

COMPLIANCE CONNECTION



JULY 2023



Compliance HOTLINE:
MIDLAND HEALTH
855-662-SAFE (7233) • ID#: 6874433130
This ID# is required to submit a report.

This newsletter is prepared by the Midland Health Compliance Department and is intended to provide relevant compliance issues and hot topics.

IN THIS ISSUE

FEATURE ARTICLE

\$30,000 Penalty for Disclosing PHI Online in Response to Negative Reviews

Midland Health PolicyTech

(See entire newsletter page 2)

DID YOU KNOW...

FRAUD & ABUSE LAWS EXAMPLES

The five most important Federal Fraud and Abuse Laws that apply to physicians are:

- 1. False Claims Act (FCA):** A physician knowingly submits claims to Medicare for medical services not provided or for a higher level of medical services than actually provided.
- 2. Anti-Kickback Statute (AKS):** A provider receives cash or below-fair-market-value rent for medical office space in exchange for referrals.
- 3. Physician Self-Referral Law (Stark law):** A physician refers a beneficiary for a designated health service to a clinic where the physician has an investment interest.
- 4. Exclusion Authorities:** Several doctors and medical clinics conspire in a coordinated scheme to defraud the Medicare Program by submitting medically unnecessary claims for power wheelchairs.
- 5. Civil Monetary Penalty Law (CMPL):** Includes making false statements or misrepresentations on applications or contracts to participate in the Federal health care programs.

Resource:

<https://oig.hhs.gov/compliance/physician-education/fraud-abuse-laws/>

Midland Health Compliance Hotline
855-662-SAFE (7233)
Midland Health ID#: 6874433130
This ID# is required to submit a report.



MIDLAND HEALTH

COMPLIANCE TEAM

Michelle Pendergrass, MBA, CHC
Chief Compliance Officer/Privacy Officer
P: 432-221-1972

Michelle.Pendergrass@midlandhealth.org

Regenia Blackmon, Compliance Auditor
Regenia.Blackmon@midlandhealth.org

Melissa Bailey, Sr. Compliance Analyst
Melissa.Bailey@midlandhealth.org



U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES

Office for Civil Rights

\$30,000 Penalty for Disclosing PHI Online in Response to Negative Reviews

The Department of Health and Human Services' Office for Civil Rights (OCR) has agreed to settle a HIPAA violation case with a New Jersey provider of adult and child psychiatric services for \$30,000. In April 2020, OCR received a complaint alleging Manasa Health Center had impermissibly disclosed patient information online when responding to a negative online review. The complainant alleged Manasa Health Center's responded to a patient's review and disclosed the patient's mental health diagnosis and treatment information.

OCR launched an investigation into the Kendall Park, NJ-based healthcare provider and discovered the protected health information of a total of four patients had been impermissibly disclosed in responses to negative Google Reviews, and notified the practice about the HIPAA Privacy Rule investigation on November 18, 2020. In addition to the impermissible disclosures of PHI, which violated 45 C.F.R. § 164.502(a) of the HIPAA Privacy Rule, the practice was determined to have failed to comply with standards, implementation specifications, or other requirements of HIPAA Privacy Rule and Breach Notification Rules – 45 C.F.R. § 164.530(i).

Manasa Health Center chose to settle the case with OCR with no admission of liability or wrongdoing. In addition to the financial penalty, Manasa Health Center has agreed to adopt a corrective action plan which includes the requirement to develop, maintain, and revise its written policies and procedures to ensure compliance with the HIPAA Privacy Rule, provide training to all members of the workforce on those policies and procedures, issue breach notification letters to the individuals whose PHI was impermissibly disclosed online, and submit a breach report to OCR about those disclosures.

Read entire article:

<https://www.hipaajournal.com/30000-penalty-disclosing-phi-online-negative-reviews/>

DID YOU KNOW...



WHAT ARE THE FTC SOCIAL MEDIA RULES?

The FTC social media "rules" are the regulations relating to deceptive acts or practices in Section 5 of the Federal Trade Commission Act. The regulations apply to all forms of advertising and marketing, and define an act or practice as deceptive if: (1) a representation, omission, or practice misleads or is likely to mislead the consumer; (2) a consumer's interpretation of the representation, omission, or practice is considered reasonable under the circumstances; and (3) the misleading representation, omission, or practice is material.

Read entire article: <https://www.hipaajournal.com/hipaa-social-media/>



MIDLAND HEALTH



HIPAA Section 10.2: Technical Safeguards

POLICY

It is the policy of Midland Memorial Hospital to employ technical safeguards to maintain the privacy of PHI in compliance with the standards, implementation guidelines or other requirements of the HIPAA Privacy and Security Rules. The Privacy Officer and the Information Security Officer shall determine which Midland Memorial Hospital workforce members shall be required to be familiar with this policy and who shall follow these procedures.

PROCEDURE

Access Control. Midland Memorial Hospital implements technical policies and procedures for electronic information systems that maintain PHI to allow access only to those persons or software programs that have been granted access pursuant to the "Information Access Management" procedures set forth in the Administrative Safeguards Policy.

- a. Unique User Identification. (Required by the Security Rules.) Midland Memorial Hospital assigns a unique name and/or number for identifying and tracking user identity.
- b. Emergency Access Procedure. (Required by the Security Rules.) Midland Memorial Hospital establishes (and implements as needed) the following procedures for obtaining necessary PHI during an emergency.
- c. Automatic Logoff. (Addressable according to the Security Rules.) Midland Memorial Hospital configures networked and standalone systems to terminate an electronic session after a predetermined time of inactivity where possible.

Audit Controls. Midland Memorial Hospital implements the following hardware, software and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic PHI.

- Midland Memorial Hospital logs user activity on the Midland Memorial Hospital network and standalone systems and utilizes intrusion detection software to alert management to unusual activity where possible.

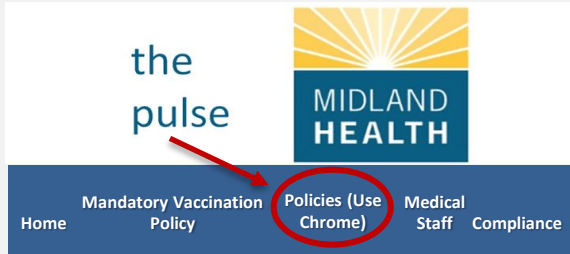
Integrity. Midland Memorial Hospital implements procedures to protect PHI from improper alteration or destruction.

Read entire Policy: Midland Health PolicyTech #2946
<https://midland.policytech.com/dotNet/documents/?docid=23360>

Midland Health PolicyTech Instructions

Click this link located on the Midland Health intranet "Policies"

<https://midland.policytech.com/dotNet/noAuth/login.aspx?ReturnUrl=%2f>



IN OTHER COMPLIANCE NEWS

LINK 1

Ransomware Attack Key Factor in Decision to Close Rural Illinois Hospital

<https://www.hipaajournal.com/ransomware-attack-key-factor-in-decision-to-close-rural-illinois-hospital/>

LINK 2

Doctor Fined for Privacy Violations Following Abortion on 10-Year-Old Rape Victim

<https://www.hipaajournal.com/doctor-fined-privacy-violations-abortion-10-year-old-rape-victim/>

LINK 3

OCR Fines Arkansas Business Associate \$350,000 for Impermissibly Disclosing Ephi

<https://www.hipaajournal.com/ocr-fines-arkansas-business-associate-350000-for-impermissibly-disclosing-ephi/>

LINK 4

Former Methodist Hospital Employees Plead Guilty to Criminal HIPAA Violations

<https://www.hipaajournal.com/former-methodist-hospital-employees-plead-guilty-to-criminal-hipaa-violations/>

Arizona Man Sentenced to 54 Months in Criminal HIPAA Violation Case

An Arizona man has been sentenced to 54 months in jail for aggravated identity theft and criminal violations of the Health Insurance Portability and Accountability Act (HIPAA). Rico Prunty, 41 years old, of Sierra Vista, Arizona, was previously employed at an Arizona medical facility where he unlawfully accessed the medical intake forms of patients between July 2014 and May 2017. The intake forms included information protected under HIPAA such as names, dates of birth, addresses, employer information, social security numbers, diagnoses, and medical information.

He then provided that information to his co-conspirators – Vincent Prunty, Temika Coleman, and Gemico Childress – who used the stolen information to open credit card accounts in the victims' names. Federal prosecutors investigating the identity theft raided an apartment linked to the suspects and found evidence of the manufacture of credit cards and the opening of fraudulent accounts in victims' names. Prunty and his co-conspirators attempted to steal more than \$181,000 from the victims.

According to court documents, the protected health information of almost 500 patients was accessed without authorization, and their information was impermissibly disclosed to Prunty's co-conspirators. Rico Prunty pleaded guilty to aggravated identity theft and criminal HIPAA violations for accessing and disclosing patients' protected health information. The HIPAA violations carried a maximum jail term of 10 years, and aggravated identity has a mandatory sentence of 2 years, which runs consecutively to sentences for other felony crimes. Senior U.S. District Court Judge James Moody imposed a sentence of 54 months with 2 years of supervised release and Prunty was ordered to pay \$132,521.98 in restitution to the victims.

Read entire article:
<https://www.hipaajournal.com/arizona-man-sentenced-to-54-months-in-criminal-hipaa-violation-case/>

HIPAA RIGHT OF ACCESS VIOLATION

Pittsburgh Counselor Fined \$15,000 for HIPAA Right of Access Violation

The HHS' Office for Civil Rights has announced its 44th enforcement action under its HIPAA Right of Access initiative with a \$15,000 financial penalty for David Mente, MA, LPC, a licensed counselor that provides psychotherapy services in Pittsburgh, PA.

The HIPAA Right of Access allows individuals to obtain a copy of their health information. Healthcare providers are required to respond to requests and provide the requested records within 30 days of the request being received, although a 30-day extension is possible in certain circumstances. This case stemmed from a complaint from a father of three children who requested a copy of his minor children's medical records from Mente in December 2017. The complainant was the personal representative of his children and should have been provided with the records as requested.

After receiving the complaint, OCR contacted Mente, provided technical assistance on the HIPAA Right of Access, and closed the complaint. The father made a second request for a copy of the records in April 2018; however, Mente again failed to provide the requested records, despite having received technical assistance from OCR. That led to the father filing a second complaint with OCR.

Read entire article:
<https://www.hipaajournal.com/pittsburgh-counselor-fined-15000-for-hipaa-right-of-access-violation/>

