COMPLIANCE CONNECTION

JULY 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

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

Healthcare Workers Violating Patient Privacy by Uploading Sensitive Data to GenAI and Cloud Accounts

Research conducted by the cybersecurity company Netskope indicates healthcare workers routinely expose sensitive data such as protected health information (PHI) by using generative AI tools such as ChatGPT and Google Gemini and by uploading data to personal cloud storage services such as Google Drive and OneDrive.

The healthcare industry has fully embraced AI tools, with almost all organizations using AI tools to some degree to improve efficiency. According to data collected by Netskope Threat Labs, 88% of healthcare organizations have integrated cloud-based genAI apps into their operations, 98% use apps that incorporate genAI features, 96% use apps that leverage user data for training, and 43% are experimenting with running genAI infrastructure locally.

As more healthcare organizations incorporate AI tools into their operations and make them available to their workforces, fewer healthcare workers are using personal AI accounts for work purposes; however, 71% of healthcare workers still use personal AI accounts, down from 87% the previous year. If genAI tools are not HIPAA-compliant and the developers will not sign business associate agreements, using those tools with PHI violates HIPAA and puts organizations at risk of regulatory penalties. Further, uploading patient data to genAI tools and cloud storage services without robust safeguards in place can erode patient trust.

“Beyond financial consequences, breaches erode patient trust and damage organizational credibility with vendors and partners,” Ray Canzanese of Netskope said. It is clear that there needs to be greater oversight of the use of AI tools, and a pressing need for authorized tools to be provided to reduce “shadow AI” risks.

According to Netskope, the mishandling of HIPAA-regulated data is the leading security concern in the healthcare sector, and PHI is the most common type of sensitive data uploaded to personal cloud apps, genAI apps, and other unapproved locations. Netskope reports that 81% of all data policy violations were for regulated healthcare data, with the remainder including source code, secrets, and intellectual property.

“Healthcare organizations must balance the benefits of genAI with the implementation of strict data governance policies to mitigate associated risks,” warns Netskope. Netskope recommends the adoption of enterprise-grade genAI applications with robust security features to ensure that sensitive and regulated data is properly protected, along with data loss prevention (DLP) tools for monitoring and controlling access to genAI tools to prevent privacy violations. Netskope says 54% of healthcare organizations now have DLP policies, up from 31% the previous year. The most commonly blocked genAI apps in healthcare are DeepAI, Tactiq, and Scite, with 44%, 40%, and 36% of healthcare organizations blocking these apps with their DLP tools due to privacy risks and there being more secure alternatives.

Read entire article:
https://www.hipaajournal.com/healthcare-workers-privacy-violations-ai-tools-cloud-accounts/

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

Destruction of Protected Health Information

PURPOSE

This policy will establish guidelines for appropriate destruction of protected health information.

Policy

I. Destruction of patient health information shall be carried out in accordance with federal and state laws, and pursuant to a written retention schedule and destruction policy approved by the Director of HIM (Health Information Management/Medical Records), Chief Executive Officer, Medical Staff and Midland Memorial Hospital legal counsel.

II. The following retention schedule will be used to determine when medical records may be destroyed:
   a. If the patient is 18 years of age or older on the day of treatment, the record for that specific treatment may be destroyed 10 years later.
   b. If the patient is under 18 years of age on the day of treatment, the record for that specific treatment may be destroyed on or after the patient's 20th birthday or on or after the 10th anniversary of the date on which the patient was last treated, whichever date is later.

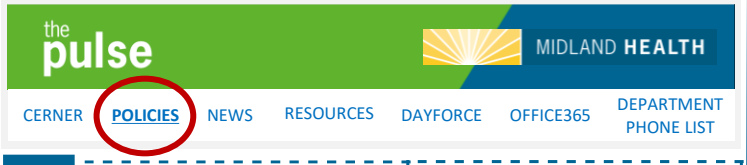
Procedure

I. The Director of HIM or designee will:
   a. Consult the above retention schedule to make sure the required retention period has been fulfilled.
   b. Contact Quality Management to ensure that the record is not subject to pending litigation.
   c. Ensure that the records are destroyed in a manner wherein there is no possibility of information reconstruction.
   d. Ensure that information on back-up media has also been destroyed.
   e. Ensure that the appropriate method of destruction is used:
      i. Paper media – Shredding, pulping or burning
      ii. Microfilm or microfiche – Shredding
      iii. CD-ROM, CD-RW or DVD - Shredding or physically destroying the disk.
      iv. Floppy disk (3.5", 5.25" or other) - Shredding/ physically destroying the disk.

Read entire Policy #88:
"Destruction of Protected Health Information"

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 Imaging Service Provider Settles HIPAA Risk Analysis & Breach Notification Failures

https://www.hipaajournal.com/vision-upright-mri-hipaa-penalty/

LINK 2
What is the Relationship Between HITECH, HIPAA, and Electronic Health and Medical Records?

https://www.hipaajournal.com/relationship-between-hitech-hipaa-electronic-health-medical-records/

LINK 3
Kettering Health Resumes Normal Operations for Key Services Following Ransomware Attack

https://www.hipaajournal.com/kettering-health-ransomware-attack/

LINK 4
HIPAA for Therapists

https://www.hipaajournal.com/hipaa-for-therapists/

FALSE CLAIMS ACT (FCA)

Texas Doctor Who Falsely Diagnosed Patients Sentenced to 10 Years' Imprisonment in Connection with $118M in Fraudulent Health Care Claims

A Texas rheumatologist was sentenced to 10 years in prison and three years of supervised release for perpetrating a health care fraud scheme involving over $118 million in false claims and the payment of over $28 million by insurers as a result of him falsely diagnosing patients with chronic illnesses to bill for tests and treatments that the patients did not need. Jorge Zamora-Quezada M.D., 68, of Mission, also falsified patient records to support the false diagnoses after receiving a federal grand jury subpoena. Following a 25-day trial, Zamora-Quezada was convicted of one count of conspiracy to commit health care fraud, seven counts of health care fraud, and one count of conspiracy to obstruct justice. In addition to his prison term, Zamora-Quezada was ordered to forfeit $28,245,454, including 13 real estate properties, a jet, and a Maserati GranTurismo.

According to the evidence presented at trial, Zamora-Quezada falsely diagnosed his patients with rheumatoid arthritis and administered toxic medications in order to defraud Medicare, Medicaid, TRICARE, and Blue Cross Blue Shield. The fraudulent diagnoses made the defendant's patients believe that they had a life-long, incurable condition that required regular treatment at his offices. After falsely diagnosing his patients, Zamora-Quezada administered unnecessary treatments and ordered unnecessary testing on them, including a variety of injections, infusions, x-rays, MRIs, and other procedures—all with potentially harmful and even deadly side effects. To receive payment for these expensive services, Zamora-Quezada fabricated medical records and lied about the patients' condition to insurers.

Read entire article:
https://www.justice.gov/opa/pr/texas-doctor-who-falsely-diagnosed-patients-sentenced-10-years-imprisonment-118m-health-care

ANTI-KICKBACK STATUTE (AKS)

Florida Ophthalmology Practice Agrees to Pay $615,000 to Resolve Allegations of Fraudulent Claims to Medicare and Medicaid for Cranial Ultrasounds

Pinellas Eye Care, P.A. doing business as Gulfcoast Eye Care ("Gulfcoast Eye"), an ophthalmology practice with offices in Pinellas Park, Palm Harbor, and St. Petersburg, Florida, has agreed to pay $615,000 to resolve alleged violations of the False Claims Act and an analogous Florida statute arising from its billing for trans-cranial doppler ultrasounds ("TCDs") provided through a kickback arrangement with a third party. Gulfcoast Eye has agreed to cooperate with the Justice Department's ongoing investigations of other participants in the alleged scheme.

The settlement resolves allegations that Gulfcoast Eye knowingly submitted, and caused the submission of, false claims to Medicare and Medicaid for medically unnecessary TCDs. Gulfcoast Eye and a third-party provider of TCD services performed TCDs on thousands of patients and billed Medicare and Medicaid hundreds of dollars per test. Before the patients received the results of the test, Gulfcoast Eye and the third-party provider identified the patients as having received a serious diagnosis — most commonly of occlusion and stenosis of their cerebral arteries — that could qualify the patient for reimbursement of a TCD by Medicare or Medicaid. However, nearly all patients who received TCDs never had occlusion and stenosis of cerebral arteries, and that diagnosis was accordingly not reflected in the patient's medical history or in the TCD results. Gulfcoast Eye paid the third-party TCD provider based on the volume or value of tests ordered and referred the patients to the TCD provider's preferred radiology group for the TCD's professional component.

Read entire article:
https://www.justice.gov/opa/pr/florida-ophthalmology-practice-agrees-pay-615000-resolve-allegations-fraudulent-claims

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