

COMPLIANCE CONNECTION

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



AUGUST 2023

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

IN THIS ISSUE

FEATURE ARTICLE

Washington Hospital Pays \$240,000 HIPAA Penalty After Security Guards Access Medical Records

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 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

WASHINGTON HOSPITAL PAYS \$240,000

OFFICE FOR CIVIL RIGHTS

HIPAA Penalty After Security Guards Access Medical Records

The HHS' Office for Civil Rights (OCR) investigates all reported breaches of the protected health information of 500 or more individuals and some smaller breaches to determine if the breach was caused by the failure to comply with the HIPAA Rules. OCR's latest HIPAA enforcement action confirms that it is not the scale of a data breach that determines if a financial penalty must be paid but the severity of the underlying HIPAA violations.

A relatively small data breach was reported to OCR on February 28, 2018, by Yakima Valley Memorial Hospital (formerly Virginia Mason Memorial), a 222-bed non-profit community hospital in Washington state. The hospital discovered security guards had been accessing the medical records of patients when there was no legitimate work reason for the medical record access, and 419 medical records had been impermissibly viewed.

OCR launched an investigation into the snooping incident in May 2018 and discovered widespread snooping on medical records by security guards in the hospital's emergency department. 23 security guards had used their login credentials to access medical records in the hospital's electronic medical record system when there was no legitimate reason for the access. The security guards were able to view protected health information such as names, addresses, dates of birth, medical record numbers, certain notes related to treatment, and insurance information. OCR determined that the hospital had failed to implement reasonable and appropriate policies and procedures to comply with the standards, implementation specifications, or other requirements of the Security Rule – 45 C.F.R. § 164.316.

Yakima Valley Memorial Hospital chose to settle the case with OCR and agreed to pay a financial penalty of \$240,000 with no admission of liability.

Read entire article:

<https://www.hipaajournal.com/washington-hospital-security-guard-snooping-240000-hipaa-penalty/>

DID YOU KNOW...



WHAT DOES THE HIPAA PRIVACY RULE DO?

The HIPAA Privacy Rule for the first time creates national standards to protect individuals' medical records and other personal health information. It gives patients more control over their health information. It sets boundaries on the use and release of health records.

Read entire article:

<https://www.hhs.gov/hipaa/for-individuals/faq/187/what-does-the-hipaa-privacy-rule-do/index.html#:~:text=The%20HIPAA%20Privacy%20Rule%20for,and%20release%20of%20health%20records.>



MIDLAND
HEALTH



**HIPAA Section 6.23:
E-mail & Text Message Communications**

POLICY

MIDLAND MEMORIAL HOSPITAL and its workforce members may not communicate with patients and business associates via e-mail or text message outside of the MIDLAND MEMORIAL HOSPITAL e-mail system, if Protected Health Information (PHI) is included in that communication. Workforce members may communicate with other health care providers for treatment, payment, or health care operations purposes (as defined by HIPAA), if it is done in a secured manner as required by HIPAA and in accordance with MIDLAND MEMORIAL HOSPITAL policy (or, MIDLAND MEMORIAL HOSPITAL has written authorization from the patient for the release of the PHI). Permitted e-mail or text message communication shall be in accordance with the procedures set forth below and other safeguards implemented in this policy. MIDLAND MEMORIAL HOSPITAL workforce members with an e-mail account, access to approved text messaging application software, or access to a wireless device enabled with approved text messaging capabilities shall be familiar with this policy and shall follow these procedures when disclosing PHI via permitted e-mail or text message. Transmitting PHI via e-mail or text message other than as permitted herein is expressly prohibited, unless pre-approved by the Privacy Officer.

Section 1: Safeguards

MIDLAND MEMORIAL HOSPITAL workforce members and medical staff may communicate with patients via hospital e-mail or text message or, in certain situations, with third parties via e-mail or text message with patient authorization, as described in Section 2 below, if appropriate safeguards are in place to protect a patient's PHI. The Health Information System (HIS) Department shall be responsible for implementing technical safeguards to protect the security of e-mail and text message communication and training Users with respect to the use of such technical safeguards. MIDLAND MEMORIAL HOSPITAL shall also implement manual or administrative procedures, such as verifying e-mail addresses, requiring user account authentication prior to accessing text messaging applications and training workforce members on how to help safeguard PHI transmitted via e-mail or text message. MIDLAND MEMORIAL HOSPITAL workforce members shall be responsible for understanding and using required safeguards when they transmit PHI via hospital e-mail or text message.

Read entire Policy: [Midland Health PolicyTech #2915](#)
"HIPAA Section 6.23: E-mail and Text Message Communications"

Midland Health PolicyTech Instructions

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

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

the pulse



Home Mandatory Vaccination Policy Policies (Use Chrome) Medical Staff Compliance

IN OTHER COMPLIANCE NEWS

LINK 1

Atlanta Women's Health Group Data Breach Impacts 33,800 Patients

<https://www.hipaajournal.com/atlanta-womens-health-group-data-breach-impacts-33800-patients/>

LINK 2

Mistrial Declared in Criminal HIPAA Prosecution of Couple Who Disclosed PHI to Undercover FBI Agent

<https://www.hipaajournal.com/mistrial-criminal-hipaa-prosecution-couple-phi-undercover-fbi-agent/>

LINK 3

24 State Attorneys General Confirm Support for Stronger HIPAA Protections for Reproductive Health Data

<https://www.hipaajournal.com/24-state-attorneys-general-support-hippa-privacy-rule-update-reproductive-health-data/>

LINK 4

Kaiser Permanente Fined \$450,000 for CMIA Violations Due to Mailing Error

<https://www.hipaajournal.com/kaiser-permanente-fined-450000-for-cmia-violations-due-to-mailing-error/>



California Skilled Nursing Facility and Management Company Agree to Pay \$3.825 Million to Settle Allegations of Kickbacks to Referring Physicians

Alta Vista Healthcare & Wellness Centre, LLC (Alta Vista), a skilled nursing facility in Riverside, California, and its management company, Rockport Healthcare Services (Rockport), have agreed to pay the United States and California a total of \$3.825 million to resolve allegations that they submitted and caused the submission of false claims to Medicare and Medicaid by paying kickbacks to physicians to induce patient referrals. The settlement amount was negotiated based on Alta Vista's and Rockport's lack of ability to pay.

The Anti-Kickback Statute prohibits offering or paying remuneration to induce the referral of items or services covered by Medicare, Medicaid, and other federally funded programs. It is intended to ensure that medical decision-making is not compromised by improper financial incentives and is instead based on the best interests of the patient.

From 2009 through 2019, Alta Vista, under the direction and control of Rockport, gave certain physicians extravagant gifts, including expensive dinners for the physicians and their spouses, golf trips, limousine rides, massages, e-reader tablets, and gift cards worth up to \$1,000. Separately, Alta Vista paid these physicians monthly stipends of \$2,500 to \$4,000, purportedly for their services as medical directors. At least one purpose of these gifts and payments was to induce these physicians to refer patients to Alta Vista.

"Kickbacks can impair the independence of physician decision-making and waste taxpayer dollars," said Principal Deputy Assistant Attorney General Brian M. Boynton, head of the Justice Department's Civil Division.

Read entire article:

<https://www.justice.gov/opa/pr/california-skilled-nursing-facility-and-management-company-agree-pay-3825-million-settle>

FALSE CLAIMS ACT

Lab Billing Company Settles False Claims Act Allegations Relating to Unnecessary Respiratory Panels Run on Seniors Receiving COVID-19 Tests



VitalAxis Inc., a Maryland-based billing company for diagnostic laboratories, has agreed to pay \$300,479.58 to resolve False Claims Act allegations that it caused the submission of false claims to Medicare for medically unnecessary respiratory pathogen panels run on seniors who received COVID-19 tests.

Throughout 2020, VitalAxis performed billing services for a diagnostic laboratory in Atlanta, Georgia that provided COVID-19 testing to residents of senior living communities. For one chain of communities, the laboratory directed VitalAxis to bill Medicare for respiratory pathogen panels purportedly ordered by a physician who had not actually ordered the tests and who was ineligible to treat Medicare beneficiaries. VitalAxis found the credentials of a different physician and, without authorization, billed Medicare using that physician's name. Medicare subsequently paid the laboratory for these medically unnecessary tests.

Read entire article:

<https://www.justice.gov/opa/pr/lab-billing-company-settles-false-claims-act-allegations-relating-unnecessary-respiratory>



Do you have a hot topic or interesting Compliance News to report?

If so, please email an article or news link to:

**Regenia Blackmon
Compliance Auditor**

Regenia.Blackmon@midlandhealth.org