THEADVIS☀R
MONTHLY COMPLIANCE COMMUNICATOR

BREACH SHOULD BE A FOUR-LETTER WORD

Most every day it seems a new report emerges about an organization that has been compromised. Big names such as Equifax, Neiman Marcus, Target and Home Depot have all made the dreaded announcement of a data breach and even a local Dunkin Donuts franchise announced that their patron's information had been inappropriately accessed. The healthcare community is not immune. In 2015, Anthem announced one of the largest breaches on record, impacting 78.8 million individuals. Through mid-November of this year, 274 breaches impacting 500 or more records are under investigation according to the Health and Human Services (HHS) website.

Making sure the definition is clear, breach is defined by Health and Human services as an impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of the protected health information.

Examples of breaches include:

- leaving inappropriate or excessive information on voicemail without the patient's permission

- mailing a financial statement to the wrong address

- losing a box of medical records or films in route to a storage facility

- loss of a computer with data that has not been encrypted

- a hacking incident impacting electronic health information

One of the challenges related to breaches in healthcare is that workers may not be aware of the significance of a data breach. Workers seem to understand that inappropriate sharing of a sensitive diagnosis, such as cancer or HIV, is not allowable and accessing health information for curiosity will lead to discipline. However, a data breach can easily lead to the risk of both medical and financial identity theft. **Information included in most health records may be used against the patient if obtained by criminals.**

CLICK HERE TO
START YOUR TRAINING TODAY!
HIPAA OSHA INFECTION CONTROL BUSINESS ASSOCIATES

TMC HIPAA COMPLIANCE

BREACH SHOULD BE A FOUR-LETTER WORD

Continued from page 1

Protection of patient information, especially information stored electronically (ePHI) is imperative. While focusing on protection of health information stored electronically is important, entities must also be diligent in protecting any patient information that is included in any type of hard copy format, such as financial information, copies of hard copy medical records and hard copy radiographs.

When thinking about the protection of patient information don't forget information shared with business associates. A business associate is a person or entity, other than workforce members of a covered entity, who is provided or allowed access to protected health information (PHI) in order to perform a function or activity for the covered entity. It is critical for covered entities to ensure that PHI is protected in any business associate relationship. A written agreement, referred to as a Business Associate Agreement, is required. In addition to the form, ask your business associate how they protect any information provided to them. The reality is that if a breach such as the data breach of 2 million patient records reported by a large healthcare organization recently, occurs on the business associate's watch, the covered entity is ultimately responsible for the communication of the breach.

A key element in a strong HIPAA compliance program is the protection of health information. It must be kept confidential and available, so the integrity of the information is intact. Consider the following strategies to protect patient information in hard copy and electronic format.

- Train all workers on the importance of the security of electronic health information.

- Develop a strong working relationship with a reputable IT individual/business.

- Establish appropriate safeguards that include antivirus protection and software updates.

- Allow access to the internet for work purposes only.

- Only open emails from known sources. Do not click links in email.

- Prohibit access to personal social media accounts.

- Use strong passwords and do not share them.

- Lock or log off computers or electronic devices when they are unattended.

- Establish physical security for computers, especially mobile devices, and servers.

CLICK HERE TO
START YOUR TRAINING TODAY!

HIPAA OSHA INFECTION CONTROL BUSINESS ASSOCIATES

TMC HIPAA COMPLIANCE

TotalMedicalCompliance.com

BREACH SHOULD BE A FOUR-LETTER WORD

Continued from page 2

Are you comfortable that your business is well positioned to prevent a breach of protected health information? About that four-letter word? STOP comes to mind! By implementing the strategies listed above it is possible to STOP many breach events.

Do you want to learn more about HIPAA topics in general? Go to our TMC complimentary webinar page and you will find several recorded webinars on HIPAA and many other compliance topics.

What does this pictogram stand for?

Last Chance to Win a Cash Gift Card: Fun with GHS!

Is everyone in your practice current on the United Nations Globally Harmonized System of pictograms that communicate hazardous chemicals? We've enjoyed receiving all of the **Fun with GHS** entries, but we're at the end of the gift card giveaway. This month is your last chance to identify a GHS pictogram and enter to win the drawing. This is also when we will have our big end-of-the-year drawing for the grand prize! Click here to enter by December 30th for your chance to win this month! We will let you know our December winner and our big year end winner in the January newsletter.

Last month our pictogram was compressed gases. Many got it right, but we had to pick only one winner and it was Cortney W. of North Carolina. Congratulations Cortney!

CLICK HERE TO ENTER

CLICK HERE TO
START YOUR TRAINING TODAY!
HIPAA OSHA INFECTION CONTROL BUSINESS ASSOCIATES

3

TMC HIPAA COMPLIANCE

PROTECT YOURSELF

Credit cards and debit cards are becoming the mainstay of consumer purchasing. In fact, in 2016 credit cards became the primary method of payment for consumers in the US. Whether on the phone, online, or when processing transactions face to face, special attention should be paid to reduce the risk of credit card theft and fraud to protect our customers and our organizations.

There are two types of card transactions: card present and card not present. Today we will focus on the later and review simple ways to protect our customers in card not present scenarios.

As the name implies, card not present (CNP) means the card is not physically present at the time of the transaction. Common scenarios include payments submitted via mail or taken over the phone. CNP has a unique set of challenges that we need to be mindful of.

1. Do not store credit card information outside of officially sanctioned processes or applications. These authorized systems have been reviewed to make sure they are secure. Do not create personal spreadsheets or notes to retain this information.

2. Card security codes (the 3- or 4-digit code on the back of the card) are designed to ensure the consumer is in physical possession of the card. Be sure to follow your organization's processes to utilize this extra protection.

3. When processing transactions, purge the data as soon as possible. This might include shredding fax reports or payment stubs.

Be mindful of the aggravation and disruption that credit card fraud can cause consumers. This sort of theft is growing.
Let's do our best to make sure this doesn't happen to our customers.

CLICK HERE TO
START YOUR TRAINING TODAY!
HIPAA OSHA INFECTION CONTROL BUSINESS ASSOCIATES

4

TotalMedicalCompliance.com

NEW OSHA REGULATIONS ON ILLNESSES & INJURIES

OSHA announced new regulations for reporting workplace illnesses and injuries in 2016. The implementation was delayed by the change in presidential administration but is now in effect. This is a two-part change. Part one involves reporting illnesses and injuries to OSHA electronically each year. Part two covers changes in the policies and procedures needed to ensure employees report their illnesses and injuries without fear of negative consequences.

Part one will not affect most of our readers. Currently employers who have 20 or more employees must post a copy of their OSHA 300A report (Summary of Work-Related Injuries and Illnesses) in their office. The change requires them to post it electronically as well, minus the employee names. OSHA plans to use this data to better ensure employee safety and will post the data on a public website.

The requirement for employers with 250 or more employees has been deleted.   In addition to the 300A report they must also electronically post the back-up documents (OSHA Report 300 and 301).

There are three ways you can be exempted (or partially exempted) from electronic reporting. You still must keep records on all injuries and illness incidents and be able to produce them if requested by OSHA, even if you are exempt from filling out and posting these reports.

1. If you have 10 or fewer employees, you are exempt from keeping or posting these reports.

2. If you have 11-19 employees, you still must post the 300A Report in your office annually but you are exempt from electronic posting.

3. If your industry is listed in Appendix A of Federal Regulation 1904 as one that is partially exempt, you do not have to produce these reports or post them, therefore you do not have to follow the electronic posting regulations.

"Partially exempt" means you are exempt, but OSHA can write you and require that your business participate in a survey that usually lasts from 1 to 3 years.

TMC OSHA COMPLIANCE

NEW OSHA REGULATIONS ON ILLNESSES & INJURIES

The following is a list of pertinent "partially exempt" industries by NAICS code.

- 4461 - Health and personal care stores

- 6211 - Offices of Physicians

- 6212 - Offices of Dentists

- 6213 - Offices of other health practitioners

- 6214 - Outpatient Care Centers

- 6215 - Medical and Diagnostic Laboratories

- 8122 - Death Care Services

Healthcare industries that are not on the partially exempt list include all residential facilities like hospitals, nursing care, drug treatment, psychiatric, and code 6219-Other Ambulatory Healthcare Services.

The new regulations do not change the fact that all businesses, with no exceptions, must report any catastrophic work-related illnesses or injuries to OSHA. A death must be reported within 8 hours and hospitalization, loss of limb or eye must be reported within 24 hours. The following link can be used for catastrophic reporting.

https://www.osha.gov/report.html

Part two of the new regulations involves changing policies and procedures to ensure that employees understand the importance of reporting work-related illnesses and injuries, understand how to report and feel safe from any negative consequences of reporting. These changes apply to all businesses.

Next month's OSHA article will discuss these changes. If you are a TMC OSHA client, these new policies and procedures for these regulations are already in your manual.

CLICK HERE TO
START YOUR TRAINING TODAY!

6

HIPAA OSHA INFECTION CONTROL BUSINESS ASSOCIATES

GETTING TO KNOW TMC EMPLOYEES

This month we are pleased to introduce you to Diane Eaton, one of our Client Service Support Team Representatives. Diane has a BA from George Mason University and has experience in the Washington, DC area in broadcasting and legal offices. She has enjoyed working with our clients as part of the Client Services Support Team since 2008.

1. What is your must-have or go-to morning beverage? Coffee with milk and lots of sugar
2. What is the most fun or unusual item you keep on your desk? A statue of Olaf from "Frozen" that I got for giving an answer at one of our Annual Meetings.
3. What is the strangest or most fun job you've ever had? In college I worked for a real estate company and got paid $10 plus dinner to get people to visit a resort that sold condos on Chincoteague Island in Virginia. I was not terribly successful, but the dinners were good.
4. How far away from home is the farthest away you've ever been? Well the farthest away in spirit as well as physically was probably the Middle East. I was born in Beirut, Lebanon and lived in other places in the Middle East until we came back to the States when I was 13.
5. What is your go-to item that you most often bring to potlucks? Tabouleh
6. Where is your favorite place to listen to music? My house. I listen to Punky Meadows (my husband) play the guitar every night.
7. What is the last movie you saw in a movie theatre? We fix popcorn and watch movies every Sunday at home. The last one was "Den of Thieves."
8. Do you have any phobias? Heights, small spaces and spiders.
9. What is the most daring thing you've ever done? I learned how to fly a plane.
10. Do you collect anything? I collect everything!
11. Do you (or would you) sing at Karaoke night? OMG no!
12. Are you related (even distantly) to anyone famous? If you look up Punky he's on Wikipedia!
12. What is your favorite holiday? Thanksgiving
13. What was the last non-work-related thing you read? I read murder mysteries all the time!
14. Is your glass half-empty or half-full? I'm a half-full kind of person.

IT'S YOUR CALL

OSHA Situation:

We have a broken fluorescent light bulb. I've heard this is an issue, but why?

HIPAA Situation:

We had an elderly patient in the office who appeared to have been abused. They had a healthcare power of attorney and asked for a right to access the medical records. Can we release the abused patient's information?

CLICK HERE FOR THE ANSWERS

CLICK HERE TO
START YOUR TRAINING TODAY!

HIPAA OSHA INFECTION CONTROL BUSINESS ASSOCIATES

THEADVISOR
MONTHLY COMPLIANCE COMMUNICATOR

SIGNATURE	PRINT	DATE

1. _____
2. _____
3. _____
4. _____
5. _____
6. _____
7. _____
8. _____
9. _____
10. _____
11. _____
12. _____
13. _____
14. _____
15. _____
16. _____
17. _____
18. _____
19. _____
20. _____
21. _____
22. _____
23. _____
24. _____
25. _____

INSTRUCTIONS

Print and post newsletter in office for staff review. Each member should sign this form when completed. Keep on file as proof of training on these topics.

IN THIS ISSUE