COMPLIANCE CONNECTION

FEBRUARY 2023

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

IN THIS ISSUE

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 Penalties 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

HIPAA Compliance for Hospitals

Discussing HIPAA compliance for hospitals in a single article is challenging. Not only is there so much to cover, but there are also many different types and sizes of hospitals. This means there is no one-size-fits-all guide to HIPAA compliance for hospitals, but rather checklists that can help hospitals cover the basics of the compliance requirements.

It is also the case that, regardless of the level of effort put in to comply specifically with HIPAA, most hospitals already comply with HIPAA to some degree due to the measures implemented in order to participate in Medicare. For example, most Medicare-participating hospitals already have:

- *A Notice of Rights which includes the hospital's grievance procedures*
- *Procedures to respond to patients' requests to access medical records*
- *Measures in place to ensure the confidentiality of patient records*
- *A system that maintains the availability of records during an emergency*
- *Physical safeguards that comply with the Health Care Facilities Code (NFPA 99)*

To start on the path to HIPAA compliance for hospitals, it does not take a great deal of effort to incorporate a Notice of Privacy Practices into the Notice of Rights, to adopt existing patient access procedures to accommodate requests for amendments or requests to limit uses and disclosures, and to upgrade confidentiality, availability, and physical safeguards to meet HIPAA standards.

What is Required to Comply with HIPAA?

Although it may not take a great deal of effort to upgrade existing Medicare measures to HIPAA standards, it is important the method used is organized. If HIPAA compliance is approached in a haphazard manner, it can result in gaps in compliance, which can result in avoidable HIPAA violations, which can lead to penalties being issued by the HHS' Office for Civil Rights.

Therefore, one of the most thorough ways to address HIPAA compliance for hospitals that already have measures in place to fulfill the Medicare requirements is to designate a Privacy Officer responsible for compliance with the HIPAA Privacy and Breach Notification Rules and a Security Officer responsible for compliance with the HIPAA Security Rule.

Thereafter, hospitals can start to identify what is required to comply with HIPAA by following the Administrative Requirements of the Privacy Rule (§ 164.530) and the Administrative Safeguards of the Security Rule (§ 164.308). Between them, these two standards will enable Compliance Officers to compile an inventory of where in the organization Protected Health Information is created, received, maintained, or transmitted, and identify threats to its confidentiality, integrity, and availability.

Read entire article:
https://www.hipaajournal.com/hipaa-compliance-for-hospitals/

DID YOU KNOW...

Anti-Kickback Statute (AKS)

Criminal penalties and administrative sanctions for violating the AKS include fines, jail terms, and exclusion from participation in the Federal health care programs. Under the Civil Monetary Penalties Law (CMPL), physicians who pay or accept kickbacks also face penalties of up to $50,000 per kickback plus three times the amount of the remuneration.

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

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

PROCUDURE

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.

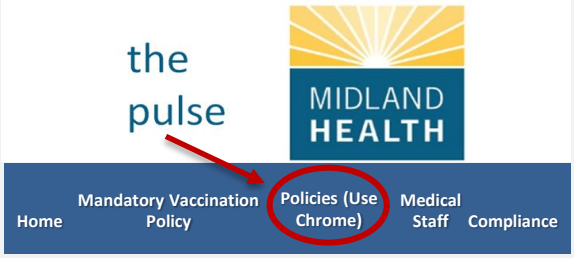
b. *Access Control and Validation Procedures. (Addressable according to the Security Rules.)* Midland Memorial Hospital implements the following procedures to control and validate a person's access to facilities

- 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
https://midland.policytech.com/dotNet/documents/?docid=23364

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

Medical Device Cybersecurity Provisions Included in Omnibus Appropriations Bill

https://www.hipaajournal.com/medical-device-cybersecurity-provisions-included-in-omnibus-appropriations-bill/

LINK 2

Six Data Breaches Reported by Healthcare Providers and Business Associates

https://www.hipaajournal.com/six-data-breaches-reported-by-healthcare-providers-and-business-associates/

LINK 3

Class Action Data Breach Lawsuit Settled by Morley Companies

https://www.hipaajournal.com/class-action-data-breach-lawsuit-settled-by-morley-companies/

LINK 4

Privacy Breaches Reported by Blue Shield of California and VA Medical Center

https://www.hipaajournal.com/privacy-breaches-reported-by-blue-shield-of-california-and-va-medical-center/

CIVIL MONETARY PENALTIES LAW (CMPL)

Sanford Health, Sanford Clinic, and Sanford Medical Center Agreed to Pay $25,000 for Allegedly Violating the Civil Monetary Penalties Law by Submitting Claims for Telemedicine Services that Did Not Meet Applicable Requirements

After they disclosed conduct to OIG pursuant to their corporate integrity agreement (CIA), Sanford Health, Sanford Clinic, and Sanford Medical Center (collectively, "Sanford"), South Dakota, entered into a $25,842 settlement agreement with OIG. OIG alleged that Sanford submitted claims to Medicare, Medicaid, TRICARE, and the Health Resources and Services Administration's COVID-19 Uninsured Program for telemedicine services provided by a physician that did not meet applicable requirements. Specifically, OIG alleged that Sanford submitted claims for services that: (1) were scheduled for times when the physician was out of the country and without access to Sanford's approved telemedicine platform; (2) did not involve interactive two-way video and audio as required; and (3) purported to be for multiple family members when the physician had only spoken to one family member.

Resource:
https://oig.hhs.gov/fraud/enforcement/sanford-health-sanford-clinic-and-sanford-medical-center-agreed-to-pay-25000-for-allegedly-violating-the-civil-monetary-penalties-law-by-submitting-claims-for-telemedicine-services-that-did-not-meet-applicable-requirements/

FALSE CLAIMS ACT (FCA)

Advanced Bionics LLC to Pay Over $12 Million for Alleged False Claims for Cochlear Implant Processors

Advanced Bionics LLC, a Valencia, California-based manufacturer of cochlear implant system devices, has agreed to pay more than $12 million to resolve allegations that it misled federal health care programs regarding the radio-frequency (RF) emissions generated by some of its cochlear implant processors.

"The United States expects device manufacturers to provide accurate information when they claim that their devices meet certain tests or standards," said Principal Deputy Assistant Attorney General Brian M. Boynton, head of the Department of Justice's Civil Division. "The integrity of our health care system depends on the government being able to rely on the information provided by manufacturers when they apply for permission to market their devices."

"The FDA's approval process requires companies to demonstrate the efficacy of their products," said U.S Attorney Jacqueline C. Romero for the Eastern District of Pennsylvania. "The settlement in this case demonstrates our commitment to hold responsible any medical device manufacturer that skirts these rules and seeks FDA approval of a device it knows is not as effective as represented. The consumers who use these devices, and the federal programs that pay for many of them, deserve better."

The tests at issue measured the extent to which cochlear implant systems generate RF emissions that can potentially interfere with other devices that use the RF spectrum. Such other devices may include telephones, alarm and security systems, televisions and radios.

The settlement resolves allegations that Advanced Bionics, in submitting pre-market approval applications to the Food and Drug Administration (FDA) for Advanced Bionics' Neptune and Naida cochlear implant processors, made false claims regarding the results of its RF emissions tests. Advanced Bionics allegedly represented that its processors satisfied an internationally recognized emissions standard when, in fact, Advanced Bionics did not comply with that standard. More specifically, Advanced Bionics allegedly failed to honor the standard's requirements to test processors using "worst-case" configurations, and improperly shielded certain emissions-generating system components during emissions testing. Advanced Bionics then allegedly sought reimbursement from Medicare, Medicaid, and other federally funded healthcare programs for these devices. .

Read entire article:
https://www.justice.gov/opa/pr/advanced-bionics-llc-pay-over-12-million-alleged-false-claims-cochlear-implant-processors