

COMPLIANCE CONNECTION

Compliance

The practice of obeying a rule, law, or regulation, or trying to fit specified standards set down by a body that prescribes regulations, policies, or the terms of a contract.

DECEMBER 2025

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:

[HIPAA For The Holidays](#)

Midland Health PolicyTech: Policy #6541 Code Of Conduct for Medical Staff and Practitioners (See Page 2)

FRAUD & ABUSE LAWS

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

- 1. False Claims Act (FCA):** The civil FCA protects the Government from being overcharged or sold shoddy goods or services. It is illegal to submit claims for payment to Medicare or Medicaid that you know or should know are false or fraudulent.
- 2. Anti-Kickback Statute (AKS):** The AKS is a criminal law that prohibits the knowing and willful payment of "remuneration" to induce or reward patient referrals or the generation of business involving any item or service payable by the Federal health care programs (e.g., drugs, supplies, or health care services for Medicare or Medicaid patients).
- 3. Physician Self-Referral Law (Stark law):** The Physician Self-Referral Law, commonly referred to as the Stark law, prohibits physicians from referring patients to receive "designated health services" payable by Medicare or Medicaid from entities with which the physician or an immediate family member has a financial relationship, unless an exception applies.
- 4. Exclusion Statute:** OIG is legally required to exclude from participation in all Federal health care programs individuals and entities convicted of the following types of criminal offenses: (1) Medicare or Medicaid fraud; (2) patient abuse or neglect; (3) felony convictions for other health-care-related fraud, theft, or other financial misconduct; and (4) felony convictions for unlawful manufacture, distribution, prescription, or dispensing of controlled substances.
- 5. Civil Monetary Penalties Law (CMPL):** OIG may seek civil monetary penalties and sometimes exclusion for a wide variety of conduct and is authorized to seek different amounts of penalties and assessments based on the type of violation at issue. Penalties range from \$10,000 to \$50,000 per violation.

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 Sheley, Senior Compliance Analyst
Melissa.Sheley@midlandhealth.org

HIPAA For The Holidays

The holiday season is filled with busy schedules, travel, and many distractions. It's essential to help your organization stay protected by educating your employees on maintaining the security and privacy of health information. A recent survey revealed that 65% of employees admitted to bypassing their organization's security policies to improve productivity, underscoring how often security measures are overlooked—especially during busy periods like the holidays. Whether your employees are working from home, traveling, or managing tasks outside the usual office setting, it's crucial to be extra cautious with sensitive data. Here are a few essential tips for HIPAA compliance during this hectic season.

1) Use a Secure Network: Public Wi-Fi might seem convenient when traveling, but it's a prime target for cybercriminals. When working outside your usual office environment, always use a secure, encrypted connection. This is essential for protecting sensitive health information.

2) Keep Devices Protected: Traveling often means you'll have your devices. Ensure that any devices, such as laptops, smartphones, or tablets, are password-protected and encrypted. This added layer of security helps prevent unauthorized access to PHI if your device is lost or stolen.

3) Be Aware of Phishing Scams: The holiday season often brings an increase in phishing attempts. Scammers may pose as colleagues or vendors, trying to trick you into revealing sensitive information. Employees should be especially cautious when opening emails or clicking on links, even if they seem to come from trusted sources. Always verify requests for health data or sensitive information through a secure channel.

4) Encrypt Data: Whether you're sending emails, working with files, or communicating via messaging apps, ensure that sensitive information is encrypted. This adds an additional layer of protection, ensuring that any health-related information stays safe during transmission.

5) Avoid Sharing PHI in Public Spaces: During the holidays, you may find yourself in public spaces, such as airports, cafes, or family gatherings, where conversations are easily overheard. To prevent accidental disclosures, avoid discussing protected health information (PHI) in these environments. If you need to communicate sensitive data, instead use secure communication methods or wait until you're in a private setting.

As the holiday season increases distractions and travel, ensuring HIPAA compliance should remain a top priority for employers. To learn more about safeguarding your organization, explore our HIPAA Solutions. Medcom offers comprehensive training, risk assessments, and compliance reviews to help maintain the highest standards of privacy and security throughout your organization.

Resource:

<https://medcombenefits.com/blog/post/hipaa-for-the-holidays>



MIDLAND HEALTH Compliance HOTLINE

855-662-SAFE (7233)

ID#: 6874433130

ID# is required to submit a report.

You can make your report or concern **ANONYMOUSLY**.



MIDLAND
HEALTH



CODE OF CONDUCT FOR MEDICAL STAFF AND PRACTITIONERS

1.0 PURPOSE

This policy is to ensure that Midland Memorial Hospital is a safe and constructive workplace for everyone who is striving to provide the highest-quality patient care and to provide a method for reviewing and reporting events of physician behavior that are unexpected or in violation of the medical staff bylaws, regulations, and policies.

- 1.1** It is the expectation of the [Midland Memorial Hospital] board of trustees that all members of the medical staff act in a professional and cooperative manner at the hospital, treating all patients and persons involved in their care with courtesy, dignity, and respect. These expectations are defined by the code of conduct.
- 1.2** Each member of the medical staff (individually, "physician") granted privileges at the hospital shall be required to acknowledge and agree to be bound by the code of conduct at the time of appointment/reappointment to promote and focus awareness of the essential elements of this policy.
- 1.3** This policy sets forth procedures for reviewing and addressing behavioral incidents when a member of the medical staff conducts himself or herself in a manner that is inconsistent with this code of conduct.

2.0 DEFINITIONS

Disruptive or inappropriate behavior can be defined as an aberrant style of personal interaction between members of the healthcare team, patients, and/or their family members that interferes with the delivery of excellent patient care. The behavior could take the form of language, personal habits, or physical confrontation. The following is a list of examples and is not intended to be all-inclusive of disruptive or inappropriate behavior.

- Using threatening, intimidating, or abusive language or gestures directed at patients, families, members of the healthcare team, or the hospital
- Making berating, degrading, derogatory, or demeaning comments regarding patients, families, members of the healthcare team, or the hospital

Read entire Policy:

Midland Health PolicyTech #6541 – "Code of Conduct for Medical Staff & Practitioners"

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



MIDLAND HEALTH

CERNER **POLICIES** NEWS RESOURCES DAYFORCE OFFICE365 DEPARTMENT PHONE LIST

IN OTHER COMPLIANCE NEWS

LINK 1

\$6.5 Million Settlement Resolves Omni Family Health Class Action Data Breach Lawsuit

<https://www.hipaajournal.com/mni-family-health-data-breach-settlement/>

LINK 2

Discovery Practice Management Settle Lawsuit Over 2020 Data Breach

<https://www.hipaajournal.com/discovery-practice-management-data-breach-settlement/>

LINK 3

Nebraska AG's Lawsuit Against Change Healthcare Survives Motion to Dismiss

<https://www.hipaajournal.com/change-healthcare-responding-to-cyberattack/>

LINK 4

Cyberattack Volume Increases Fueled by 48% YOY Increase in Ransomware Attacks

<https://www.hipaajournal.com/cyberattack-volume-increase-october-2025/>

Marketer Sentenced for \$11.5M Genetic Testing Fraud and Kickback Scheme

Robert Desselle, 47, was sentenced in Tampa, Florida, to 57 months in prison for conspiracy to defraud the United States and to pay and receive health care kickbacks. Desselle pleaded guilty in February 2025. In addition, Desselle was ordered to pay \$4.5 million in restitution and to forfeit \$2.1 million of the criminal proceeds.

According to court documents, Desselle and his co-conspirators convinced Medicare beneficiaries to take genetic tests that they did not need. Desselle paid other marketers, who were not medical professionals, to recruit vulnerable Medicare beneficiaries at grocery stores, pharmacies, or car dealerships and persuade them to take the tests using deceptive methods. Desselle then bribed a telemedicine company to supply doctors' orders for the tests. The orders and test kits were then sent to clinical laboratories who paid Desselle and his co-conspirators kickbacks in exchange for the referrals.

From June 2018 to December 2020, Desselle and his co-conspirators caused the laboratories to bill \$11.5 million to Medicare. Medicare paid out \$4.5 million on these claims. Desselle personally earned over \$2.1 million from the scheme.

The Department of Health and Human Services Office of the Inspector General (HHS-OIG) investigated the case.

Acting Assistant Attorney General Matthew Galeotti of the Justice Department's Criminal Division and Deputy Inspector General for Investigations Christian J. Schrank for HHS-OIG made the announcement.

Read entire article:

<https://www.justice.gov/opa/pr/marketer-sentenced-115m-genetic-testing-fraud-and-kickback-scheme>

HIPAA VIOLATION

Nurse Fired for Disclosing Teenager's Pregnancy Status to Family Member

An Iowa nurse has been terminated for a HIPAA violation and has lost her unemployment benefits after disclosing the pregnancy status of a 17-year-old patient to a family member without the patient's consent. Erica Hulsing was a registered nurse at Waverly Health Center in Waverly, Iowa, where she had been employed since September 2016. On April 17, 2025, Hulsing received a call from a family member of a 17-year-old patient inquiring about the patient's recent stay at the hospital.

The patient had made an explicit request for her pregnancy status to be kept confidential; however, Hulsing informed the family member that the patient had been pregnant. Following the disclosure, the patient and family members filed complaints with the hospital over the disclosure, prompting an internal investigation. The hospital determined that Hulsing had disclosed highly sensitive information about a patient to an individual who was not authorized to receive that information, as the family member was not listed on her consent form. The hospital determined that the disclosure was a violation of the HIPAA Privacy Rule, which prohibits disclosures of protected health information to unauthorized individuals. The disclosure also violated hospital policies on professional conduct, resulting in termination for gross misconduct.

Read entire article:

<https://www.hipaajournal.com/nurse-fired-disclosing-teenagers-pregnancy-status-family/>



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