COMPLIANCE CONNECTION Newsletter

MARCH 2026

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

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

58% of College Students Would Violate HIPAA and Sell Patient Data for the Right Price

A recent study exploring insider cybersecurity threats revealed that a majority of college students would be willing to violate the HIPAA Rules and steal and disclose patient data if they were paid to do so, provided the price was right. The amount of money required ranged from less than $10,000 to more than $10 million.

The study was conducted by Lawrence Sanders, professor emeritus, University of Buffalo, Department of Management Science and Systems, and colleagues at the School of Management, and builds on a 2020 study that explored the price of healthcare privacy violations.

The 2020 study, published in JMIR Medical Informatics, was conducted on 523 students (average age of 21) who were about to enter the workforce. The respondents were asked to imagine that they had been employed by a hospital and were given five scenarios in which they were asked if they would illegally obtain and disclose sensitive health information. 46% of respondents admitted that they would violate HIPAA and patient privacy if the price was right. In one of the scenarios, study participants were asked if they would obtain and disclose a politician's medical records in exchange for $100,000, if the money was needed to pay for an experimental treatment for their mother that insurance wouldn't cover. 79% of respondents said they would.

The follow-up study, which focused on cybersecurity insiders, was conducted on 500 undergraduate college students in technology-related programs, who represented future IT workers in the healthcare industry. They were asked to imagine they had been employed by a hospital, were being paid between $30,000 and $100,000, and were under financial stress and had been approached and asked to obtain and leak information about a famous patient at the hospital.

They were informed about HIPAA and how the federal law prohibited unauthorized access and disclosure of protected health information, yet 58% said they would violate HIPAA in exchange for payment. The amount of money required was less than $10,000 in some cases, and whether they would be tempted – and the amount required – varied depending on the employee's salary level and the perceived probability of being caught. The higher the employee's salary, the more money was required to violate HIPAA and steal data. Individuals who had an interest in ethical hacking generally required less money to violate HIPAA, as was the case with individuals with an interest in unethical hacking, if they were assured that they would not be caught. The study highlights the risk of insider data breaches and the importance of training on the HIPAA Privacy Rule requirements and the consequences of HIPAA violations, making it clear to all workers that if violations are discovered, the consequences of HIPAA violations can be severe.

"As cyberattacks and data breaches continue to rise, particularly in health care and other data-intensive sectors, our findings underscore the need for organizations to address the human and economic dimensions of cybersecurity alongside traditional technical controls," said Professor Sanders. "Promoting awareness and education can discourage people from engaging in cybercrime by highlighting the negative consequences and risks associated with it. Initiatives that promote economic opportunity, social inclusion, cybersecurity literacy and a more secure digital environment are part of the solution."

Resource:
https://www.hipaajournal.com/college-students-would-violate-hipaa-for-money/

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

MIDLAND HEALTH POLICYTECH

MIDLAND HEALTH • PT POLICYTECH® Policy & Procedure Management

HIPAA Section 10.3: Physical Safeguards

POLICY

It is the policy of Midland Memorial Hospital to employ physical 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 Information Security Officer shall determine which Midland Memorial Hospital workforce members shall be required to read and attest in writing that they understand this policy and who shall follow these procedures. All workforce members who have access to PHI shall be familiar with this policy and shall follow these procedures.

PHYSICAL SAFEGUARDS

PROCEDURE

It Facility Access Controls. Midland Memorial Hospital implements policies and procedures to limit physical access to its PHI and the facility or facilities in which PHI is housed, while ensuring that properly authorized access is allowed.

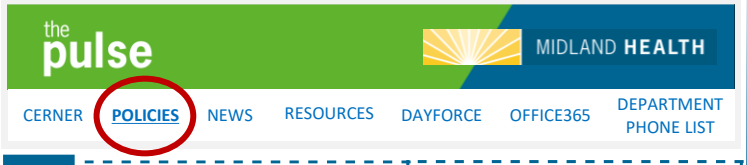
a. Facility Security Plan. (Addressable according to the Security Rules.) Midland Memorial Hospital implements the following procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering and theft.
   - Midland Memorial Hospital security routinely patrol all Midland Memorial Hospital facilities to ensure that locked doors remain locked and that facilities remain generally secure.
   - Midland Memorial Hospital keeps its facilities secure from unauthorized access by requiring all employees and subcontractors to use identification badges and by requiring all contractors to sign in and out.

b. Access Control and Validation Procedures. (Addressable according to the Security Rules.) Midland Memorial Hospital implements the following procedures to control and validate a person's access to facilities
   - Midland Memorial Hospital shall issue identification badges to employees and subcontractors.
   - Midland Memorial Hospital's computer systems are not accessible without user ids and passwords.
   - Midland Memorial Hospital shall entrust certain individuals to maintain keys to the locked room or file cabinets where records containing PHI are stored.

Read entire Policy:
Midland Health PolicyTech #2932 – "HIPAA Section 10.3: Physical Safeguards"

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
HHS Applies Inflation Increase to Penalties for HIPAA Violations
https://www.hipaajournal.com/hhs-applies-inflation-increase-penalties-for-hipaa-violations/

LINK 2
Comstar to Pay State AGs $515,000 to Settle Alleged HIPAA Violations
https://www.hipaajournal.com/comstar-hipaa-violation-penalty-mass-conn-2025/

LINK 3
OCR Advises HIPAA-Regulated Entities to Take Steps to Harden System Security
https://www.hipaajournal.com/ocr-harden-system-security/

LINK 4
What are the HIPAA Laws in Texas?
https://www.hipaajournal.com/hipaa-laws-in-texas/

ANTI-KICKBACK STATUTE (AKS)

South Carolina Laboratory Pleads Guilty and Agrees to Pay At Least $6.8M to Settle Allegations of Kickbacks to Doctors

Clinical laboratory LTD Holding LLC, formerly known as Labtech Diagnostics LLC (Labtech), of Anderson, South Carolina, and its founder and CEO Joseph Labash, of the United Arab Emirates, have agreed to pay at least $6.8 million to the United States to resolve False Claims Act allegations involving illegal kickbacks to doctors. With this settlement, the Department of Justice has secured over $11.5 million in civil False Claims Act settlements relating to Labtech, including recoveries from nine doctors.

In addition to the civil settlement, Labtech has agreed to plead guilty to five counts of offering and paying health care kickbacks in violation of the Anti-Kickback Statute, Title 42, United States Code, Sections 1320a-7b(b)(2)(A) and (B). Pursuant to the terms of the plea agreement in the criminal matter, Labtech will pay $103,551.90 in restitution, in addition to the civil recoveries above.

"Patients trust doctors to exercise their unbiased medical judgment in ordering clinical testing," said Assistant Attorney General Brett A. Shumate of the Justice Department's Civil Division. "Companies and executives who pay illegal kickbacks to referring doctors corrupt those doctors' independence, leaving patients vulnerable to expensive and unnecessary testing."

"Every dollar spent, and every decision made in health care must prioritize the patient's wellbeing and care," said U.S. Attorney Bryan Stirling for the District of South Carolina. "We will continue to work with our partners to pursue those engaged in illegal kickback schemes and hold them accountable."

"This settlement reaffirms the FBI's unwavering commitment to investigating fraud and holding accountable anyone who seeks to undermine our healthcare system," said Special Agent in Charge Kevin Moore of the FBI Columbia Field Office. "The public deserves complete confidence in the integrity of medical practices, and the FBI — alongside our law enforcement partners—will continue to ensure fairness and integrity of healthcare for all citizens."

Read entire article:
https://www.justice.gov/opa/pr/south-carolina-laboratory-pleads-guilty-and-agrees-pay-least-68m-settle-allegations

ANTI-KICKBACK STATUTE (AKS) • PHYSICIAN SELF REFERRAL (STARK LAW)

Traditions Health Agrees to Pay $34M to Resolve False Claims Act Liability Relating to Home Health Services Following Self Disclosure

Traditions Health LLC (Traditions) has agreed to pay $34 million to resolve its civil liability under the False Claims Act for billing medically unnecessary home health claims to Medicare and providing financial benefits to physicians in exchange for referrals. Traditions self-disclosed the conduct at issue to the government.

The settlement resolves allegations that, from 2021 to 2024, Traditions submitted claims to Medicare from its McAlester, Oklahoma, location for home health services that were not medically necessary. It also resolves claims that, between 2019 and 2024, Traditions paid remuneration to physician-medical directors in Oklahoma and Texas who referred Medicare beneficiaries to Traditions for home health services and that this remuneration potentially violated the Anti-Kickback Statute and the Physician Self-Referral Law.

The Anti-Kickback Statute prohibits the provision of remuneration to induce referrals of government health care program business. The Physician Self-Referral Law, commonly known as the Stark Law, prohibits physicians from making referrals for the furnishing of certain designated health services, including home health, payable by Medicare to an entity where the physician has a "financial relationship," unless the arrangement meets the requirements of a statutory or regulatory exception. Federal law prohibits payment by federal health care programs of medical claims that result from arrangements that violate the Anti-Kickback Statute or the Stark Law.

Read entire article:
https://www.justice.gov/opa/pr/traditions-health-agrees-pay-34m-resolve-false-claims-act-liability-relating-home-health

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