HIPAA Compliance Recommendations

Last Edit: February 2, 2024

HIPAA Compliance

The Health Insurance Portability and Accountability Act (HIPAA) is a federal law that requires the creation of national standards to protect sensitive patient heath information from being disclosed without the patient's consent or knowledge. Through a series of regulatory rules, HIPAA compliance is an agreed upon requirement that healthcare organizations must implement within their own business to protect the privacy, security, and integrity of protected health information. This includes, but is not limited to hospitals, clinics, medical insurance offices, etc.

In the following sections, we will outline some recommendations to help ensure that customers are providing patients with the required privacy to remain within compliance of HIPAA.

****NOTE:** DW products (or 3rd party products) are not required to be inherently HIPAA compliant. It is the responsibility of the facility's staff and organization to ensure that HIPAA compliance is maintained.

****NOTE:** This document is intended merely for the guidance and consideration of the installer and of users and is NOT a catchall for all legal scenarios. Please consult the proper legal authority for the organization to ensure that HIPAA compliance is being met.

DW Hardware Involvement

It is the sole responsibility on part of the healthcare provider's organization to ensure that they are within HIPAA compliance. Compliance is not necessarily dependent upon the use of DW hardware, or any 3rd party surveillance products. Rather, compliance is the responsibility of the healthcare organization

with the way that the security hardware has been deployed, transparency about patient privacy, and ensuring that access to patient information is secure.

Surveillance Recommendations

Security cameras are typically installed to watch public areas such as hallways, elevators, stairwells, and building access points. They are also commonly used to watch parking garages and the exterior premises of buildings.

However, the hospital or medical office must make it clear to patients that they are being recorded. If the camera is installed in such a way that disregards open disclosure using a surveillance system, a camera has been positioned to where patient information can be captured within the field of view, or private audio can be recorded, this can lead to a violation of HIPAA compliance.

Basic HIPAA Compliance

Here are some things that are worth considering when installing security cameras and other surveillance hardware.

- The facility must have it clearly stated to patients that there is video surveillance on the premises and that they are being recorded in public areas.
- Indoor surveillance cameras can be used to record videos in common areas such as entrances, exits, waiting rooms, and hallways.
    - Cameras should NOT be mounted in such a way that viewers can see the inside of examination rooms.
- Security cameras should NOT be placed in private areas such as restrooms, changing rooms, or examination rooms.
    - If a camera is mounted in a public area, such as a hallway, and is close to a restroom, it must be confirmed that the camera will not record any private or sensitive footage (such as when the restroom door is opened).
- Outdoor surveillance cameras are prohibited by HIPAA from being mounted in areas that have a reasonable expectation of privacy. For example, any outdoor patio area that might be a private rest area.

    - Locations such as parking garages, entrance points, exit points, etc. can be considered permissible locations to mount cameras. However, it must be publicly posted to make it clear to patients that the area is being watched by a surveillance system.
- HIPAA requires healthcare facilities to identify if any cameras are installed in physical spaces that have access to Personal Health Information (PHI). Some examples include but are not limited to labs, operating rooms, nurses' stations, or any other areas where the camera may have a view of the computer screens displaying the patient's PHI.
    - The use of privacy masks to block the camera's view of computer screens can be applied. Additionally, limiting/restricting access to the video is also another method that can be used in scenarios where this might be unavoidable.
- If video recordings are to be used for educational purposes, clearly expressed approval must be received from each patient before being recorded.
- The facility staff are prohibited from accessing recorded video surveillance to gather information on patients or from their personal devices.
- Recording audio of conversations between patients, between staff, or interactions between patients and staff have the potential to create legal and ethical implications. Each patient must know that they will be recorded and provide clearly expressed approval before being recorded.

Guidelines for Facility Staff

To ensure that video surveillance follows HIPAA and that the privacy of patients, staff, and the general facility are respected, consider the following:

1) Identify what data needs to be recorded, the intended purpose of the data, and if there are any other options for achieving the intended purpose ethically without using the surveillance system.
2) Understand what you are recording. Identify if any camera views may expose patient privacy.
    a. Bathrooms.
    b. Changing rooms.

    c. Staff computers and other display monitors, where patient information may inadvertently be recorded.

3) Secure the storage of any video (including archived and/or exported copies).
    a. Limit access to recorded footage. Cameras that are used for patient monitoring should only be accessible to appropriate clinical staff. Access should NOT be available for any staff or personnel that are not assigned for this purpose.
    b. Do NOT access security systems using personal devices such as mobile phones, tablets, laptops, or remotely from home computers.
    c. Any security workstations that will be used to monitor live camera video or to view recorded video must be placed in a restricted area to avoid accidental viewing by unauthorized personnel such as unassigned staff, patients, etc.
    d. It is highly recommended to encrypt and password protect video footage, especially in cases where recorded video has been exported.
4) Consider the implementation of multi-factor authentication and advanced password protection practices to secure access to surveillance software.
5) Keep an audit log of all staff and personnel who access the system and video recordings.
6) It is recommended that the security system and its associated devices are NDAA-compliant.
7) If the device or system is equipped with extra privacy settings, such as the ability to identify a person's face and redact/pixelate their identify, it may be worth considering to enable such features.

The above information includes some of the limitations and guidelines of using security surveillance systems and devices. For more in-depth information, please consult the proper legal authority of the medical group to ensure that HIPAA compliance is being met.

For More Information or Technical Support

DW Technical Support: 866.446.3595 (option 4)

https://www.digital-watchdog.com/contact-tech-support/

DW Sales: 866.446.3595 sales@digital-watchdog.com www.digital-watchdog.com