

MAY 2019



# COMPLIANCE CONNECTION

COMPLIANCE HOTLINE  
877-780-9367

## COMPLIANCE CONNECTION: Providing Relevant Issues and Hot Topics

### IN THIS ISSUE

#### FEATURE ARTICLE

Health Apps Share User Data but Lack Transparency About the Practice

#### HIPAA Quiz

(See Page 2 for Question & Answer)

#### DID YOU KNOW...



#### HIPAA privacy rule: Myths & Facts

**Myth:** "As long as medical records are on good old paper, there is no need to comply with HIPAA privacy regulations that apply to electronically stored and transmitted electronic."

**Fact:** HIPAA covers all patient records, regardless of their nature. Paper sign-in records and medical records do not make your healthcare facility exempt from adhering to the HIPAA Privacy Rule.

HIPAA privacy requirements cover not only electronic health information. As long as the information can be stored, handled, transmitted, breached or stolen, it needs to be protected by HIPAA. So even if you only have paper patient records, you must be compliant with the HIPAA Privacy Rule.

Also, it's the 21st century. Paper medical records are so last millennium.

Resource:

<https://www.qminder.com/hipaa-myths-debunked/>



### Health Apps Share User Data but Lack Transparency About the Practice

Mobile health apps are commonly used to track health metrics and promote healthier lifestyles, and as such, they record a range of sensitive health information. What consumers may be unaware of is how that data is used and with whom the information is shared.

Information entered into an app is commonly shared with multiple third parties and the data is often monetized, but consumers are left in the dark about the practice.

A study of data sharing practices by medicines-related apps, published in the BMJ, revealed that out of 24 apps that were studied, 19 (79%) shared user data with third parties.

The types of apps that were assessed pertained to dispensing, administration, prescribing or use of medicines. Each app was subjected to simulated real world use with four dummy scripts.

The researchers found user data was shared with 55 different entities, from 46 parent companies, which either received or processed the data. Those entities included app developers, parent companies, and third-party service providers. 67% of the third parties provided services related to the collection or analysis of data, including analytics and advertising, and 33% provided infrastructure related services.

71% of apps transmitted user data outside of the app, including information such as the name of the device, the operating system, email address, and browsing behavior. Some of the apps transmitted sensitive information such as the user's drug list and location.

While some of the data that was shared was not particularly sensitive, such as the Android ID or device name, the information could be aggregated with other information that could allow a user to be identified. Several companies within the network had the ability to aggregate and re-identify user data.

Read entire article:

<https://www.hipajournal.com/health-apps-share-user-data-but-lack-transparency-about-the-practice/>

#### DID YOU KNOW...



#### What are Some Important Facts About the History of HIPAA?

- Aug. 21, 1996 – Former U.S. President Bill Clinton signed HIPAA.
- Feb. 16, 2006 – The HIPAA Enforcement rule signed.
- Dec. 28, 2000 – HIPAA Privacy Rule was signed and compliance began Apr. 14, 2003 but enforcement began on Apr. 21, 2006.
- Feb. 17, 2009 – HITECH (Health Information Technology for Economic & Clinical Health) Act was signed and took effect starting Aug. 24, 2009.
- Jan. 17, 2013 – HIPAA Omnibus Rule signed.



NEWS



### Amazon Announces 6 New HIPAA Compliant Alexa Skills

Six new HIPAA compliant Alexa skills have been launched by Amazon that allow protected health information to be transmitted without violating HIPAA Rules.

The new HIPAA compliant Alexa skills were developed by six different companies that have participated in the Amazon Alexa healthcare program.

The new skills allow patients to schedule appointments, find urgent care centers, receive updates from their care providers, access their latest blood sugar reading, and check the status of their prescriptions.

This is not the first time that Alexa skills have been developed, but a stumbling block has been the requirements of the HIPAA Privacy Rule, which limit the use of voice technology with protected health information. Now, thanks to HIPAA compliant data transfers, the voice assistant can now be used by a select group of healthcare organizations to communicate PHI without violating the HIPAA Privacy Rule. You can read more about the issues related to virtual assistants and HIPAA compliance here. Amazon has stated that it plans to work with many other developers through an invite-only program to develop new skills to use within its HIPAA-eligible environment. Amazon is offering those organizations business associate agreements to meet HIPAA requirements. The initial roll-out has been limited to six new HIPAA compliant Alexa skills as detailed below:

#### New HIPAA Compliant Alexa Skills

The purpose of the new skills is to allow patients, caregivers, and health plan members to use Amazon Alexa to manage their healthcare at home through voice commands.

Read entire article:

<https://www.hipaajournal.com/hipaa-compliant-alexa-skills/>

## HIPAAQuiz

**A billing clerk calls to verify information about a patient's treatment. Can you give this information?**

Answer: In general, you may share patient information for the purpose of treating or billing a patient.



**DO NOT** access protected health information (PHI) unless you are providing treatment or billing the patient.

### 1,600 Ohio Patients Notified of Impermissible PHI Disclosure



993 Ohioans who receive benefits from Medicaid or the Ohio Department of Job and Family Services (ODJFS) are being notified that some of their protected health information has been disclosed to unauthorized individuals as a result of a computer error.

Three separate incidents were identified. On February 16, 2019, a computer error resulted in a limited amount of protected health information (PHI) of 250 users of the Ohio Benefits Self-Service Portal to appear in another user's account. The error was identified and corrected the same day.

Two further incidents occurred on March 20, 2019. A computer error caused information entered into the Ohio Benefits portal to be saved to incorrect accounts. The computer error has been temporarily fixed and a permanent solution is being developed to prevent any recurrences. As many as 100 individuals were affected.

608 members of ODJFS, 34 recipients of Medicaid benefits, and one individual who received both types of benefits, had some of their PHI mailed to 5 different people as a result of a computer error. The computer error was corrected on March 22, 2019.

In all cases, the privacy breach was limited to names, dates of birth, case numbers, and claim numbers stored in the Ohio Benefits System. Affected individuals have been offered identity theft protection services for 12 months at no cost as a precaution.

840 University Hospitals Rainbow Babies & Children's Hospital Patients Notified of Impermissible PHI Disclosure

University Hospitals Rainbow Babies & Children's Hospital in Cleveland, OH, has discovered the PHI of 840 patients has been accidentally disclosed due to an error made by one of its employees.

Read entire article:

<https://www.hipaajournal.com/1600-ohio-patients-notified-of-impermissible-phi-disclosures/>

IN OTHER COMPLIANCE NEWS

LINK 1

Study Reveals Health Information the Least Likely Data Type to be Encrypted

<https://www.hipaajournal.com/study-reveals-health-information-the-least-likely-data-type-to-be-encrypted/>

LINK 2

Lawsuit Alleges Sharp Grossmont Hospital Secretly Recorded Patients Having Gynecology Operations

<https://www.hipaajournal.com/lawsuit-alleges-sharp-grossmont-hospital-secretly-recorded-patients-having-gynecology-operations/>

### THUMBS UP!!!

Thumbs Up To ALL Departments For Implementing

Awareness of HIPAA, PII, PHI, ePHI & Social Media



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

### Civil Penalty for Knowingly Violating HIPAA....

Resource: <https://www.hipaajournal.com/civil-penalty-for-knowingly-violating-hipaa/>

The civil penalty tier system for healthcare organizations is based on the extent to which the HIPAA covered entity was aware that HIPAA Rules were violated. The maximum civil penalty for knowingly violating HIPAA is \$50,000 per violation up to a maximum of \$1.5 million per violation category.

- Tier 1 – \$100 – \$50,000 per violation (Maximum \$1.5M per year)
- Tier 2 – \$1,000 – \$50,000 per violation (Maximum \$1.5M per year)
- Tier 3 – \$10,000 – \$50,000 per violation (Maximum \$1.5M per year)
- Tier 4 – \$50,000 per violation (Maximum \$1.5M per year)

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](mailto:Regenia.Blackmon@midlandhealth.org)

