TMC
TOTAL MEDICAL COMPLIANCE

888.862.6742
www.totalmedicalcompliance.com

MARCH 2017

THE ADVISOR

MONITORING INTERNAL ACCESS CAN SAVE YOU FROM HUGE FINES

Everyone is aware of the dangers of someone hacking into your patient records. Hopefully lots of checks and balances are in place to identify and protect you from outside access into your systems. But, what are you doing to protect yourself from inappropriate internal access?

HHS Office of Civil Rights (OCR) oversees the enforcement of HIPAA laws. OCR recently settled with a Healthcare System in Florida for $5.5 million in violation fines. What did they do to earn fines so high that they eventually settled for millions? The password of a former employee of an affiliated physician's office had been used to access their electronic protected health information (ePHI) on a daily basis without detection for one year, affecting 80,000 individuals. They further discovered that inappropriate access by their own employees resulted in another 35,000 records breached. Although they had policies and procedures in place, they failed to implement procedures for reviewing, modifying and/or terminating access. Further, they failed to regularly review system activity on applications with ePHI by their users despite having identified this risk on several risk analyses over a period of five years.

The HIPAA Security Rule provision on Audit Controls (45 C.F.R. § 164.312(b)) requires Covered Entities and Business Associates to implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use ePHI. The majority of systems provide some level of audit reports.

Continued on page 2

IN THIS ISSUE

TMC
TOTAL MEDICAL COMPLIANCE

OSHA/HIPAA eCOMPLIANCE OPTIONS

eCompliance BASIC

24 / 7 ONLINE TRAINING AVAILABLE THROUGH THE CLIENT PORTAL SO YOU HAVE OSHA & HIPAA TRAINING RESOURCES

eCompliance PLUS

ECOMPLIANCE BASIC + CURRENT HIPAA & OSHA COMPLIANCE MANUALS AND MONDAY - FRIDAY CUSTOMER SERVICE BY PHONE

eCompliance PRO

ECOMPLIANCE PLUS + LIVE WEBINAR TRAINING FOR EMPLOYEES AND A FREE SPILL KIT FOR OSHA CLIENTS

PROCEED TO FIND OUT MORE ABOUT THE TMC PRODUCTS OPTIONS

eCompliance BASIC

OSHA AND HIPAA COMPLIANCE

online training available 24/7 through the Client Portal

ONLINE TRAINING

COMPLIANCE MANUAL

ELECTRONIC FORMS

PROCEED TO FIND OUT MORE ABOUT THE TMC PRODUCTS OPTIONS

eCompliance PLUS

OSHA AND HIPAA COMPLIANCE

HIPAA & OSHA manuals and Mon - Fri customer service by phone

ONLINE TRAINING

COMPLIANCE MANUAL

ELECTRONIC FORMS

OSHA & HIPAA SUPPORT

PROCEED TO FIND OUT MORE ABOUT THE TMC PRODUCTS OPTIONS

MONITORING INTERNAL ACCESS CAN SAVE YOU FROM HUGE FINES

Continued from page 1

Examples of audit trails include:

- **Application audit trails** – User activities that are monitored and logged in applications include data files opened and closed, and the creating, reading, editing, and deleting of records.
- **System-level audit trails** – This type of audit captures successful or unsuccessful log-on attempts, log-on ID/username, date and time of each log-on/off attempt, devices used to log-on, and the application the user successfully or unsuccessfully accessed.
- **User audit trails** – These audits log user activity in a ePHI system or application by recording events initiated by the user, such as all commands directly initiated by the user, logon attempts with identification and authentication, and access to ePHI files and resources.

Audit reports work in conjunction with audit logs and trails to reduce risk associated by reviewing inappropriate access, tracking unauthorized disclosures, detecting performance problems and flaws in applications, and detecting potential intrusions and other malicious activity. These reports can be used to provide evidence during an investigation of security incidents and breaches.

When determining reasonable and appropriate audit controls for systems containing or using ePHI, you must consider risk analysis results and your current technical infrastructure, hardware, and software security capabilities. It is imperative to review audit trails regularly, both after security incidents or breaches, and during normal operations. Access to audit trails should be tightly restricted to only authorized personnel.

MONITORING INTERNAL ACCESS CAN SAVE YOU FROM HUGE FINES

Continued from page 2

Questions that Covered Entities and Business Associates should consider:

- What audit control mechanisms are reasonable and appropriate to implement so as to record and examine activity?
- What are the audit control capabilities of your systems?
- Do the audit controls implemented allow you to meet your policies and procedures?
- Are changes or upgrades of your audit capabilities necessary?

OCR offers helpful guidance on the importance of audit controls and audit trails at https://www.hhs.gov/sites/default/files/january-2017-cyber-newsletter.pdf

Make sure you have the following in place:

- A risk analysis and on-going risk management.
- A Corrective Action Plan (CAP) that includes evidence that you've fixed or mitigated the risks identified or dates of expected implementation.
- Policies and procedures that require the regular review of system activity by audit logs, access reports, and security incident tracking.
- Access Protocols for access set-up, modification and termination by type of user: employees, business associates, affiliated physicians, their practices, and their employees.

Make sure you have a good list of all systems to ensure you cover all your ePHI.

DEMYSTIFYING OSHA INSPECTIONS: AFTER THE INSPECTION

After the physical inspection is over, the inspector will have a "Closing Meeting" to cover the preliminary findings. This meeting can happen immediately after the inspection or can be scheduled for a future date. At the Closing Meeting the inspector will meet with the OSHA Officer (and management if you request it) to go over all issues noted during then inspection. This list of issues may include issues that are noted but so minor that they will not end up on the official list. Feel free to ask questions and to volunteer information that could prove you have addressed the issue. Start fixing the problems identified immediately.

What happens after the inspection?

After the Closing Meeting the inspector will return to their office and write up their results. They may call you to get follow up information. Once the report is written it is submitted to their manager. The manager will review the report and create an official citation letter listing each issue, the regulation that was involved and the amount of the fine for each citation. This letter will include information on your rights to contest the OSHA citations and your responsibilities to post the results for your employees and the dates by which you are required to fix the problems. This letter will usually be sent to you within two weeks of the Closing Meeting.

OSHA divides citations between "Serious" and "Non-Serious" categories. Non-Serious violations usually are not fined but can be minimally fined. OSHA increased their fine structure in August 2016 and again in January 2017. Under OSHA's new charter they can increase their fines each year. Each serious violation now starts at $12,675. There is a series of reductions to the fine that OSHA will apply: 60% for small businesses, 15% off for being "courteous and cooperative," and 10% if you had an OSHA program in place. (If OSHA notes that this is a repeated violation from a previous inspection or if they determine that it is a "willful" violation the fine starts at $126,749.)

You will then have to submit a form (included in your citation letter) back to OSHA to prove that you have fixed the problems listed within the timeframe allotted. This is called Abatement. Abatement should include a short explanation, supporting documents or even pictures if necessary. You can request an extension if necessary. Failure to abate the citations by the stated date can result in a fine of $12,675.

An important right you have in the inspection process is to contest the citations and fines. The first step of this process is to request an "Informal Conference" with the manager/supervisor who sent you the citation letter. Next month's final article in the series will be on your right to contest the OSHA findings.

If you missed the previous three articles in this series they can be viewed on our website at www.TotalMedicalCompliance.com .

December, 2016: How your practice is selected for inspection
January, 2017: The steps of the inspection process
February, 2017: The physical inspection

ENGINEERED SAFETY DEVICES

Is Our Facility Required to Use Engineered Safety Devices?

We get a lot of questions at TMC about the OSHA Bloodborne Pathogens (BBP) standard requirement to use engineering controls, specifically sharps with engineered sharps protection often referred to as safety devices. Here are some specifics and resources you might find helpful if you are looking to implement a specific type of safety device.

Engineering controls (e.g., sharps disposal containers, self-sheathing needles, safer medical devices, such as sharps with engineered sharps injury protections and needleless systems) isolate or remove the bloodborne pathogens hazard from the workplace. Sharps with engineered sharps injury protections are a subset of engineering controls. They are a non-needle sharp or a needle device used for withdrawing body fluids, accessing a vein or artery, or administering medications or other fluids, with a built-in safety feature or mechanism that effectively reduces the risk of an exposure incident.

The excerpts below are taken from the Revision to OSHA's Bloodborne Pathogens Standard - Technical Background and Summary. It specifically addresses the Needlestick Safety and Prevention Act and the changes it required to the BBP standard. (https://www.osha.gov/needlesticks/needlefact.html)

Changes to the Exposure Control Plan

Employer must:

- take into account innovations in medical procedure and technological developments that reduce the risk of exposure (e.g., newly available medical devices designed to reduce needlesticks); and
- document consideration and use of appropriate, commercially-available, and effective safer devices (e.g., describe the devices identified as candidates for use, the method(s) used to evaluate those devices, and justification for the eventual selection).

The document goes on to allow for the following considerations in adoption of a safety devices:

No one medical device is considered appropriate or effective for all circumstances. Employers must select devices that, based on reasonable judgment:

- will not jeopardize patient or employee safety or be medically inadvisable; and
- will make an exposure incident involving a contaminated sharp less likely to occur.

Employee Input

Employers must solicit input from non-managerial employees responsible for direct patient care regarding the identification, evaluation, and selection of effective engineering controls, including safer medical devices.

Documentation of employee input

Employers are required to document, in the Exposure Control Plan, how they received input from employees.

This obligation can be met by:

- Listing the employees involved and describing the process by which input was requested; or
- Presenting other documentation, including references to the minutes of meetings, copies of documents used to request employee participation, or records of responses received from employees.

Continued on page 6

Continued from page 5

ENGINEERED SAFETY DEVICES

Bottom line, if there is a safety device available and it will not jeopardize patient or employee safety or be medically inadvisable, the device should be implemented for use during patient care. But, how would you identify which devices are appropriate for use? There are engineering controls on the market for needles, scalpels, IV/port access devices, and blood draw equipment. If you are utilizing any of these sharps and have not implemented a safety device, please contact your medical supply/device distributor for samples to use during the evaluation phase.

Your TMC consultant will help you walk through this process if they work with you in your practice. Additionally, you may find the following websites and articles helpful.

https://www.medicalcenter.virginia.edu/epinet/new/safetydevice.html
https://www.osha.gov/SLTC/bloodbornepathogens/bloodborne_quickref.html
https://www.osha.gov/SLTC/etools/hospital/hazards/sharps/sharps.html
https://www.cdc.gov/niosh/docs/2000-108/pdfs/2000-108.pdf
https://www.cdc.gov/oralhealth/infectioncontrol/forms.htm

If you have not implemented safety devices, now is the time to begin the process. There is a wealth of data about the effectiveness of these devices to reduce sharps injuries which are a real health risk to healthcare providers.

DID YOU KNOW?

"Did you know that you don't have to be afraid to speak up? Reporting drug abuse signs in a healthcare setting." CLICK FOR MORE INFO

IT'S YOUR CALL

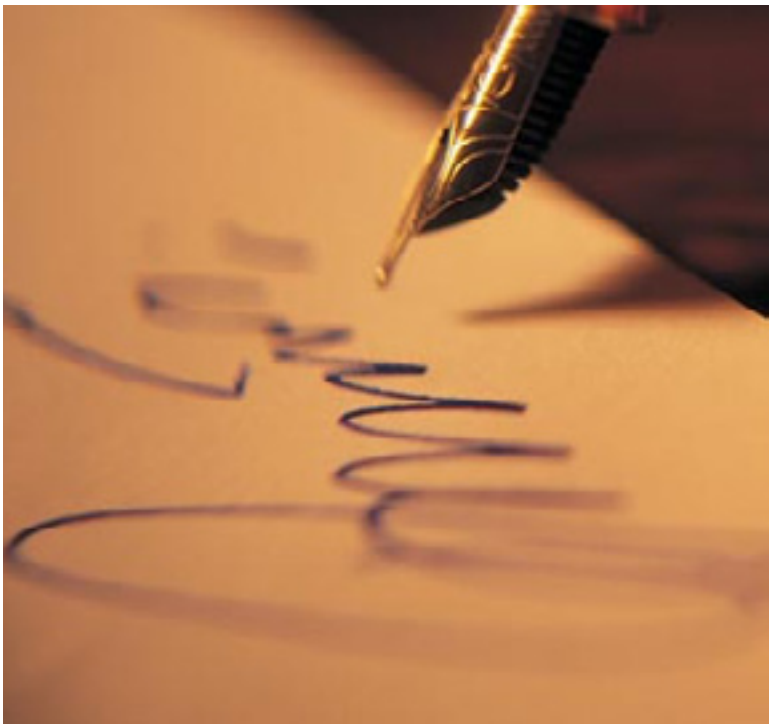
OSHA Situation:

Your office has annual Personal Protective Equipment (PPE) training, and, as needed to train new hires. Is there ever a need to train employees outside of these time frames?

HIPAA Situation:

A 20-year old, incompetent patient has just arrived for her first office visit accompanied by her biological parent. The biological parent gives you a handwritten letter stating that she is the legal guardian, but it is not a legal document. Does your office staff know how to handle this type of scenario properly?

VISIT OUR BLOG FOR THE ANSWERS



TMC
TOTAL MEDICAL COMPLIANCE

888.862.6742
www.totalmedicalcompliance.com

MARCH 2017

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