical billing services. That individual used First Choice's company name and website, but according to the owner of First Choice, those services were provided without the knowledge or permission of First Choice.

A local hospital notified ACH on February 11, 2014 that some patient information – including names, birth dates, Social Security numbers, and some clinical information – was viewable on the First Choice website. The website was shut down the following day.

In April 2014, ACH submitted a breach report to OCR about the impermissible disclosure of patients' protected health information (PHI). Its breach report stated the PHI of 400 patients had been impermissibly disclosed, but later amended the breach report after it was discovered a further 8,855 patients' PHI had also been impermissibly disclosed.

OCR investigated the breach and discovered that despite having been in operation since 2005, ACH did not implement any HIPAA Privacy, Security, and Breach Notification Rule policies and procedures before April 1, 2014, and had failed to implement appropriate security measures. ACH also failed to conduct a risk analysis until March 4, 2014.

*Read entire article:*
*https://www.hipaajournal.com/ocr-fines-florida-contractor-physicians-group-500000-for-multiple-hipaa-compliance-failures/*

DID YOU KNOW...

***The Largest HIPAA Breach Affected Nearly 5 Million People***

*Tricare Management, a health benefits service provider for military personnel, veterans, and their families, experienced the largest recorded HIPAA breach, which affected an estimated 4.9 million patients. This monumental security breach was reported by Science Applications International (SAI) on September 14, 2011 and involved thousands of tapes containing patients' healthcare records.*

MIDLAND HEALTH

## NEWS

# DHS/FBI Issue Fresh Alert About SamSam Ransomware

In late November, the Department of Justice indicted two Iranians over the use of SamSam ransomware, but there is unlikely to be any let up in attacks.

Due to the high risk of continued SamSam ransomware attacks in the United States, the Department of Homeland Security (DHS) and FBI have issued a fresh alert to critical infrastructure organizations about SamSam ransomware.

To date, there have been more than 200 SamSam ransomware attacks, most of which have been on organizations and businesses in the United States. The threat actors behind SamSam ransomware have received approximately $6 million in ransom payments and the attacks have resulted in more than $30 million in financial losses from computer system downtime.

The main methods of attack have been the use of the JexBoss Exploit Kit on vulnerable systems, and more recently, the use of Remote Desktop Protocol (RDP) to gain persistent access to systems. Access through RDP is achieved through the purchase of stolen credentials or brute force attacks.

Once access is gained, privileges are escalated to gain administrator rights. The threat actors then explore the network and deploy and execute the ransomware on as many devices as possible to maximize the disruption caused. A ransom demand is then placed on the desktop. Ransoms of between $5,000 and $50,000 are usually demanded, depending on the extent of encryption.

The FBI has analyzed the systems of many SamSam ransomware victims and has determined in many cases there has been previous unauthorized network activity unrelated to the SamSam ransomware attacks. This suggests the SamSam ransomware threat actors have purchased stolen credentials that have previously been used by other threat actors.

*Read entire article:*
https://www.hipaajournal.com/dhs-fbi-issue-fresh-alert-about-samsam-ransomware/

# HIPAAQuiz

**A parent arrives in the emergency room demanding to know what is happening to his or her child. Can you answer?**

*Answer: According the Privacy Rule, PHI can generally be shared with the child's parents if they are the child's personal representatives. Follow your organization's rules for disclosing this information. For example, you may need to refer the parents to another healthcare provider.*

# AMIA and AHIMA Call For Changes to HIPAA to Improve Access and Portability of Health Data

The American Medical Informatics Association (AMIA) and the American Health Information Management Association (AHIMA) have called for changes to HIPAA to be made to improve patients' access to their health information, make health data more portable, and to better protect health data in the app ecosystem.

At a Wednesday, December 5, 2018, Capitol Hill briefing session, titled "Unlocking Patient Data – Pulling the Linchpin of Data Exchange and Patient Empowerment," leaders from AMIA and AHIMA joined other industry experts in a discussion about the impact federal policies are having on the ability of patients to access and use their health information.

Currently, consumers have access to their personal information and integrate and use that information to book travel, find out about prices of products and services from different providers, and conduct reviews and comparisons. However, while many industries have improved access to consumer information, the healthcare industry is behind the times and has so far failed to implement a comparable, patient-centric system.

"Congress has long prioritized patients' right to access their data as a key lever to improve care, enable research, and empower patients to live healthy lifestyles," said AMIA President and CEO Douglas B. Fridsma. "But enacting these policies into regulations and translating these regulations to practice has proven more difficult than Congress imagined."

AHIMA CEO Wylecia Wiggs Harris said, "AHIMA's members are most aware of patient challenges in accessing their data as they operationalize the process for access across the healthcare landscape… the language in HIPAA complicates these efforts in an electronic world."

The P in HIPAA does stand for portability, yet patients are still struggling to obtain their health data in a usable form that allows them to share that information with other entities. Health data should be portable, as is the case with other types of consumer information. Changes to HIPAA legislation will help the healthcare sector catch up with other industries.

*Read entire article:*
*https://www.hipaajournal.com/amia-and-ahima-call-for-changes-to-hipaa-to-improve-access-and-portability-of-health-data/*

## IN OTHER COMPLIANCE NEWS

**LINK 1**

**University of Maryland Medical System Discovers 250-Device Malware Attack**

https://www.hipaajournal.com/university-of-maryland-medical-system-discovers-250-device-malware-attack/

**LINK 2**

**EmblemHealth Pays $100,000 HIPAA Violation Penalty to New Jersey for 2016 Data Breach**

https://www.hipaajournal.com/emblemhealth-pays-100000-hipaa-violation-penalty-to-new-jersey-for-2016-data-breach/

## THUMBS UP!!!

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


MIDLAND HEALTH

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

## *A closer look at Protected Health Information (PHI)….*

*Remember, PHI is any health information an organization has or gets from another organization that could be used to identify a specific individual.*

*If PHI is used publicly, make sure you don't use more than necessary.*
***For example, if you:***

- *call out a person's name in a **pharmacy**, don't say what medication the person is picking up.*

*If PHI is used publicly, make sure you don't use more than necessary.*
***For example, if you:***

- *call out a patient's name in a **waiting room**, don't reveal any other information about the patient's condition or reason for their visit.*

*If PHI is used publicly, make sure you don't use more than necessary.*
***For example, if you:***

- *ask patients to use a sign-in sheet, ask only for their name, not the reason for their visit.*

***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**