TMC
TOTAL MEDICAL COMPLIANCE

888.862.6742
www.totalmedicalcompliance.com

JUNE 2021

THE ADVISOR

MONTHLY COMPLIANCE COMMUNICATOR

The Recognized Security Practices Safe Harbor and the OCR

It is hard going a day without seeing a cybersecurity attack in the headlines. Over the past year and a half, the number of attacks has increased by over 350%. Healthcare entities of all sizes are an enticing target for attackers because just 1 patient record can fetch $200 or more on the dark web. If a hacker steals a practice's entire patient database, it adds up to a very nice payday. Avoiding a cyberattack like ransomware, and the increasing costs to recover and repair the damage to your business's reputation is a huge incentive to ensure you have appropriate security policies, procedures, and technical controls in place.

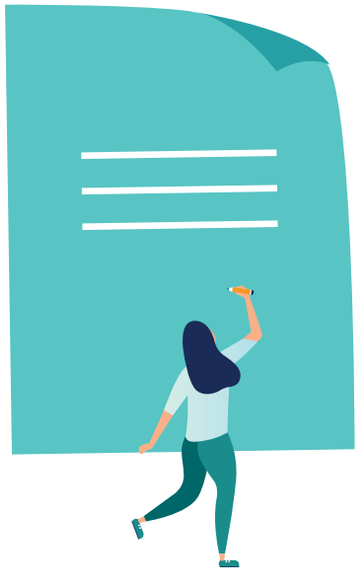
Continued on Page 2

IN THIS ISSUE

HIPAA COMPLIANCE

Continued from Page 1

A new incentive referred to as the Safe Harbor for Recognized Security Practices was signed into law earlier this year. The OCR's regional offices are required to investigate all reported breaches involving the PHI of 500 or more individuals. They have the option to investigate smaller breaches too. When the OCR investigates a breach, the entity under investigation has the opportunity to show that it has had recognized security practices in place for (at least) the past 12 months. If they do, the safe harbor law requires the OCR to consider a lower penalty and lessen the severity of other methods of enforcement, such as a corrective action plan. The length of time of the investigation and its depth or level of detail must also be reduced. These new requirements could potentially save a provider or business associate a lot of time, money, and worry.



What are recognized security practices? The safe harbor law provides two examples and a general definition. Basically, any security practices that have been developed from or recognized by laws, regulatory agencies, and official guidance meet the requirement. Neither the HIPAA Rules nor the OCR require a particular source or program to follow for security practices. Security practices include things like ensuring passwords are long and complex, keeping an accurate inventory of hardware and software that handle PHI, performing an annual risk analysis and training employees when hired and annually. Guidelines published by the National Institute of Standards and Technology (NIST) are specifically referenced in the safe harbor law and the OCR provides educational material and links to the NIST Cybersecurity Framework and its other guidance on implementing the HIPAA Security Rule on its website.

The safe harbor law provides two examples and a general definition. Basically, any security practices that have been developed from or recognized by laws, regulatory agencies, and official guidance meet the requirement.

Continued on Page 3

HIPAA COMPLIANCE

Continued from Page 2

Another perk of the safe harbor law is that the OCR cannot increase fines or penalties if the security practices an entity has in place meet the standards of the HIPAA Security Rule but are not part of a specific program or from a particular organization. In other words, you can mix and match any practices that meet the standards of the HIPAA Security Rule.

It is important to remember that there is no such thing as HIPAA Certification or being "HIPAA Certified." The Office of the National Coordinator for Health Information Technology (ONC) certifies technical specifications in EHR software, but no other area of HIPAA compliance has an official certification by a government agency. Endorsements by commercial programs show an entity's practices meet the standards of that program. They cost money and require ongoing fees to continue using the endorsement. Your IT service provider is a business associate and required to comply with the HIPAA Security Rule, Breach Notification Rule, and parts of the Privacy Rule. They can support the technical component of your HIPAA compliance program.

Total Medical Compliance gives clients the tools and first-class support to help comply with the HIPAA Rules and training requirements. TMC's policies, procedures, forms, and guides are kept current to reflect changes to rules and regulations. Clients receive customized support during audits, investigations, and breaches.

It is important to remember that there is no such thing as HIPAA Certification or being "HIPAA Certified."

Managing an Exposure Event

Performing certain procedures during the delivery of healthcare can increase risk of exposure to blood, bloody secretions, or other body fluids. Once an exposure occurs, fast action is required on the part of many people in the practice. Successful management requires preplanning and education of all staff at risk.

Addressing prevention is always important in the over-all review. Prevention must be at the top of your priority list and should include training on the appropriate use of personal protective equipment, use of engineering controls including safety devices, and appropriate surface disinfection. Worker safety should be a part of the culture in every practice and as such may lead to the prevention of an exposure event.

Potential routes of exposure include:

- Stick with a contaminated needle.
- Stick with a contaminated sharp object, for example, scalers, surgical instruments, or scalpel blades.
- Splash to the mucous membranes of the eyes, nose, mouth.
- Splash to non-intact skin.

Once the exposure occurs the clock literally starts ticking. Employees MUST know the correct measures to take, and how and to whom to report the incident. Your practice should have a health care provider identified in advance who can provide an immediate medical evaluation and counseling of your worker and testing of the source patient.

Continued on Page 5

OSHA COMPLIANCE

When establishing this relationship, consider the following items in your selection process:

- Ease of access for both the worker and the source patient.
- Potential wait times prior to being seen.
- Ability to obtain the rapid HIV test for the source patient.
- Availability of post exposure medication if indicated for the employee.

Source Patient Testing Process: Practices must have a process identified for source patient testing. After informing the patient of the exposure, immediate access to care is necessary. In some states post exposure testing of the source patient is required by law and written consent is not required, while in other states, the source patient may be allowed the leeway to decline testing. The test results of the source patient are critical in assisting the healthcare provider in determining the plan of care for the exposed worker.

Based on CDC guidelines, the following tests will be ordered by the provider for the source patient unless already known to be infected. The testing recommendation for the hepatitis C virus was changed by the CDC in July of 2020.

1. HIV Antibody: A rapid HIV test will be used if available. If rapid HIV is not available, expedite the HIV test.
2. Hepatitis B Surface Antigen (HBsAG): Source patient testing is not indicated if exposed worker has documented serologic evidence of hepatitis B immunity.
3. Hepatitis C: Nucleic acid test for HCV RNA. (MMWR: July 24, 2020)

The results of the source patient tests will be reviewed by the ordering provider. If requested by the source patient, forward the results to other providers.

As a reminder, *the cost of all source patient testing is the responsibility of the practice.*

Continued on Page 6

OSHA COMPLIANCE

Continued from Page 5

Care of the Exposed Employee

The employee should immediately wash the affected area with soap and water or flush the mucous membranes with copious amounts of water. As soon as the first step is completed the event should be reported. Follow these steps for the benefit of the exposed employee.

1. Complete an incident report identifying the route(s) of exposures and the circumstances under which the exposure incident occurred.

2. Make a confidential medical evaluation available immediately and follow-up, post exposure prophylaxis if indicated, and counseling by a qualified healthcare provider. This step is required by the Bloodborne Pathogen standard. As of July 2020, baseline hepatitis C testing should be obtained for all exposures, unless declined by the worker.

3. Obtain employee consent to treatment and any bloodwork which may be completed. If the worker does not choose to receive testing or treatment, employers must get a signed declination of care to document that care was offered.

Hopefully an employee in your practice will never experience an exposure event, but advance planning and training can ensure care is provided to both the source patient and practice employee in timely and efficient manner.

If you would like to learn more about the details of responding to an exposure event in your practice, join Karen Gregory, RN on Tuesday, August 24th, at 12 noon for **Managing an Exposure Event**.

Join Now!

OSHA COMPLIANCE

OSHA JOINS WITH THE FDA TO ISSUE AN ALERT ON HAIOU SAFETY NEEDLES

The FDA is recommending healthcare providers stop using certain syringes and needles with needle safety devices manufactured by Guangdong Haiou Medical Apparatus Co., LTD. The FDA received information about quality issues, including certain Haiou needles detaching from the syringe and needle safety device failures.

- 1ml syringe with 25g x 1-inch needle
- 1ml syringe with 23g x 1-inch needle

Be aware that these syringes and needle configurations may be available as individual units or as part of a kit.

The FDA has reports where these needles have detached and remained in the patient's arm. Incidents where the needle safety function failed has caused injuries to healthcare workers which increases risk of bloodborne pathogens transmission. The FDA issued an import alert to prevent these syringe and needle configurations from entering the United States. The FDA is working to identify where these configurations have been distributed and inform those sites of quality issues.

Continued on Page 8

COMPLIANCE

The FDA is evaluating whether other HAIOU syringe and needle configurations may have similar problems. They encourages health care to report adverse events or suspected adverse events experienced with any syringe and needle configurations.

- Voluntary reports can be submitted through MedWatch, the FDA Safety Information and Adverse Event Reporting program.
- Device manufacturers and user facilities must comply with the applicable Medical Device Reporting (MDR) regulations.
- Health care personnel employed by facilities that are subject to these reporting requirements *should follow* their facilities reporting procedures.

To read the full alert: https://www.osha.gov/quicktakes/06012021

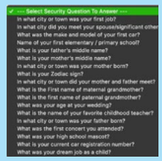
IT'S YOUR CALL

OSHA:

Several of our vaccinated employees have a greater risk of being exposed to SARS-CoV-2 and the potential for prolonged, close contact with someone with SARS-CoV-2. If vaccinated workers are asymptomatic, what testing is recommended?

HIPAA:

True or False:
Responding to games and posts like this are just fun and not a way to guess passwords and security questions to your personal or work accounts.



CLICK HERE
FOR ANSWERS

TMC
TOTAL MEDICAL COMPLIANCE

888.862.6742
www.totalmedicalcompliance.com

JUNE 2021

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