MED-NET CONCEPTS LETTER ©

Where Compliance and Ethics, Risk Management/Safety, Quality Assurance and Performance Improvement, Reimbursement and Law Come Together.

Vol. 3, Issue 2 May 19, 2020

Dear Colleague,

Awareness is the first step toward an effective Compliance, Risk Management, Quality Assurance, Performance Improvement, and Law program. The following true reports are intended to broaden your understanding and awareness of potential exposures of liability throughout healthcare settings with the expectation that, as a starting point, forewarned is forearmed.

We believe a first-hand opinion of our sector of healthcare provides invaluable insight into the daily challenges facing our community.

Remember, it is important to immediately report any abuse of residents/patients, no matter the circumstances.

Please contact us for additional information as well as to discuss potential proactive programs to detect, prevent, and mitigate potential exposures and damages.

ALERTS

CMS Issues New Nursing Homes Toolkit to Combat COVID-19

CMS released a new toolkit developed to aid nursing homes, governors, states, departments of health, and other agencies who provide oversight and assistance to these facilities, with additional resources to aid in the fight against the coronavirus disease 2019 (COVID-19) pandemic within nursing homes. Access the toolkit here.

Illinois Nursing Home Allegedly Hired Registered Nurse with No License

Identity theft, a misdemeanor, two felony arrest warrants, and no nursing license, is what an Illinois nursing home should have discovered in early April when they hired a 23-year-old registered nurse who did not have a license. Nurses at the facility said they noticed something was wrong when they saw that the woman was unable to complete basic medical treatments without first searching for video demonstrations online. They said she was allowed to independently administer medication and provide treatment for at least fifty residents. A former LPN at the facility said she was fired for raising concerns to the facility administrator and the Director of Nursing on April 19th. "Instead of taking into consideration that she was lying, she covered for her. None of them were willing to listen to any of us. There was another nurse who quit because she said she wouldn't work with [the woman] because she didn't think she was safe." Another former LPN at the facility said, "I don't understand how you bring someone into that kind of position without doing a thorough background check. She could have killed somebody." Text messages show that the Director of Nursing responded to the allegations on April 23rd by saying the woman was "a good nurse" who had been "holding her own and stepped it up."

Compliance and Ethics Perspective:

To meet federal and state mandated requirements for providing sufficient and competent nursing services to care for its residents, nursing homes are required to screen and evaluate nurses being considered for employment. This screening and evaluating should involve the verification of a nurse's license and performing of a background check to determine if he/she has been convicted of any criminal activity or is listed in the Office of Inspector General (OIG) exclusion database. A facility is also forbidden

www.mednetconcepts.com, info@mednetconcepts.com
Tel: (609) 454-5020, Fax: (609) 454-5021
196 Princeton-Hightstown Road, Bldg. 1A, Suite 1A, West Windsor, NJ 08550

from exerting any type of retribution against an employee who reports concerns to a supervisor about another employee's incompetence in providing care and administering medications to residents. All reported concerns and incidents must be investigated, and employees must be trained in how to confidentially report a suspected incident through the use of the facility's Hotline if reporting to management has not resulted in necessary actions.

Kentucky Foot and Ankle Center Agrees to Pay $750,000 to Resolve Allegations of Violations of the False Claims Act

A Kentucky podiatry practice and doctor have recently agreed to resolve civil allegations that they violated the False Claims Act, agreeing to pay the United States $750,000. The agreement resolves a civil lawsuit filed by the United States against them on November 28, 2018. In the lawsuit, the United States alleged that the practice, at the doctor's direction, submitted false claims to Medicare and the Federal Employee Health Benefits Program, seeking payment for nail debridement services, for which podiatrists or other practitioners either did not assess or observe medical necessity or only performed less involved procedures. The lawsuit alleged that the defendants nevertheless submitted reimbursement claims for nail debridement, which are reimbursed at a higher rate. The United States further alleged that they created cloned (or nearly identical) patient records, in order to secure reimbursement for the false debridement claims. In addition to the monetary payment, the defendants have also agreed to submit to an integrity agreement with the Office of Inspector General of the Department of Health and Human Services (HHS-OIG), which will require additional review of their Medicare claims over a five-year period.

Compliance and Ethics Perspective:

There are two key elements that indicate liability in a False Claims Act violation: 1. The fraud needs to be perpetrated against the federal government, state government, or a government agency, and 2. the perpetrator must knowingly or deliberately show ignorance of the fraudulent action. A good example is a doctor's office knowingly providing unnecessary procedures to patients and intentionally over-billing Medicare. Creating cloned or nearly identical patient records in order to knowingly submit false claims for medically unnecessary podiatry procedures billed at a higher rate is a violation of the False Claims Act.

To help prevent these types of violations committed by unscrupulous physicians, nursing homes should consider performing screening and background checks on any physicians providing services to residents in their facilities to ensure that they have not been excluded as a Medicare and Medicaid provider.

Former Healthcare President Pleads Guilty to Embezzling over $763,000

A former healthcare president, 50, of Louisiana, pleaded guilty to embezzling $763,887 from a healthcare company. According to court documents, between July 2013 and May 2017, the defendant was the president of a company which sold diabetic testing kits. He entered into a plea agreement, in which he admitted that from December 2013 through January 2017, he embezzled approximately $763,887 from the company by submitting false and fraudulent reimbursement requests to the controller, claiming that he had purchased supplies and incurred travel expenses which he had not. To justify his reimbursement requests, he fabricated receipts to include with his fraudulent reimbursement requests. He submitted reimbursement requests for diabetic testing products, falsely claiming he had purchased those products, but he never actually purchased the supplies. Instead, he

visited multiple online vendors, such as Amazon or Diabetessupplies4less.com, placed the products in his online shopping cart, printed the computer screens displaying his shopping cart as the "receipt," and then attached those "receipts" to his reimbursement requests. He also fabricated credit card transaction receipts falsely showing he had purchased the products, and attached those fabricated receipts with his reimbursement requests. He was reimbursed at least $484,328 for supplies that he never purchased.

The defendant also admitted that he frequently submitted false travel expense reimbursements and travel advances, claiming that he traveled for business to meet with suppliers, customers, and individuals from the corporate office, and to attend conferences. In fact, he did not take the majority of the flights for which he was reimbursed approximately $203,747.83. Similar to how he falsified his expense reports for diabetic testing supplies, he would visit an airline's website, print an itinerary that displayed a cost for the flight, and submit that as the receipt without ever purchasing the flights. In addition to the airline reimbursements, he falsely claimed that he had attended conferences and fabricated credit card transaction receipts of at least $102,056. In an effort to further conceal the fraud, rather than depositing the reimbursement checks into his bank accounts, he cashed them at a bank or a check cashing business and either spent the cash or deposited it onto prepaid debit cards. He often used the funds for gambling.

Compliance and Ethics Perspective:
Knowingly submitting false and fraudulent reimbursement requests to an employer for purchases of medical supplies and incurred travel expenses, and failing to report those false reimbursement earnings as income to the IRS, may be considered a violation of the False Claims Act and result in federal charges for wire fraud and tax evasion. Violation of the False Claims Act involves two key elements for liability: 1. perpetrating the act knowingly and 2. against a government agency (federal, state, or local).

OCR Issues Guidance on Covered Healthcare Providers and Restrictions on Media Access to Protected Health Information about Individuals in Their Facilities

The Office for Civil Rights (OCR) at the US Department of Health and Human Services (HHS) issued additional guidance reminding covered healthcare providers that the HIPAA Privacy Rule does not permit them to give media and film crews access to facilities where patients' protected health information (PHI) will be accessible without the patients' prior authorization. The guidance explains that even during the current COVID-19 public health emergency, covered healthcare providers are still required to obtain a valid HIPAA authorization from each patient whose PHI will be accessible to the media ***before*** the media is given access to that PHI. The guidance clarifies that masking or obscuring patients' faces or identifying information before broadcasting a recording of a patient is not sufficient, as a valid HIPAA authorization is still required ***before*** giving the media such access. Additionally, the guidance describes reasonable safeguards that should be used to protect the privacy of patients whenever the media is granted access to facilities.

"The last thing hospital patients need to worry about during the COVID-19 crisis is a film crew walking around their bed shooting 'B-roll,'" said Roger Severino, OCR Director. "Hospitals and healthcare providers must get authorization from patients before giving the media access to their medical information; obscuring faces after the fact just doesn't cut it," Severino added.

www.mednetconcepts.com, info@mednetconcepts.com
Tel: (609) 454-5020, Fax: (609) 454-5021
196 Princeton-Hightstown Road, Bldg. 1A, Suite 1A, West Windsor, NJ 08550

The guidance may be found at https://www.hhs.gov/sites/default/files/guidance-on-media-and-film-crews-access-to-phi.pdf.

Risk Management Perspective:
Allowing media and film crews to access areas in a facility where residents' protected health information (PHI) might be accessible violates the HIPAA Privacy Rule unless the residents have signed a HIPAA Authorization Form. The authorization form must be written in plain language to ensure it can be easily understood, and as a minimum must contain the following elements:

- Specific and meaningful information, including a description, of the information that will be used or disclosed
- The name (or other specific identification) of the person or class of persons authorized to make the requested use or disclosure
- The name(s) or other specific identification of the person or class of persons to whom information will be disclosed
- A description of the purpose of the requested use or disclosure. In cases where a statement of the purpose is not provided, the phrase, "at the request of the individual," is sufficient.
- A specific time frame for the authorization, including an expiration date. In the case of uses and disclosures related to research, "at the end of the study" can be used or "none" in the case of the creation of a research database or research repository
- A date and signature from the individual giving the authorization. If the authorization is being given by an individual's authorized representative, a description of the person's authority to act on behalf of the individual must be detailed.

Statements must also be included on the HIPAA authorization to notify the individual of the right to revoke the authorization in writing and include either exceptions to the right to revoke and a description of how the right to revoke can be exercised, or the extent to which the information is included in the organization's notice of privacy practices. The individual providing consent must be given a copy of the authorization form for their own records.

Maze Ransomware Hackers Post Patient Data Stolen from Two Providers
The Maze ransomware hacking group failed to follow through with their assurance that the healthcare sector would be off-limits during the COVID-19 pandemic, by publishing data stolen from two separate doctors for sale on the dark web. Maze claims to have attacked the first victim with ransomware on May 1. As proof of their successful attack, they published a number of large files containing protected health information (PHI), including patient appointments, full names, dates of birth, contact information, social security numbers, health information, and provider comments. They also posted the doctor's QuickBooks and wireless merchant account passwords. The second victim was also attacked on May 1. The hackers published their patient PHI, including full names, diagnostic data, dates of birth, complete details of patient histories, and some health insurance information.

The Department of Homeland Security in conjunction with the United Kingdom's National Cyber Security Centre issued a joint alert warning that advanced persistent threat (APT) groups are exploiting the pandemic as part of their cyber operations. It describes some of the methods these actors are using to target organizations and provides mitigation advice. The joint CISA-NCSC Alert: (AA20-099A) COVID-19 Exploited by Malicious Cyber Actors from April 8, 2020, previously detailed the

www.mednetconcepts.com, info@mednetconcepts.com
Tel: (609) 454-5020, Fax: (609) 454-5021
196 Princeton-Hightstown Road, Bldg. 1A, Suite 1A, West Windsor, NJ 08550

exploitation of the COVID-19 pandemic by cybercriminals and APT groups. This joint CISA-NCSC Alert provides an update to ongoing malicious cyber activity relating to COVID-19. For a graphical summary of CISA's joint COVID-19 Alerts with NCSC, see the guide available here, https://www.cisa.gov/sites/default/files/publications/Joint_CISA_UK_Tip-COVID-19_Cyber_Threat_Exploitation_S508C.pdf.

Risk Management Perspective:

HIPAA regulations require healthcare providers to have defenses in place to mitigate the risk of cybercriminal and advanced persistent threat (APT) groups using the COVID-19 pandemic as part of their cyber operations. These cyber threat actors will often masquerade as trusted entities. Their activity includes using coronavirus-themed phishing messages or malicious applications, often masquerading as trusted entities that may have been previously compromised. Their goals and targets are consistent with long-standing priorities such as espionage and "hack-and-leak" operations.

Due to COVID-19, an increasing number of individuals and organizations are turning to communications platforms—such as Zoom and Microsoft Teams— or online meetings. In turn, malicious cyber actors are hijacking online meetings that are not secured with passwords or that use unpatched software.

Tips for defending against online meeting hijacking (Source: FBI Warns of Teleconferencing and Online Classroom Hijacking During COVID-19 Pandemic, FBI press release, March 30, 2020):

- Do not make meetings public. Instead, require a meeting password or use the waiting room feature and control the admittance of guests.
- Do not share a link to a meeting on an unrestricted publicly available social media post. Provide the link directly to specific people.
- Manage screensharing options. Change screensharing to "Host Only."
- Ensure users are using the updated version of remote access/meeting applications.
- Ensure telework policies address requirements for physical and information security.

Yours truly,

David S. Barmak, JD, CEO.

www.mednetconcepts.com, info@mednetconcepts.com
Tel: (609) 454-5020, Fax: (609) 454-5021
196 Princeton-Hightstown Road, Bldg. 1A, Suite 1A, West Windsor, NJ 08550

AFFILIATES

Med-Net Compliance, LLC
- Compliance and Ethics Programs
- Compliance/Privacy Officer Mentoring

Med-Net Healthcare Consulting, LLC
- Quality Assurance Performance Improvement Programs
- Administrator/Director of Nursing Mentoring
- Mock Surveys

Med-Net Academy, LLC
- Education Programs
- E-learning
- Webinar
- Videoconference

Med-Net Risk Management, LLC
- Risk Management/Safety Programs
- Administrator/Human Resource Mentoring

Med-Net IPA, LLC
- Managed Care Organization Contracting

NEW COMPLIANCE OFFICER-QUALIFIED CERTIFICATE PROGRAM

Med-Net Compliance, LLC has introduced its Compliance Officer-Qualified Certificate Program to assist in preparing candidates to lead an effective Compliance and Ethics Program according to Centers for Medicare and Medicaid Services (CMS) Phase 3 compliance and ethics requirements.

Upon successful completion of the program's curriculum and examination, Med-Net Compliance will award the Compliance Officer-Qualified (CO-Q) designation to participants. Candidates who successfully complete the NAB approved seven element program, will earn a total of 8.75 CEs.

Candidates for the CO-Q designation are those who include compliance practices as an integral component of current or future professional responsibilities including compliance officers, quality and risk management professionals, healthcare executives, and healthcare professionals with the requisite background.

Candidates must possess academic and professional experience by having a Baccalaureate degree or related education and experience in a healthcare setting or with a provider of services to the healthcare sector.

For more information on the Compliance Officer-Qualified (CO-Q) Program, please go to the Med-Net Compliance website at: https://www.mednetcompliance.com/co-q-program/.

www.mednetconcepts.com, info@mednetconcepts.com
Tel: (609) 454-5020, Fax: (609) 454-5021
196 Princeton-Hightstown Road, Bldg. 1A, Suite 1A, West Windsor, NJ 08550