

SEPTEMBER
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

FEATURE ARTICLE

Former Scripps Health Worker Charged Over HIPAA Violation in COVID-19 Unemployment Benefit Fraud Case

HIPAA Humor (See Page 2)

HIPAA Quiz (See Page 2 for Question & Answer)

DID YOU KNOW...



Former Scripps Health Worker Charged Over HIPAA Violation in COVID-19 Unemployment Benefit Fraud Case

The Department of Justice has announced nine San Diego residents have been charged in two separate indictments in connection with the theft of patients' protected information and the submission of fraudulent pandemic unemployment insurance claims.

Under the Coronavirus Aid, Relief, and Economic Security (CARES) Act of 2020, new unemployment benefits were offered to individuals affected by the COVID-19 pandemic, who would not, under normal circumstances, qualify for payments.

In one of the cases, Matthew Lombardo, a former Scripps Health employee, was charged with felony HIPAA violations for obtaining and disclosing the protected health information of patients to his alleged co-conspirators. Lombardo was also charged with conspiracy to commit wire fraud, along with three alleged co-conspirators – Konrad Piekos, Ryan Genetti, and Dobrila Milosavljevic. Piekos, Genetti, and Milosavljevic were also charged with aggravated identity theft and are alleged to have used the stolen information to submit fraudulent pandemic unemployment insurance claims.

The San Diego Sheriff's Department had initiated a traffic stop on Konrad Piekos for driving without a license plate. When police officers approached the vehicle, they saw an assault rifle in plain sight in his vehicle. Piekos admitted possessing an unregistered assault rifle, and the subsequent vehicle search revealed several loaded firearms and ammunition. A warrant was obtained to search Piekos' properties and police officers found several other firearms and ammunition, quantities of heroin and fentanyl, and mobile phones. After obtaining warrants to search the phones, detectives identified text messages between Piekos, Genetti, and Lombardo discussing the illicit distribution of narcotics, firearms, and a scheme to obtain unemployment benefits using other persons' personal identifying information (PII).

Piekos and Genetti had conspired together to fraudulently obtain PUA benefits in July 2020, with Lombardo joining the scheme in August 2020. Lombardo is alleged to have used his position as a patient financial service representative to access patients' PII, which he then distributed to Piekos, Genetti, and Milosavljevic starting on August 15, 2020, according to the indictment. Scripps Health terminated Lombardo on April 14, 2021.

Read entire article:

<https://www.hipaajournal.com/former-scripps-health-worker-charged-over-hipaa-violation-in-covid-19-unemployment-benefit-fraud-case/>



HIPAA Privacy Rule Myths & Facts

Myth

"Healthcare providers can share PHI with employers."

Fact

Not true!

Healthcare providers cannot share PHI with employers without the patient's consent. The Privacy Rule controls how a health plan, or a covered health care provider shares your protected health information with an employer.

Resource:

<https://www.cloudapper.com/hipaa-myths-vs-facts/>

DID YOU KNOW...



Regarding HIPAA violations: Can patients sue healthcare providers?

Patients cannot sue healthcare providers for HIPAA violations as HIPAA does not create the right for a patient to sue. Although, they can file a complaint which is then investigated by authorities.

Resource: <https://www.cloudnexusit.com/2020/12/31/hipaa-fun-facts/>





30 Month Jail Term for Texas Woman Who Stole and Sold Patients' PHI

The U.S. Department of Justice has announced a Texas woman has been sentenced by a federal court in the Eastern District of Texas to serve 30 months in federal prison for conspiring to obtain protected health information from a protected computer.

Amanda Lowry, 40, of Sherman, TX, was a member of a fraud ring that used stolen protected health information to create fraudulent physician orders. The proceeds from the sale of the data were used to purchase a range of luxury items.

Lowry, along with co-conspirators Demetrius Cervantes and Lydia Henslee, were named in a federal indictment on Sept. 11, 2019. The three defendants were charged with conspiracy to obtain information from a protected computer and conspiracy to unlawfully possess and use a means of identification. Lowry pleaded guilty to the charges on December 4, 2020.

According to court documents, the defendants are alleged to have accessed a healthcare provider's electronic health record system to steal the personal and protected health information of patients. The stolen data were repackaged as false and fraudulent physician orders, which were then sold to durable medical equipment providers and contractors. The proceeds from the sale of the data were used to purchase items such as off-road vehicles, jet skis, and sport utility vehicles. The defendants were paid around \$1.4 million from the sale of the data.

Demetrius Cervantes of McKinney, TX, was sentenced to serve 48 months in jail on July 8, 2021 for his role in the fraud ring after pleading guilty to the charges. Henslee also pleaded guilty to the charges on March 25, 2021 and is awaiting sentencing. Henslee was also named in a separate indictment along with three men from Florida, who have been charged with conspiracy to commit illegal remunerations.

Read entire article:

<https://www.hipaajournal.com/30-month-jail-term-for-texas-woman-who-stole-and-sold-patients-phi/>

HIPAAQuiz

Physical security includes which of the following

- a. Locking doors and desks
- b. Keeping PHI out of view of those around you
- c. Storing computer equipment safely
- d. All of the above

Answer: d

Physical security involves common-sense steps to safeguard information from physical threats (e.g., theft). These steps include locking doors and desks, making sure that those around you cannot easily view PHI, and storing computer equipment safely and securely.

IN OTHER COMPLIANCE NEWS

LINK 1

Sierra Nevada Primary Care Physicians Alerts Patients About Theft of PHI

<https://www.hipaajournal.com/sierra-nevada-primary-care-physicians-alerts-patients-about-theft-of-phi/>

LINK 3

Ohio Personal Privacy Act Introduced to Improve Privacy Protections for Ohioans

<https://www.hipaajournal.com/ohio-personal-privacy-act-introduced-to-improve-privacy-protections-for-ohioans/>

LINK 2

Colorado Privacy Act Passed and Signed into Law

<https://www.hipaajournal.com/colorado-privacy-act/>

LINK 4

Radiology Specialists Facing Class Action Lawsuit Over PACS Data Breach

<https://www.hipaajournal.com/radiology-specialists-facing-class-action-lawsuit-over-pacs-data-breach/>



Paperwork Containing PHI of Oklahoma Heart Hospital Patients Accidentally Donated to Charity

Oklahoma Heart Hospital has started notifying certain patients about a privacy incident in which paperwork containing limited patient information was accidentally donated to charity.

A former employee had made handwritten notes which contained the protected health information of a limited number of patients during the course of that individual's employment at Oklahoma Heart Hospital between 2011 and 2014.

Some of the former employee's personal possessions were donated to charity in May 2021, with the handwritten notes accidentally included in the donated items. Oklahoma Heart Hospital was contacted by the individual who found the notes and arrangements were immediately made to collect the paperwork. The documents were then cataloged to identify the patients involved and the types of information that had been exposed.

The notes included information such as patients' names, medical record numbers, OHH visit numbers, dates of birth, ages, admit dates, genders, and clinical information consisting of diagnosis, lab results, medications and/or treatment information. No information was exposed that would have provided unauthorized individuals with access to patient record systems. While the protected health information of some patients was viewed by an individual not authorized to view the information, Oklahoma Heart Hospital has not uncovered any evidence to suggest any patient data has been further disclosed or misused; however, out of an abundance of caution, all affected individuals have been notified by mail and advised to monitor their account and explanation of benefits statements for signs of fraudulent activity.

Read entire article:

<https://www.hipaajournal.com/paperwork-containing-phi-of-oklahoma-heart-hospital-patients-accidentally-donated-to-charity/>

HIPAA Humor



"Mr. Peabody! You need to sign this HIPAA privacy form before we can look at your rash!"

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

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



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

