TMC TOTAL MEDICAL COMPLIANCE

888-862-6742
www.totalmedicalcompliance.com

JULY 2023

THEADVISOR
MONTHLY COMPLIANCE COMMUNICATOR

Protecting Privacy: Lessons from the OCR-Yakima Valley Memorial Hospital Snooping Settlement

In a digital era where personal information is vulnerable to cyber threats, privacy protection has become more critical than ever. A recent settlement between the Office for Civil Rights (OCR) and Yakima Valley Memorial Hospital in Washington state highlights the importance of safeguarding sensitive data. We explore the key details of the settlement and provides actionable steps to help organizations avoid similar incidents and protect their users' privacy.

The OCR, a division of the U.S. Department of Health and Human Services, reached a $240,000 settlement with Yakima Valley Memorial Hospital following an investigation into a privacy breach. The breach involved unauthorized access to 419 patient health records by 23 security guards working in the emergency department. The guards lacked an employment-related reason for accessing the information. As part of the settlement, the hospital agreed to pay a penalty and implement a comprehensive two-year corrective action plan.

Newsletter Content

Action Items for Your Privacy Protection

1. Strengthen Security Measures:

Review and enhance security protocols to protect against unauthorized access. This includes user authentication mechanisms, regular password updates, and multi-factor authentication for sensitive systems.

2. Educate Employees:

Conduct regular training sessions to educate staff members on privacy best practices and the consequences of privacy breaches. Emphasize the importance of handling sensitive information securely and remind employees of their legal and ethical obligations.

3. Implement Access Controls:

Limit access to sensitive data by implementing role-based access controls. Ensure that only authorized personnel can access specific information based on their job responsibilities.

4. Regular Audits and Monitoring:

Establish a comprehensive auditing and monitoring system to track access and usage of sensitive data. Regularly review access logs and user activity to identify any unusual patterns or potential breaches promptly.

5. Encrypt Data:

Encrypt sensitive data both at rest and in transit. Implement policies and procedures to ensure secure transmission protocols are used to protect data during storage and transmission.

6. Incident Response Plan:

Develop a well-defined incident response plan that outlines the steps to be taken in the event of a privacy breach. This includes immediate containment, investigation, notification of affected individuals, and collaboration with law enforcement and regulatory agencies as needed.

7. Vendor Due Diligence:

Conduct thorough due diligence when selecting and working with vendors who have access to sensitive data. Confirm they adhere to robust privacy and security standards and regularly monitor their compliance.

8. Regular Risk Assessments:
Conduct periodic risk assessments to identify potential vulnerabilities and implement appropriate controls. This includes evaluating system architecture, network infrastructure, and internal processes to mitigate risks proactively.

9. Privacy Policies and Consent:
Develop transparent privacy policies that clearly communicate how user data is collected, stored, and used. Obtain explicit consent from individuals before collecting and sharing their personal information, adhering to applicable data protection regulations.

10. Continual Improvement:
Privacy protection is an ongoing process. Regularly evaluate and enhance privacy practices based on emerging threats, industry best practices, and regulatory changes. Stay informed about new technologies and adopt measures to address evolving risks.

The OCR-Yakima Valley Memorial Hospital settlement serves as a reminder of the importance of privacy protection in today's digital landscape. By implementing the recommended action items, organizations can proactively safeguard sensitive data and mitigate the risk of privacy breaches. Prioritizing privacy not only protects individuals but also maintains trust, reputation, and compliance with regulatory standards.

Emergency and Fire Preparedness in Healthcare Offices: The OSHA Way

'Expect the unexpected' is one phrase that comes to mind when considering how healthcare offices run. An example of an unforeseen event is an emergency and/or fire scenario. These situations can quickly turn a normal day into a life-altering crisis.

Data shows there are an average of 5,750 fires reported annually in healthcare facilities, resulting in about $50.4 million in property damage. This doesn't account for the potential loss of life or emotional trauma.

The Occupational Safety and Health Administration (OSHA), as a federal protector of workers, advocates for strong safety measures during emergencies.

Emergency and fire preparedness are vital elements of a safe, efficient healthcare office, not just legal obligations. Following OSHA rules shows dedication to employee safety.

Every year, there are hundreds of fire-related incidents in healthcare facilities, leading to injuries, property damage, and the loss of life. Understanding OSHA's emergency and fire preparedness regulations can significantly reduce these risks.

Under the General Duty Clause of the Occupational Safety and Health Act, OSHA requires healthcare practices to maintain safe and healthful workplaces for their employees. This encompasses an effective emergency action plan (EAP) and a fire prevention plan (FPP), both of which are critical in minimizing damage and ensuring employee safety during emergencies.

Emergency Action Plan (EAP): OSHA's Minimum Requirements

An EAP is a well-structured plan detailing the actions employees must take in case of an emergency. The OSHA standard for emergency action plans demands that they at least contain:

- Procedures for reporting fires and other emergencies.
- Methods for emergency evacuation, including exit route assignments.
- Procedures for employees who stay behind to run key activities before being evacuated.
- Procedures to account for all employees after evacuation.
- Rescue and medical duties for those employees performing them.
- The preferred means of alerting employees to an emergency.

Moreover, the plan must be in writing, kept in the workplace, and available to employees for review. However, if you have 10 or fewer employees, the plan can be communicated orally.

Fire Prevention Plan (FPP): OSHA Guidelines

The OSHA guidelines for a fire prevention plan must cover the following:

- List any key fire hazards, proper hazardous material handling and storage techniques, potential ignition sources and their control, and the type of fire protection equipment required to control each major hazard.
- Controlling the accumulation of flammable and combustible waste products.
- Procedures for maintaining the safeguards installed on heat-producing equipment to prevent the unintentional ignition of flammable materials on a regular basis.
- Employees' names or work titles who oversee maintaining devices installed to prevent or regulate ignitions.
- Employees in charge of controlling fuel source dangers are identified by name or job title.

Like the EAP, the FPP must be in writing, kept in the workplace, and available for employees to review. The same guidelines apply here if there are 10 or fewer employees, the plan can be communicated orally.

Implementing OSHA's Emergency and Fire Preparedness Guidelines

- Employee Training: Training is crucial when it comes to implementing your EAP and FPP. Conduct yearly training sessions and drills to familiarize your staff with emergency procedures, routes, and assembly points.
- Assign Roles: Designate individuals responsible for critical operations and those in charge of the evacuation. Ensure they have the skills to perform their duties effectively.
- Maintain Equipment: Regularly inspect and maintain your fire prevention and protection equipment. This includes fire extinguishers, smoke detectors, fire suppression systems, and emergency lighting systems.
- Cleanliness and Orderliness: Properly and regular dispose of combustible waste and maintain orderliness to prevent accidental fires.
- Review and Update Your Plans: At least once per year, review your EAP and FPP, making necessary adjustments to accommodate changes in staff, equipment, or your facility's layout.

Fire and emergency preparedness in healthcare offices are not topics to be taken lightly. As a medical and dental compliance company, TMC can help you navigate OSHA requirements for EAP and FPP to suit your practice's needs.
At Total Medical Compliance, we believe in proactive OSHA and HIPAA compliance. We invite you to check out our Emergency and Fire Preparedness course to learn more about creating a safe, compliant workplace environment. Stay compliant to stay safe!

It's Your Call

HIPAA: What is snooping under the HIPAA Privacy Rule?

Snooping, in the context of HIPAA, refers to unauthorized access or inappropriate disclosure of someone's personal health information (PHI) by individuals who have access to it in their professional capacity but do not have a legitimate need to know or use that information. Snooping is a violation of the HIPAA Privacy Rule and is considered a serious breach of patient confidentiality.

Examples of snooping might include healthcare employees accessing the medical records of friends, family members, coworkers, or celebrities without a valid reason or outside the scope of their job responsibilities. It can also involve employees accessing PHI out of curiosity or for personal gain. Snooping incidents can lead to disciplinary actions, legal consequences, and damage to the affected individuals' privacy and trust.

HIPAA regulations require covered entities to have policies and procedures in place to prevent and detect snooping. They must also provide training to their employees on HIPAA rules and the importance of patient privacy. In the event of a snooping incident, covered entities are responsible for investigating and taking appropriate action, such as disciplinary measures, to address the violation and prevent future occurrences.

OSHA: What are OSHA's rules about fire extinguisher placement?

Employers should select, mount, and place portable fire extinguishers throughout the workplace so that they are readily available and do not subject their workers to potential danger or injury (29 CFR 1910.157(c)). Device selection and position should be based upon the anticipated class of fire and the size and degree of hazard.

Portable fire extinguishers can usually be found in or around hallways, laundry rooms, meeting rooms, kitchens, mechanical/electrical rooms, and near exit doors. Portable fire extinguishers should also be visually inspected monthly and receive annual maintenance to comply with the OSHA regulation 1910.157(e).

TMC
TOTAL MEDICAL COMPLIANCE

888-862-6742
www.totalmedicalcompliance.com

JULY 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!