NEWS & VIEWS

A Complimentary Newsletter from Med-Net Concepts, LLC
and its Network of Independent Affiliated Companies

Volume 5 Issue 3
March 2019

In This Issue:

Med-Net Concepts, LLC

Nursing Homes Are Potential Targets for Protected Health Information (PHI) Breaches

By:
Louise Lindsey, Editor

Most people are familiar with identity theft that seeks to access a bank account or use a credit card to make unauthorized purchases - very serious issues. However, banks and credit card providers have developed effective methods to quickly discover and stop the impact of this type of identity theft. Usually, all it takes to address the threat is to change passwords and issue new debit and credit cards. That doesn't totally alleviate the theft that may have occurred, but it does mitigate the outcome, stop further losses, and heighten awareness about the threat.

An article published by ComputerWorld.com titled "Hackers are coming for your healthcare records-here's why," raises a red flag and gives some alarming statistics about the theft of protected health information (PHI). They report that "medical identity theft due to provider data breaches will impact 1 in 13 patients over five years. A graph showing this impact predicts that in 2019, 7 million patients will be affected, and 1.8 million patients will be the victims of data breaches.

Another study by the Brookings Institution predicted that one-fourth of all data breaches will involve the healthcare sector.

Research by the Identity Theft Resource Center reports that "more data breaches happen in the medical and healthcare industry now than in any other sector, including financial, education, and government."

The *HIPAA Journal* published an article in January 2018 titled, "What is Protected Health Information?" that gives a clear understanding of the term PHI. It reads,

Protected health information is the term given to health data created, received, stored, or transmitted by HIPAA-covered entities and their business associates in relation to the provision of healthcare, healthcare operations and payment of healthcare services. Protected health information is often shortened to PHI, or in

the case of electronic health information, ePHI.

The article also explains that PHI/ePHI-

Relates to the past, present, or future physical or mental health or condition of an individual; the provision of healthcare to an individual; or the past, present, or future payment for the provision of healthcare to an individual that is:

- Transmitted by electronic media;
- Maintained in electronic media; or
- Transmitted or maintained in any other form or medium.

Protected health information includes all individually identifiable health information, including demographic data, medical histories, test results, insurance information, and other information used to identify a patient or provide healthcare services or healthcare coverage. 'Protected' means the information is protected under the HIPAA Privacy Rule.

Why Steal Protected Health Information (PHI)?

Thieves steal PHI/ePHI for several reasons-to receive medical care, buy drugs, or file false claims in order to receive reimbursement from Medicare and Medicaid and other insurers.

Another reason that health data is so tempting to thieves is that it is often easier to obtain than financial information, more valuable on the black market, and can be used longer. Once thieves have access to personal medical information, they can do almost anything with it. For example, with Social Security numbers and dates of birth, a thief can open new credit cards and file fake tax returns. Health insurance information can be used to get medical care and purchase medical equipment and drugs, which can then be sold illegally.

If someone steals another's protected health information (PHI) and uses it to get medical care, it can cause the victim to receive improper treatment because the thief's information gets mixed in with the victim's information.

How Do PHI Breaches Occur in a Nursing Home?

Before looking at how PHI breaches occur in a nursing home, it might be helpful to understand exactly what constitutes a PHI breach.

As identified in HIPAA §164.402 Definitions, the term breach involves-"the acquisition, access, use, or disclosure of protected health information in a manner not permitted under subpart E ... which compromises the security or privacy of the protected health information."

The PHI/ePHI data of nursing home residents can be compromised in a number of ways including:

- Authentication failure or inadequate security software
- Failure of staff to follow procedures
- Lost or stolen laptops, mobile phones, and equipment with PHI data
- Stolen or hacked passwords
- External hackers
- Disgruntled employees
- Employee collusion with identity thieves
- Viruses and worms
- Improper records disposal

The following is an example of a HIPAA data breach involving a business associate who provided management and information technology services to six skilled nursing facilities. The business associate had to pay $650,000 and develop a corrective action plan for combined breaches of 412 nursing home residents. This breach involved the theft of a business-issued employee iPhone that was not encrypted and not password protected. The information on the phone included Social Security numbers, information regarding diagnosis and treatment, medical procedures, names of family members and legal guardians, and medical information. The investigation into the breach discovered that the business associate did not have any policies and procedures addressing the removal of mobile devices containing PHI from its facility or what to do in the event of a security incident. The U.S. Department of Health and Human Services Office for Civil Rights (OCR) also determined that the vendor had no risk analysis or risk management plan.

Thieves seeking PHI/ePHI often don't just try once and go away. In one example, thieves used a phishing attack over several months until they were able to access an employee email account. The email account contained unsecured, breached PHI data that included patient names, Social Security numbers, health insurance information, treatment details, diagnoses, and addresses.

The HIPAA breach notification rule requires healthcare providers and business associates to provide notification

to individuals, regulators, and the media after a PHI breach occurs. However, there are specific guidelines for healthcare providers and business associates to follow regarding reporting of breaches involving unsecured PHI. Questions that need to be answered in determining a reportable breach are:

1. Was there a violation of the privacy rule?
2. Does the violation fit within the breach exception?
3. Is there a "low probability" that the data has been compromised?
4. When in doubt, it is likely safer to report.

If a report is required, the healthcare provider and the business associate must make the required reports to both the individual(s) affected and to the department of health and human services (HHH).

There are specific guidelines for the reports regarding timing and dependent upon the size of the breach. For breaches involving more than 500 persons in a state, the media must be notified within 60 days of discovery. Documentation about the breach is required to be kept for six years, and the breach must be disclosed in the healthcare provider's and business associates' accounting log.

State breach reporting requirements should also not be overlooked.

The HIPAA Breach Reporting Tool (HBRT) may be found at:
https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

For additional information on HIPAA breach notification, visit:
https://www.hhs.gov/hipaa/for-professionals/breach-notification

"Don't Let Fraud Allegations Upset You ... Learn How to Avoid Them Take Med-Net Compliance's NAB Accredited Courses"

Jo Ann Halberstadter, Esq

ADMINISTRATORS TAKE NOTE

Med-Net Compliance, LLC now offers two series of fraud modules with NAB/NCERS CEs on our website. Modules 1-8 offers 3 NAB CEs and modules 9-16 offer 3.75 CEs. All modules provide education on fraud, waste and abuse prevention and offer a combined total of 6.75 CEs for successful completion.

To review the NAB Accredited courses visit our website:
https://www.mednetcompliance.com/med-net-academy/nab-accredited-courses/

All 16 courses on fraud, waste and abuse were developed by Betty Frandsen, our Vice President of Professional Development and her staff.

Med-Net Concepts, LLC Affiliates

Med-Net Compliance, LLC

Med-Net Healthcare Consulting, LLC

Med-Net IPA, LLC

Med-Net Rehabilitation Solutions, LLC

STAY CONNECTED