JUNE
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

*"Calling out the patient's name is prohibited under HIPAA"*

### Fact

HIPAA permits incidental disclosures that may occur as a byproduct of an otherwise permitted disclosure. Calling out patient names in the waiting room can reveal health information, especially in a highly specialized facility. For example, simply calling your name associated with an oncology unit or a fertility clinic can reveal PHI.

*Resource:*
https://www.cloudapper.com/hipaa-myths-vs-facts/

# Montefiore Medical Center Fires Employee for Unauthorized Record Access

Montefiore Medical Center has discovered another employee has accessed patient information with no legitimate work reason for doing so.

The New York hospital announced in February 2020 that an employee had been discovered to have accessed medical records without authorization for 5 months in 2020, and another employee was found to have obtained the PHI of approximately 4,000 patients between January 2018 and July 2020.

The latest discovery involved an employee accessing the records of patients without authorization for more than a year. The breach was identified by Montefiore's FairWarning software, which monitors records for inappropriate access.

When unauthorized medical record access was discovered, the employee was suspended pending an investigation. A review of record access confirmed that the employee had accessed records with no legitimate work reason for doing so between January 2020 and February 2021.

The types of information accessed varied from patient to patient and included first and last names, medical record numbers, addresses, emails, dates of birth, and the last 4-digits of Social Security numbers. Montefiore found no evidence that financial information or clinical information was accessed.

The unauthorized record access violated Montefiore's policies and HIPAA. The employee was fired, and the matter was referred to law enforcement for possible criminal prosecution. The OCR breach portal indicates 943 individuals were affected.

Belden Facing Class Action Lawsuit Over November 2020 Data Breach

Belden, a U.S. vendor of networking equipment, is facing a class action lawsuit over a November 12, 2020 data breach in which the personal information of current and former employees was compromised. Hackers gained access to a limited number of file servers and exfiltrated employee data and information about some of its business partners.

The breach has recently been reported to the HHS's Office for Civil Rights as involving the protected health information of 6,348 individuals. Names, Social Security numbers, tax identification numbers, financial account numbers, home addresses, email addresses, dates of birth and other employment-related information were stolen. Belden announced the breach on November 24, 2020 and started notifying affected individuals on December 14, 2020.

*Read entire article:*
https://www.hipaajournal.com/montefiore-medical-center-fires-employee-for-unauthorized-record-access/

DID YOU KNOW...

**HIPAA Mandates Training**

*HIPAA stipulates that all employees involved in handling personal medical information be given training in proper security practices, and be made aware of the policies, reporting needs, data protection protocols and more.*

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

MIDLAND HEALTH

NEWS

## Wyoming Department of Health Announces GitHub Data Breach Affecting 1/4 of Wyomingites

The Wyoming Department of Health (WDH) has discovered the protected health information of 164,021 individuals has been accidentally exposed online due to an error by a member of its workforce.

On March 10, 2021, WDH discovered an employee had uploaded files containing medical test result data to private and public repositories on the software development platform GitHub. While security controls are in place to protect users' privacy, an error by the employee meant the data could potentially have been accessed by individuals unauthorized to view the information from January 8, 2021.

In total 53 files were uploaded to the platform that included COVID-19 and influenza test result data, along with one file that contained breath alcohol test results. The exposed information included patient IDs, dates of birth, addresses, dates of service, and test results. The COVID-19 test result data had been reported to WDH for Wyoming residents, although the tests themselves may have been performed anywhere in the United States between January 2020 and March 2021. The alcohol test results related to tests performed by law enforcement in Wyoming between April 19, 2012 and January 27, 2021.

"While WDH staff intended to use this software service only for code storage and maintenance rather than to maintain files containing health information, a significant and very unfortunate error was made when the test result data was also uploaded to GitHub.com," said WDH Director Michael Ceballos. "We are taking this situation very seriously and extend a sincere apology to anyone affected. We are committed to being open about the situation and to offering our help."

*Read entire article:*
*https://www.hipaajournal.com/phi-of-164000-individuals-accidentally-uploaded-to-github-by-wyoming-department-of-health-employee/*

## HIPAA**Quiz**

The privacy rule's minimum necessary standard requires providers to

a. include all treatment-related disclosures in accountings of disclosures
b. refrain from accessing PHI during emergencies
c. determine who needs what information and only provide the necessary amount and type
d. document all conversations that include PHI

*Answer: c*
*Some staff members do not need access to PHI and others may need only partial access. HIPAA's minimum necessary standard requires staff members to consider this and judge who needs access to what information. The minimum necessary standard does not apply to treatment situations.*

NEWS

## Health Aid of Ohio
### Security Incident Affects up to 141,00 Individuals

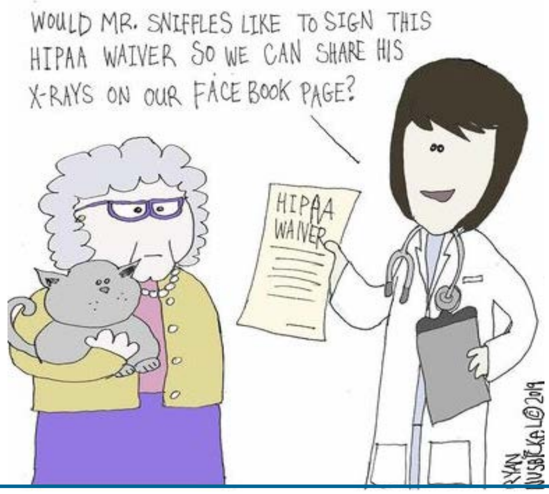
Health Aid of Ohio, a Parma, OH-based full-service home medical equipment provider, has discovered unauthorized individuals gained access to its systems and exfiltrated some files from its network. The breach was detected on February 19, 2021 when suspicious network activity was detected. Action was quickly taken to eject the attackers from the network and secure all patient data.

An investigation into the breach confirmed that files were accessed and exfiltrated from Health Aid's systems, but it was not possible to determine exactly which files had been removed from its systems. It is possible that some of the exfiltrated files contained the protected health information of VA plan members.

That information potentially included names, addresses, telephone numbers, and details of the type of equipment delivered to houses or was repaired in individuals' homes. The protected health information of individuals who received services through their insurance carrier or healthcare provider included names, telephone numbers, dates of birth, Social Security numbers, insurance information, diagnosis information, and equipment type.

*Read entire article:*
*https://www.hipaajournal.com/health-aid-of-ohio-security-incident-affects-up-to-14100-individuals/*

## HIPAA Humor


WOULD MR. SNIFFLES LIKE TO SIGN THIS HIPAA WAIVER SO WE CAN SHARE HIS X-RAYS ON OUR FACE BOOK PAGE?
HIPAA WAIVER
RYAN NUSBICKEL©2019

## IN OTHER COMPLIANCE NEWS

**LINK 1**

**COVID-19 Vaccine Cold Chain Continues to Be Targeted by Threat Groups**

https://www.hipaajournal.com/covid-19-vaccine-cold-chain-continues-to-be-targeted-by-threat-groups/

**LINK 2**

**HHS Information Blocking and Interoperability Regulations Now in Effect**

https://www.hipaajournal.com/hhs-information-blocking-and-interoperability-regulations-now-in-effect/

**LINK 3**

**Californian Healthcare Provider Discovers Patient Data was Exposed on the Internet for Over a Year**

https://www.hipaajournal.com/californian-healthcare-provider-discovers-patient-data-was-exposed-on-the-internet-for-over-a-year/

**LINK 4**

**What is the Relationship Between HITECH, HIPAA, and Electronic Health and Medical Records?**

https://www.hipaajournal.com/relationship-between-hitech-hipaa-electronic-health-medical-records/

## THUMBS UP to all MH Departments

***for implementing awareness of…***

***HIPAA, PII, PHI, ePHI, Security, and Social Media***

MIDLAND HEALTH

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

**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**