TMC TOTAL MEDICAL COMPLIANCE

888-862-6742
www.totalmedicalcompliance.com

OCTOBER 2023

THE ADVISOR
MONTHLY COMPLIANCE COMMUNICATOR

The Importance of Cybersecurity for Healthcare Practices: A Necessity Not to be Overlooked

In the rapidly evolving world of technology, cybersecurity has emerged as a critical issue, particularly in the healthcare sector. Cybersecurity isn't just an optional add-on but rather an essential component of a successful and compliant healthcare practice.

Why is Cybersecurity Important in Healthcare?
Healthcare practices handle a lot of sensitive and confidential data. Potential targets for cybercriminals range from personal health records to billing information. According to the HHS Office for Civil Rights data breach portal, healthcare data breaches impacted over 39 million people in the United States so far in 2023. This emphasizes the critical importance of good cybersecurity safeguards.

Getting to Know Cybersecurity Basics
The world of cybersecurity can seem daunting, but knowing the basics can significantly enhance your healthcare practice's safety. Here are a few key concepts:

1. **Data Encryption:** Converting your data into a code to prevent unauthorized access.
2. **Firewalls:** Network security systems that monitor and control incoming and outgoing network traffic based on security rules.
3. **Multi-Factor Authentication:** A way in which a computer user is permitted access only after providing two or more pieces of evidence to an authentication system successfully.
4. **Regular Software Updates:** Keeping your software up to date is vital, as updates often include security patches for vulnerabilities that cybercriminals could exploit.

Creating a Cyber-Secure Culture
The best cybersecurity tools are of no use if your employees are not taught safe online behavior. Cybersecurity is a people issue as much as a technical one. Implementing a cybersecurity culture

Newsletter Content

entails frequent employee training and awareness seminars that emphasize the importance of simple acts such as not clicking on suspicious links and updating passwords on a regular basis. Encourage your employees to be watchful and report any questionable behavior. This allows concerns to be addressed quickly, minimizing potential damage.

The Cybersecurity Journey: An Ongoing Process
Cybercriminals are constantly evolving and seeking weaknesses in company security. As such, cybersecurity policies and procedures should be reviewed and updated on a regular basis. The idea is to stay one step ahead of any threats and trends to protect your practice against cyber threats.

Your Next Steps
What should you do next now that you are aware of the significance of cybersecurity in healthcare? We suggest conducting a cybersecurity audit of your practice to find any possible vulnerabilities. Then create a plan to solve the issues and make sure you're in compliance.

If you're not sure where to start, don't worry, we can guide you with our Cybersecurity Basics course. This course will take you through the steps involved in safeguarding the data used in your practice and adhering to compliance requirements.

It's Your Call

HIPAA: Why is a Password Policy Important?
One of the critical aspects of achieving HIPAA compliance is enforcing a mandatory password policy. Failing to do so could have severe consequences that compromise patient privacy and expose healthcare entities to a range of other negative outcomes.

1. Vulnerability to Data Breaches:
Without a stringent password policy in place, healthcare organizations become vulnerable targets for cybercriminals seeking unauthorized access to patient records. Weak passwords or lax security measures create opportunities for hackers to exploit vulnerabilities and enter sensitive systems. Once inside, hackers can steal personal health information (PHI), leading to data breaches that tarnish the reputation of the healthcare provider and put patients at risk of identity theft and medical fraud.

2. Compromised Patient Privacy:
HIPAA's primary goal is to protect patient privacy and ensure the confidentiality of medical information. Failing to enforce a mandatory password policy can lead to unauthorized access to patient records, potentially revealing sensitive PHI details about medical conditions, treatments, and personal information. This breach of trust not only violates patient rights but can also result in legal repercussions for the healthcare organization.

3. Regulatory Non-Compliance:
HIPAA mandates that healthcare organizations adhere to specific security standards to safeguard patient data. Enforcing a mandatory password policy is an integral part of these security measures. Neglecting to implement such policies can lead to non-compliance with HIPAA regulations, exposing healthcare entities to significant fines, penalties, and legal action.

4. Financial Consequences:
The repercussions of non-compliance with HIPAA regulations can be financially crippling for healthcare organizations. Fines for HIPAA violations can range from thousands to millions of dollars, depending on the severity of the breach and the organization's response to the incident. These financial penalties can drain resources, hinder growth, and impact the overall financial health of the entity.

5. Erosion of Trust:
Patient trust forms the foundation of a successful healthcare practice. A breach in patient data due to weak password policies or lax security measures can severely erode this trust. Patients rely on healthcare providers to keep their PHI secure and private. Once this trust is lost, patients may seek care elsewhere, damaging the provider's reputation and potentially leading to revenue loss.

The importance of enforcing a mandatory password policy under HIPAA cannot be overstated. The consequences of overlooking this aspect of data security are significant, ranging from compromised patient privacy and regulatory non-compliance to financial penalties and may also lead to legal battles. Healthcare organizations must recognize that patient data is a responsibility that demands unwavering protection. By implementing and enforcing robust password policies, healthcare providers can reinforce their defenses against cyber threats, uphold the principles of HIPAA, and ensure the continued trust of patients.

OSHA: The transport container is contaminated with blood and other potentially infectious material (OPIM) from our instruments. How should we clean these reusable, transport containers?
OSHA regulation 1910.1030(d)(4)(ii)(C) states: All bins, pails, cans, and similar receptacles intended for reuse which have a reasonable likelihood for becoming contaminated with blood or other potentially infectious materials shall be inspected and decontaminated on a regularly scheduled basis and cleaned and decontaminated immediately or as soon as feasible upon visible contamination.

This can be accomplished by wearing the appropriate personal protective equipment (PPE) and using the same product that you use to clean and disinfect the surfaces in your clinical areas such as OPTIM, Caviwipes, Saniwipes and many others.

HIPAA-Compliant Video Conferencing: Your Guide to Secure Healthcare Communications

Modern healthcare has evolved dramatically with the integration of technology. While digitization has indeed elevated patient care and broadened its accessibility, it has also brought along challenges, primarily concerning privacy and security. A significant part of this conversation involves the use of communication tools like video conferencing and their compliance with HIPAA.

If you are wondering if services like Zoom, Microsoft Teams, Google Meet, etc. are HIPAA-compliant, you're in the right place. This article delves into the essentials of HIPAA-compliant video conferencing. Our goal is to help healthcare providers navigate this space and ensure they uphold patient confidentiality in their communications.

What Makes Video Conferencing HIPAA-compliant?

A HIPAA-compliant platform needs to fulfill the following requirements:

- Encryption: The video conferencing software should have end-to-end encryption, ensuring unauthorized parties cannot access the communication.
- Access controls: Only authorized personnel should be able to initiate, join, or view the video conference.
- Audit controls: The platform should provide a way to track and document activity within video conferences.
- Breach management: In the event of a data breach, there should be established procedures to identify and respond to the situation.
- Business Associate Agreement (BAA): HIPAA regulations stipulate that the platform provider must be willing to provide a BAA, taking responsibility for the protection of patient data.

Is Microsoft Teams HIPAA-compliant?

Yes, Microsoft Teams is HIPAA-compliant. Microsoft offers a BAA for their paid versions, thus taking responsibility for the security of patient data. It also provides robust security features like encryption, two-factor authentication, and extensive audit logs.

Is FaceTime HIPAA-compliant?

No, FaceTime is not HIPAA-compliant. Apple does not currently offer a BAA for Facetime, making it non-compliant . While Facetime does employ end-to-end encryption, without a BAA, it fails to meet HIPAA standards.

Is Zoom HIPAA-compliant?

Yes, Zoom is HIPAA-compliant, but only for the paid versions. Zoom offers a BAA for these versions and includes robust security measures such as encryption and user authentication.

Is Skype HIPAA-compliant?

No, Skype is not HIPAA-compliant in its standard form. Skype does not offer a BAA and should not be used for sharing protected health information (PHI).

Is Google Meet HIPAA-compliant?

Yes, if part of Google Business Workspace, Google Meet, is HIPAA-compliant. Google Business offers a BAA for all Google Workspace customers, covering Google Meet. The platform includes necessary security features such as encryption and audit logs. Learn more about Google Meet and HIPAA compliance here. It should be noted that the free version of Google Meet is not HIPAA-compliant and should not be used to share PHI.

Takeaways

While the world of HIPAA-compliant video conferencing can seem daunting, understanding the basics of what makes a platform compliant is the first step. Keep in mind that HIPAA-compliance only comes with the paid versions of these platforms and requires the provider to sign a BAA.

We hope this guide will help you understand HIPAA-compliant video conferencing. As part of your compliance journey, remember that ongoing training and an understanding of HIPAA requirements are vital for all healthcare professionals. We invite you to learn more and take advantage of our compliance products and services.

Ensuring Workplace Fire Safety: OSHA Requirements for Fire Prevention Plans, Fire Extinguishers, and Exit Routes

Fire safety regulations date back to 1895 when concerns arose from the lack of standards for sprinkler systems and plumbers had logistical challenges when they attempted to install or maintain these systems. Following this initial attempt, the need for fire safety regulations was stressed due to the deadly fire that broke out at the Illinois' Iroquois Theater. This incident led to the requirement and standardization of emergency exits, clear walkways, and exit signs. Subsequently, in 1911, the Triangle Shirtwaist Fire killed nearly 150 people which then lead to the development of outdoor fire escapes and implementation of fire drills.

Fire safety is an incredibly important measure to have in place in any company, including healthcare and dental companies. Fire safety covers a multitude of regulatory areas including fire prevention plans, fire extinguishers, and exit signs.

OSHA Fire Prevention Plan

The Occupational Health and Safety Administration (OSHA) has developed a fire prevention plan – 1910.39. This standard states that a fire prevention plan must be: in writing, kept in the workplace, made available to employees for review. If there are 10 or fewer employees, the plan may be communicated orally to employees.

The employer is required to inform employees upon initial assignment about any fire hazards they are exposed to, and they must review the parts of the fire prevention plan necessary for self-protection with each employee. There are other minimum requirements to each fire prevention, including:

- A list of all major fire hazards,
- Proper handling and storage procedures for hazardous materials,
- Potential ignition sources and their controls,
- Type of fire protection equipment necessary to control each major hazard,
- Procedures to control accumulations of flammable and combustible waste materials,
- Procedures for regular maintenance of safeguards installed on heat-producing equipment to prevent accidental ignition of combustible material, and
- Name/job title of employees who are responsible for maintaining equipment to prevent/control sources of ignition/fires.

Fire Extinguisher Requirements

Unless there is an explicitly stated statement in a fire safety policy requiring the immediate evacuation of all employees upon the sounding of a fire alarm, all employers must provide portable fire extinguishers. (It should be noted that employers must install and maintain alarm systems with distinctive signals to warn of fire or other emergencies).

There are additional requirements surrounding fire extinguishers for employers, including ensuring:

- the correct quantity and class of fire extinguishers are readily available,
- the fire extinguishers are operable and fully charged, and
- that extinguishers are in a conspicuous, designated location.
- If an extinguisher is discharged, it must be refilled and replaced immediately. Additionally, fire extinguishers must be visually inspected monthly and receive an annual maintenance check. Training is also vitally important and required. Upon initial employment and at least on an annual basis, training must be completed on the general principles of fire extinguishers and hazards. One of the most important principles that should be taught is that fighting a fire should never supersede an employees' safety and they should never put them at risk. Although, those who have been designated to use firefighting equipment must be trained in the use of the equipment upon initial assignment and at least annually.

Exit Route Requirements

Exit routes present many tedious steps that must be taken to ensure that employees are kept safe in the event of a fire. Minimizing danger is key. As an employer, there are certain questions you should respond to with a "yes," including:

- Is the exit route free of explosive or highly flammable furnishings or decorations?
- Is the exit route out of the way of high hazard areas?
- If so, is it shielded from the high hazard by suitable barriers?
- Is the exit route free and unobstructed?
- Are the safeguards designed to protect employees during an emergency in proper working order at all times?
- Are exit routes adequately lit?
- Are exit signs illuminated and distinctive in color? Is "Exit" plainly legible?
- Are exits clearly visible and marked by an "Exit" sign? Is the line-of-sight to an "Exit" sign clearly visible?
- Are non-exit doors labeled as "Not an Exit" or clearly identified by a sign indicating its use?
- Are exit route doors free of decorations or signs that could obscure visibility?

If there is construction, repair, or alterations to the company's building, exit routes must be maintained. Employees may not occupy a workplace until an exit route is safely and easily accessible to them. Additionally, existing fire protections must be maintained, or alternate fire protection must be supplied that provides an equivalent level of safety. Employees must not be exposed to hazards of flammable or explosive substances or equipment used during construction, repairs, or alterations that are beyond the normal permissible conditions in the workplace, or that would impede exiting the workplace.

Fire safety regulations' history has been marred by tragic events that acted as a catalyst for necessary safety measures. Fire safety is an indispensable aspect of any company, spreading across many regulatory areas such as fire prevention plans, fire extinguishers, and exit routes. It is not just a set of regulations and guidelines; fire safety is a commitment to safeguarding the lives and well-being of employees and visitors alike.

TOTAL MEDICAL COMPLIANCE

888-862-6742
www.totalmedicalcompliance.com

OCTOBER 2023

THE ADVISOR

MONTHLY COMPLIANCE COMMUNICATOR

PRINT SIGNATURE 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.

Newsletter Content

Need to contact us? Scan the QR code for all the ways to get in touch!