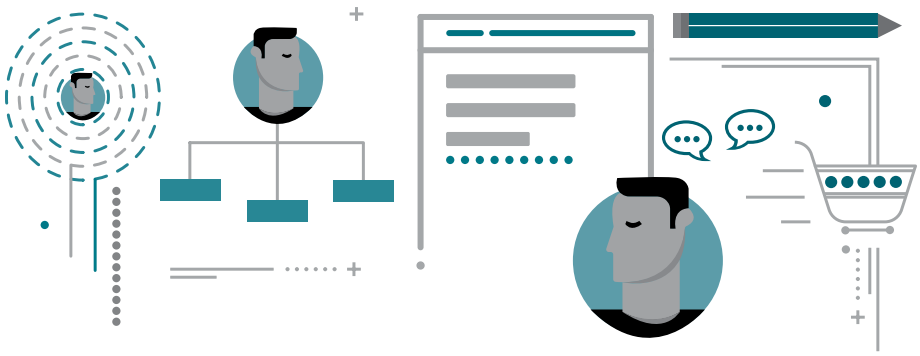
October 2018 – Vol. 34 No. 10
Published for Health Care Providers by ACA International
www.acainternational.org
pulse

Safe and Sound

How well do you understand privacy considerations under HIPAA?

By Anne Rosso May



If your agency collects health care accounts, you need to be familiar with The Health Insurance Portability and Accountability Act (HIPAA.)

HIPAA privacy laws were put in place to safeguard consumers' protected health care information, or PHI. HIPAA governs how you access, distribute and protect PHI, and failure to comply can result in huge consequences, not only for your company, but for you, personally. While there is no private right of action under HIPAA, Health and Human Services can take action against those who violate HIPAA and consumers can file complaints with them for HIPAA violations.

In 2010, for instance, a doctor who accessed medical records without a valid reason was fined $2,000 for violating HIPAA and sentenced to four months in prison. And in 2015, a lab employee at a student health center was fired after she mentioned the results of a patient's pregnancy test to a coworker.

What is PHI?

As a debt collector, you are expected to help protect consumers' sensitive and confidential health care information. Anything that could be used to identify consumers in relation to their health care information is considered PHI. This can include a person's name, address, phone number, medical history, insurance details and health care bills.

How Can You Protect PHI?

Don't discuss information in the consumer's file with anyone but the consumer—unless the consumer has given you permission to do so. This includes idle chit-chat with co-workers, even if you don't mention the consumer's name.

Sometimes a situation may call for you to contact the consumer's insurance company or you may get an information request from an attorney. Before you email, fax, mail or discuss PHI with third parties, ask yourself: Do my company's rules authorize me to do this? If so, has the consumer consented to the PHI release under HIPAA, and will the information I send be encrypted? (Email in particular is an often-overlooked PHI disclosure risk because it might not be secure.)

Although the Fair Debt Collection Practices Act allows you to communicate with a consumer's spouse, parent or guardian, HIPAA may not. If consumers request that they do not want certain people, such as family members, to have knowledge of their situation or condition, you can't disclose any health information to third parties.

How Should You Store PHI?

While your company is responsible for securing its computer system and designing its collection notices to protect PHI, you also play a key role in this process. Don't leave consumer

continued on page 2

DATA SECURITY

Data Breach Risks Continue in the Health Care Industry

Data breaches in health care are becoming "routine" with millions of patient records affected in the second quarter this year, according to the quarterly Breach Barometer report from Protenus, a data analytics firm specializing in patient privacy.

> More than three million patient records were impacted by a data breach in the second quarter.

From April to June 2018, there were 143 data breach incidents reported to the U.S. Department of Health and Human Services (HHS) or the media. Details provided for 116 of the 143 incidents show they impacted more than 3.1 million patient records, according to the Protenus report.

This is almost triple the patient records impacted in the first quarter (1.13 million.)

Protenus also finds that 29.71 percent of privacy violations resulting in a data breach were repeat offenses.

"On average, if an individual health care employee breaches patient privacy once, there is a greater than 30 percent chance that they will do so again in three month's time, and a greater than 66 percent chance they will do so again in a year's time. In other words, even minor privacy violations that are not promptly detected and mitigated have the potential to compound risk over time," according to the report.

Investigators also have a difficult time keeping up with the volume of "insider threats" when it comes to patient data. In fact, due to the volume of electronic access to health care data at hospitals and other providers on a daily basis, one investigator monitors an average of nearly 4,000 employees.

The average number of employees with privacy violations increased from 5.08 per 1,000 in the first quarter to 9.21 in the second quarter.

Whether inadvertent or intentional, these internal violations are a big risk to patients' privacy. And, employees in the health care industry are often looking for information on people they know when they commit a violation.

Approximately 71 percent of insider-related breaches in the second quarter included employees accessing records on their family members, according to the Protenus report.

Outside of internal risks, hacking continues to lead to data breaches. Hacking incidents nearly doubled in the second quarter with 52 reported between June and April.

Health care providers and their business associates, including third-party debt collectors, need to know the privacy rules and take care when accessing patient data, whether medical or financial, to avoid violation of the Health Insurance Portability and Accountability Act (HIPAA.)

Twenty six incidents reported in the second quarter involved business associates or third-party vendors working with health care providers, affecting nearly 800,000 patient records, Protenus reports.

As data security risks in health care increase, consumers are increasingly anxious about their privacy as well. A recent survey shows almost half of U.S. adults participating are "extremely or very concerned about their health care data security, such as diagnoses, health history and test results," according to healthsecurity.com.

So what can providers and their business associates do to get ahead of data security risks and protect their systems, patients and consumers?

Protenus reports best practices are critical for organizations that allow an audit of every employee's access to patient data. "Full visibility into how their data [are] being accessed and used will help organizations secure patient trust while preventing data breaches from having costly consequences for their organization."

Read the complete Breach Barometer report from Protenus here: https://bit.ly/2OYOmmW. See Data Watch for a graph from this report.

Safe and Sound *cont. from page 1*

information on your computer screen when you're not at your desk, even if you just get up for a minute to get a drink of water.

Only print out documents containing PHI when you have a legitimate business reason to do so, and even then, you'll need to dispose of those papers in a secure environment—a shredder your company uses for such a purpose, for example, not the day-to-day recycling bin by your desk.

Even written notes you leave on your desk referencing PHI can be considered a HIPAA violation, so either avoid doing this altogether or use HIPAA as good motivation to keep your desk clean and free of clutter, safely disposing of these written reminders as soon as possible.

Anne Rosso May is editor of Collector *magazine. To try out ACA's new computer-based training program, HIPAA Essentials for Collectors, visit* www.acainternational/shop.

COSTS

Are Health Care Costs Affordable to Most Americans?

Many Americans are struggling to cope with the rising cost of health care. Recent findings by The Commonwealth Fund show that Americans' confidence in their ability to afford their health care continues to deteriorate as the cost of health care escalates.

This year, 62 percent of adults told The Commonwealth Fund they were confident they could afford their health care if they became ill or injured, down from 70 percent in 2015. Nearly one in four Americans said health care had become harder to afford.

"Uninsured adults are the least confident in their ability to pay medical bills," the report found. "But the risk of high out-of-pocket health care costs doesn't end when someone enrolls in a health plan. The proliferation and growth of high-deductible health plans in both the individual and employer insurance markets is leaving people with unaffordable health care costs."

The group with the most confidence about their health insurance and the ability to pay for an unexpected medical bill are people with employment-based health plans; the least confident group included those enrolled in Medicare and people with preexisting medical conditions.

Unexpected medical bills can take a toll on both uninsured and insured Americans. The percentage of consumers not paying their hospital bills in full has increased in recent years, according to an analysis from TransUnion Healthcare. Since last year, approximately 68 percent of consumers with medical bills of $500 or less did not pay the total balance, an increase from 53 percent of consumers in 2015 and 49 percent in 2014.

"There are many reasons why more patients are struggling to make their health care payments in full, the most prominent of which are higher deductibles and the increase in patient responsibility from 10 percent to 30 percent over the last few years," said Jonathan Wiik, principal for health care revenue cycle management at TransUnion.

TransUnion health care also projects these challenges could continue in the future, speculating that the percentage of consumers not paying their total hospital bills will increase to 95 percent by 2020.

"With millions of dollars in unpaid medical debt, hospitals have begun implementing new processes to prevent revenue leakage while also providing a better patient experience," said John Yount, vice president for health care products.

More information: https://bit.ly/2MxTxxy

NEWS & NOTES

CMS Finalizes Rule Including Price Transparency Initiatives

The Centers for Medicare and Medicaid Services is advancing a rule designed to improve access to hospital price information, give patients greater access to their health information and allow clinicians to spend more time with their patients. One component of the rule focused on value-based care and reducing administrative workloads at hospitals requires health care providers to publish costs and policies for price transparency online. https://go.cms.gov/2nAL2mp

Study: Why Do Consumers Use Out of Network Providers?

Nearly 18 percent of inpatient admissions for consumers with health insurance coverage from their employer are with out of network providers, which may increase their costs. Why do consumers have care from out of network providers? The Kaiser Family Foundation analyzed employer plans to find out. One reason is consumer preference; however in some cases they may not have a choice in their care provider, such as treatment in the emergency room. https://kaiserf.am/2BJy2of

We Want To Hear From You

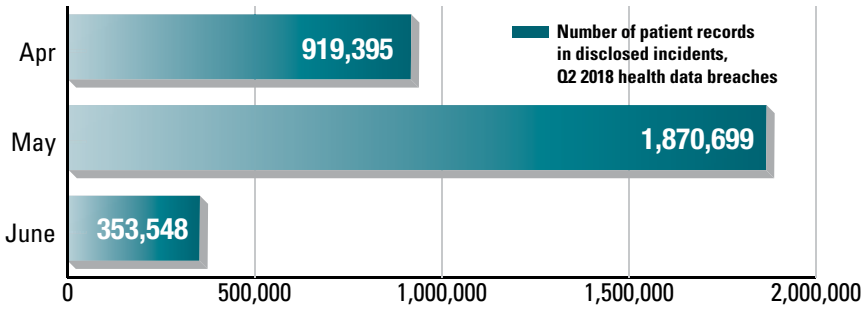
Pulse is published for ACA health care collection agencies to provide current industry information for health care providers. ACA International welcomes article ideas and submissions for consideration in *Pulse* to the Communications Department at comm@acainternational.org.

For more health care collections news, visit ACA's Health Care Collections page at www.acainternational.org/pulse.

datawatch

Patient Records Impacted by Data Breach Incidents

Millions of patient records were disclosed in data breach incidents in the second quarter of 2018, according to the quarterly Breach Barometer report from Protenus, a data analytics firm specializing in patient privacy. In May 2018 alone, more than 1.8 million patient records were part of disclosed data breach incidents, compared to about 919,000 in April.



Source: Protenus https://bit.ly/2OYOmmW

pulse is a monthly bulletin that contains information important to health care credit and collection personnel. Readers are invited to send comments and contributions to:

Communications Department
ACA International
P.O. Box 390106
Minneapolis, MN 55439-0106
comm@acainternational.org

Note: Requests for reprints or additional information on material herein must be made through the ACA International member who sponsored your receipt of this publication.

Do we have your correct name, title and address? Please advise your sponsor of any corrections.