SEPTEMBER 2024

COMPLIANCE CONNECTION

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, *Sr. Compliance Analyst*
Melissa.Sheley@midlandhealth.org

Organ Transplant Coordinator Convicted of Illegally Accessing Health Records of Supreme Court Judge

An organ transplant coordinator has been found guilty of illegally accessing the health records of Supreme Court Justice Ruth Bader Ginsburg and deleting evidence but was acquitted on the charge of publishing a copy of the records online.

Trent J. Russell, 34, was charged over the illegal access to Ginsburg's health records while she was undergoing cancer treatment at George Washington University Hospital in 2019 and posting the information on the 4chan online message board, a location well known for conspiracy theory discussions. The shared screenshot showed Ginsburg's name, treatments, and treatment dates between 2014 and 2018. Users of the 4chan platform shared conspiracy theories about Ginsburg, including one that she had died, and her death was being kept a secret to prevent President Trump from appointing a replacement Supreme Court judge.

George Washington University Hospital officials searched access logs and identified unauthorized access to Ginsburg's records using Russell's credentials, with the access traced to his home computer. Russell worked as an organ transplant coordinator at the Washington Regional Transplant Community (WRTC) and had legitimate access to medical records at George Washington University Hospital to perform his work duties, which included visiting the hospital to evaluate patients for organ transplants.

Russell was aware of his responsibilities under HIPAA as he had undergone training and knew that he was not permitted to access the medical records of individuals outside of his job responsibilities, which included Ginsburg's records as she had not been referred to WRTC as a potential organ donor. WRTC founder and former CEO, Lori Brigham, explained that coordinators had no business looking at the charts of individuals who had not been referred to WRTC as potential donors.

Russell was interviewed in 2019 over the unauthorized access and initially claimed that his phone had been stolen. He also maintained that he had not accessed Ginsburg's records and said he had shared his hospital login credentials with other individuals. George Washington University Hospital's chief information officer, Nathan Read, testified that Russell's access to medical records was terminated in January 2019 when he was identified as a suspect in the case and that Russell had asked for his access to be restored a month later, but that request was denied.

Read entire article:
https://www.hipaajournal.com/organ-transplant-coordinator-guilty-medical-record-access-ginsburg/

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

HIPAA Section 14: Progressive Discipline Policy

Purpose: To provide research and guidelines for addressing the appropriate sanction/corrective action for violation of patient privacy and security by a workforce member.

Related Policies and Procedures:

- HR-522: Sanctions Policy
- Confidentiality of Protected Health Information Policy
- Workforce Member Protected Health Information Agreement

Definitions:

Privacy/Security Violation: Any inappropriate access, use, disclosure, destruction or other misuse of PHI, failure to comply with MIDLAND MEMORIAL HOSPITAL privacy and security policies, or any violation of federal or state privacy and security regulations. A violation may involve, but is not necessarily limited to, verbal communications, paper medical records, electronic health records, or any other medium used to create, maintain, or transmit PHI. A violation of patient privacy through access to electronic patient health information applications and systems is both a Privacy and Security violation.

Protected Health Information (PHI): Individually identifiable health information that is created by or received by MIDLAND MEMORIAL HOSPITAL, including demographic information that identifies an individual, or provides a reasonable basis to believe the information can be used to identify an individual, and relates to:

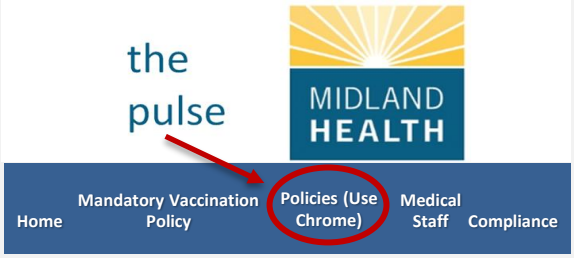
- Past, present or future physical or mental health or condition of an individual.
- The provision of health care to an individual.
- The past, present, or future payment for the provision of health care to an individual.

Workforce: Under HIPAA, the workforce is defined to include employees, medical staff members, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity, is under the direct control of such entity, whether or not they are paid by the covered entity.

Read entire Policy:
Midland Health PolicyTech #2648 – "HIPAA Section 14: Progressive Discipline Policy"

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
Jail Terms for HIPAA Violations by Employees
https://www.hipaajournal.com/jail-terms-for-hipaa-violations-by-employees/

LINK 2
Editorial: The Role of Nursing Education in Ensuring HIPAA Compliance
https://www.hipaajournal.com/nursing-education-hipaa-compliance/

LINK 3
Iowa Doctor Pleads Guilty to HIPAA Violations
https://www.hipaajournal.com/iowa-doctor-pleads-guilty-to-hipaa-violations/

LINK 4
Lurie Children's Hospital Sued Over January 2024 Ransomware Attack
https://www.hipaajournal.com/lurie-childrens-hospital-lawsuit-january-2024-ransomware-attack/

CIVIL MONETARY PENALTIES LAW (CMPL)

American Medical Response Pays $115K Civil Monetary Penalty for HIPAA Violation

American Medical Response (AMR), a private ambulance company, has paid a $115,200 civil monetary penalty to the HHS' Office for Civil Rights (OCR) to resolve a violation of the HIPAA Right of Access. AMR failed to provide a patient with timely access to their medical records, taking more than a year to provide the requested records.

The HIPAA Right of Access is an important provision of the HIPAA Privacy Rule and requires patients to be provided with a copy of their records, on request, within 30 days of submitting that request. In certain circumstances, a 30-day extension is permitted. The fine relates to American Medical Response Ambulance Service, a subsidiary of American Medical Response and a HIPAA-covered entity.

On October 31, 2018, the affected party sent a written request to AMR by fax requesting a copy of her medical records, specifically all billing records pertaining to treatment rendered for a 9/15/2015 injury date, patient balance verification, and all medical records pertaining to treatment rendered for the 9/15/2015 injury. She requested those records be provided in electronic format. Those records should have been provided by November 30, 2018. Follow-up requests were sent by the affected party on January 24, 2019, to AMR's Los Angeles office and its business associate Centrex. AMR responded to the request on March 1, 2019, 121 days after the initial request was submitted.

Read entire article:
https://www.hipaajournal.com/american-medical-response-pays-115k-civil-monetary-penalty-for-hipaa-violation/

SECURITY RULE VIOLATIONS

Heritage Valley Health System Pays $950,000 to Settle Alleged HIPAA Security Rule Violations

The HHS' Office for Civil Rights (OCR) has agreed to settle alleged HIPAA Security Rule violations with Heritage Valley Health System for $950,000. Heritage Valley is a 3-hospital health system with more than 50 physician offices and many community satellite facilities in Pennsylvania, eastern Ohio, and the panhandle of West Virginia.

In 2017, Heritage Valley was affected by a global malware attack that saw NotPetya malware installed on its network via a connection with its business associate, Nuance Communications. OCR launched an investigation of Heritage Valley in October 2017 following media reports of a data security incident to determine whether Heritage Valley was compliant with the requirements of the HIPAA Security Rule.

OCR's investigation uncovered multiple Security Rule compliance failures, including the most commonly identified Security Rule issue – The failure to conduct an accurate and thorough risk analysis to identify potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information (ePHI), as required by 45 C.F.R. § 164.308(a)(1)(ii)(A).

The HIPAA Security Rule – 45 C.F.R. § 164.308(a)(7) – requires covered entities to develop and implement a contingency plan for responding to an emergency that damages systems containing ePHI. Heritage Valley was found not to be compliant with this requirement. OCR also identified a failure to implement technical policies and procedures for electronic information systems that maintain ePHI only to permit access by authorized persons or software programs – 45 C.F.R. § 164.308(a)(4) and 164.312(a)(1)).

Read entire article:
https://www.hipaajournal.com/heritage-valley-health-system-ocr-hipaa-settlement/

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