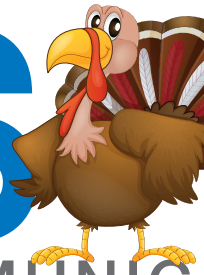
TMC
TOTAL MEDICAL COMPLIANCE

888.862.6742
www.totalmedicalcompliance.com

NOV 2019

THE ADVISOR



MONTHLY COMPLIANCE COMMUNICATOR

WHAT'S YOUR DATA WORTH?

The cost of a healthcare data breach

It is difficult to argue that technology has not improved our lives and businesses in many ways. On the other hand, it's just as difficult to argue that technology advancements are not without some very serious risks. IBM's 2019 *Cost of a Data Breach Report* illustrates the fact that the healthcare industry is the most expensive industry in which to experience a data breach. It can be catastrophic to a healthcare provider, hospital system, or healthcare service provider. No industry is immune, and prevention and detection require constant attention from humans as well as technology. In IBM's report, the average cost of a data breach is $3.9 million. However, the healthcare industry exceeds all other industries by 65% at $6.45 million average total cost per data breach. Unfortunately, that means that a data breach can often cripple or even close a small to medium sized business.

Costs are affected by the type of industry, the cause of the breach and the cost of notifying patients and regulatory authorities. Heavily regulated industries like finance and healthcare face potential fines and increased reporting requirements. A cost that is difficult to quantify, though, is the potential loss of new business as well as existing patients/customers during and after a breach. Small businesses must rely on other companies or consultants like IT support and attorneys, which can cause response times to drag as well as increase overall cost. The residual impact of a data breach can be felt for up to two years after its occurrence.

Continued on Page 2

IN THIS ISSUE

What's your data worth?
PAGE 1 - 2

It's Your Call
PAGE 2

Ransomware
PAGE 3

Stop the spread of Infection
PAGE 4 - 5

Did You Know?
PAGE 6

November Breaches by the Numbers
PAGE 7

Sign-in sheet
PAGE 8

HIPAA COMPLIANCE

Continued from Page 1

SAFETY MEASURES

It can be overwhelming to think about the many components that might keep your practice safe from a breach and recovering from one when it happens. For small businesses, three things that will have the greatest impact on prevention, detection, and mitigation are:

1) employee training
2) encryption of data in transit and saved on servers, and
3) a contingency plan.

Set a date to review the plan with key employees at least once per year. It should also be reviewed when any technology or facility changes occur.

It is human nature to avoid thinking about and planning for unpleasant events, but a good plan of prevention, detection, and mitigation is well worth the investment when one happens.

IT'S YOUR CALL

OSHA Situation:
Some offices are partially exempt from maintaining OSHA injury and illness records. How can I find out if our office is exempt?

HIPAA Situation:
When should a Business Associate Agreement (BAA) be executed and what are the fines if the BAA is not available?

CLICK FOR ANSWERS

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

HIPAA COMPLIANCE

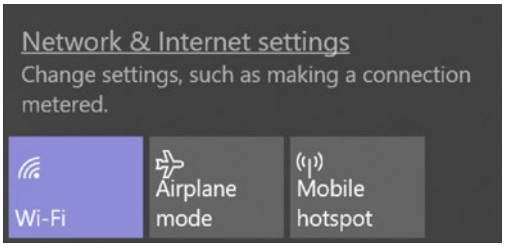
RANSOMWARE

The rise of ransomware and its increased impact on small to medium sized organizations can keep most business owners and security professionals awake at night. Ransomware is a form of malware where a hacker gains access to a business's data, encrypts it, and demands payment for the access code for the organization to recover the data. The outcome is never certain, though. Even if the ransom is paid, many hackers still steal and/or delete the victim's data, rendering all of the victim's data lost. In many cases that data is its most valuable asset.

The U.S. Department of Health and Human Services (HHS) reports that 58% of malware victims are small businesses. HHS advises that in the event of a ransomware attack, DO NOT turn the computer off or unplug it. DO disconnect it from your network and internet connection.

The reason for this is so that valuable forensic information can be retained on its hard drive. If a computer is connected wirelessly, disable the Wi-Fi. Go to your computer's settings or find the wireless icon in your toolbar. If the computer is connected by an ethernet cable, disconnect the cable from the machine. Ethernet cables are usually blue and look like a large phone connector.

Preventative measures are an effective antidote. Regularly back up your practice's data. Test it with your IT support to be sure that it can be restored without error in the event of a disaster or ransomware attack. Ensuring employees are aware of the ways an attacker might gain access to your practice's systems can also reduce the likelihood of a security incident or data breach. The most effective defenses include reminding employees to avoid clicking on links, downloading attachments in emails, and to verify that a recipient of protected health information is legitimate before sending.



Check your network and internet settings for security.

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

INFECTION CONTROL

STOP THE SPREAD OF INFECTION:

Three things to know

There are many processes which must be followed in order to break the chain of infection and prevent susceptible individuals from becoming ill. The individual could be the patient or the worker. In order to reduce the likelihood of spreading infection, remember these three important concepts.

1. **First Do No Harm** – Patient safety must always be at the forefront of each patient encounter. Have you posted the Cover Your Cough posters yet? We are entering the time of the year where there will be an increase in respiratory illness and it is important to protect all patients while they wait for their appointment.

2. **Standard Precautions** – These provide the baseline to reduce the spread of infection to workers and patients. When used in combination, the risk of spreading infection decreases. Take the following actions when providing patient care:
   - Wash hands prior to providing care, after touching a patient or a contaminated surface, and after removal of personal protective equipment (PPE).
   - Utilize PPE in every situation where there is potential exposure to blood, body fluid, or respiratory secretions. The selection of PPE should be based on the risk of exposure to the worker. For instance, if there is the likelihood of a splash to the eyes, nose, or mouth, use a mask and safety glasses to protect the face.
   - Disinfect surfaces with a hospital level surface cleaner/disinfectant. Follow the manufacturer's directions for both contact time and the use of appropriate PPE. Establish a cleaning schedule based on the tasks performed and the potential for contamination during patient care.

Continued on Page 5

STOP THE SPREAD OF INFECTION

Continued from Page 4

3. **Instrument processing** – Your processes should meet the national standards outlined by the CDC and the Association for the Advancement of Medical Instrumentation (AAMI). Depending on the type of instrumentation being processed in your facility, there may be other organizational guidelines that must be considered. Patients should never wonder about the sterility of the instruments being used for a procedure. As a best practice, packages should be opened in front of the patient when the procedure is to begin. There are several other important items to remember when managing instrumentation used for procedures.

   - Single use items are designed to be used for one patient during one procedure. The item must be discarded after use; never disinfected or sterilized for reuse.
   - Dental practices should consider disposable tips for air/water syringes. Any non-disposable instrument which enters the patient's mouth must be cleaned, packaged and sterilized after patient use. This includes metal impression trays and mouth mirrors which can withstand the sterilization process.
   - Utilize heavy duty utility gloves when handling contaminated instruments. These gloves may be reused, but should be surfaced disinfected or washed with soap and water after each use. Some gloves have the ability to be sterilized on a routine basis, but follow manufacturer's direction to protect the integrity of the gloves.
   - Equipment utilized for processing instruments such as an ultrasonic cleaner or washer disinfector must be cleared by the FDA. Always follow manufacturer's recommendations for cleaning, maintenance, and use of the equipment.
   - Monitoring of the sterilization process includes the use of internal and external chemical indicators in each package and spore testing as a general rule each week and with implantable items.

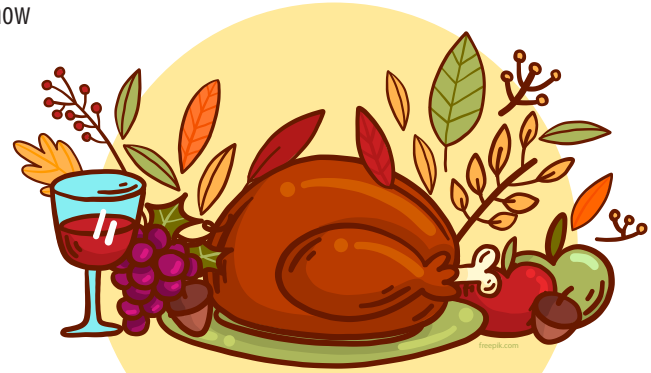
This list includes several important concepts which if implemented will create a culture of safety and reduce the likelihood of spread of infection. Take the time now to compare these recommendations to the activities in your practice and make any necessary corrections for a safe environment for patients and staff.

DID YOU KNOW?

"I yam what I yam and dats all what I yam."

– Popeye the Sailor Man

Many families will be serving candied yams with Thanksgiving turkey. Did you know that the yams you buy in the grocery store, are actually sweet potatoes?



Yams and sweet potatoes are not even distantly related. They are in two different botanical families. Although the terms are generally used interchangeably, the US Department of Agriculture requires that the label "yam" always be accompanied by "SweetPotato."

More Fun Yam Facts:

- There are about 600 species of yam. Many are poisonous, but about 150 species are cultivated for food.
- Yams have been used throughout history for medicinal purposes. They were used commercially to produce hormones for contraceptive pills, and steroids in the 1960s.
- Yams can grow to huge sizes. The water yam cultivated in Southeast Asia, grows up to 8 feet long and can weigh over 100 pounds.
- Yams are a daily staple food for more than 60 million people in Africa. The Global Crop Diversity Trust wants to collect 3,000 yam samples to preserve biodiversity in the African "yam belt."

For more information, check out these links:
http://www.foodreference.com/html/fyams.html and
http://www.foodreference.com/html/art-sweet-potato-yam.html
from the North Carolina SweetPotato Commission.

BREACHES BY THE NUMBERS

Although breach numbers for 2019 still soar above 2018, October 2019 saw an improvement over October 2018 in the number of individuals impacted by breaches filed with DHHS Office for Civil Rights (OCR). However, there was a 75% increase in the number of breaches reported this October over October 2018. Social engineering is still the leading cause of breaches which is indicated in the number of breaches from emails and unauthorized access/disclosures in the table below.

Note: These figures do not include any 2019 breaches that involved fewer than 500 individuals. A covered entity must notify the Secretary of a PHI breach affecting fewer than 500 individuals within 60 days of the end of the calendar year in which the breach occurred.

The table below compares the first ten months of 2018 to the first ten months of 2019.

	2018 Jan - Oct Totals	2019 Jan - Oct Totals	2019 % Jan-Oct increase	Oct 2018	Oct 2019
Number of individuals affected	6,093,930	39,271,407	544%	1,953,546	212,885
Number of reports	133	340	133%	16	28
Covered Entities	110	306	178%	13	24
Business Associates	26	77	196%	3	4
Type of breach					
Hacking/IT incident	68	203	199%	9	13
Improper media/equipment disposal	3	4	33%	0	1
Loss or theft	20	37	85	1	2
Number of unauthorized access/disclosure	42	95	126%	6	12

TMC
TOTAL MEDICAL COMPLIANCE

888.862.6742
www.totalmedicalcompliance.com

NOV 2019

THE ADVISOR

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

What's your data worth?
PAGE 1 - 2

It's Your Call
PAGE 2

Ransomware
PAGE 3

Stop the spread of Infection
PAGE 4 - 5

Did You Know?
PAGE 6

November Breaches by the Numbers
PAGE 7

Sign-in sheet
PAGE 8