Health System Risk Management - Guidance

Ask ECRI: Best Practices When Using Security Cameras

Published 7/24/2023

A member recently asked about best practice recommendations when using mounted video cameras for security purposes in a hospital and on the grounds, including notice of video surveillance for nontreatment purposes. In our response we provide considerations for related policies and procedures, signage and consent, privacy, and storage or retention of recordings.

Policies and Procedures

According to a MedPro Group article, providers should seek to balance security concerns with an obligation to safeguard patients' protected health information (PHI) and comply with Health Insurance Portability and Accountability Act (HIPAA) requirements when using security cameras. They should also determine the legality and appropriateness of live video monitoring versus recording in their state. Once a video surveillance program is planned, a written policy should address:

- The purpose of the surveillance
- The locations of security cameras
- Posting of signage stating that security cameras are in use
- Method of notifying employees of the surveillance
- System security
- Privacy considerations
- Archiving

The International Association for Healthcare Security and Safety's (IAHSS) Security Design Guidelines for Healthcare Facilities (purchase required) contains several recommendations regarding security cameras, including potential locations in which security cameras may be indicated. In addition, conducting a security risk assessment can help identify potential locations for security camera placement. See the guidance article Hospital Security for more information on conducting such assessments.

© 2024 ECRI

Signage and Consent for Patients, Visitors, and Employees

Citing a California Dental Association article and a Cooperative of American Physicians article on security cameras in dental and physician offices, the MedPro Group article suggests informing patients and employees of security camera use in the facility. Providers should post signage indicating that security cameras are in use, and they should consider the need to post signs in additional languages, taking care to follow any state-specific requirements. Providers may consider having patients sign consent forms stating that video surveillance is in use and indicating how long the organization will store video that may include recordings of patients.

Employers should also inform all employees, in writing, that surveillance cameras are being used in the hospital. The employer should have employees sign an acknowledgment form and should file the signed form in their human resources file.

Privacy

An article on a law firm website states that, generally speaking, cameras in public areas do not invade individuals' privacy because people don't have an expectation of privacy in public. Most hospitals, nursing homes, and skilled nursing facilities use surveillance cameras for security purposes in the public areas of their facilities. However, use of cameras in private patient care areas without patient consent may violate HIPAA. In addition, states may have laws that provide additional protection to health information beyond HIPAA protections.

The Centers for Medicare and Medicaid Services (CMS) also addresses patient privacy. The Patient's Rights Condition of Participation for hospitals states, "The patient has the right to personal privacy" (42 CFR § 482.13[c][1]). According to CMS's surveyor guidance for hospitals, this right includes, at minimum, that "patients have physical privacy to the extent consistent with their care needs during personal hygiene activities (e.g., toileting, bathing, dressing), during medical/nursing treatments, and when requested as appropriate."

If it does not include recording, audio or video monitoring of patients in medical-surgical, intensive care, or similar units would not be considered a violation of the patient's privacy if there is a *clinical* need, the patient or their representative is aware of the monitoring, and the public can't readily see the monitors or hear audio, the guidance states. Video recording of patients undergoing medical treatment requires the consent of the patient or their representative. A patient's right to privacy may also be limited if they must be continuously observed for their safety (e.g., in cases of simultaneous restraint and seclusion or suicide precautions). However, these circumstances fall outside video monitoring strictly for security purposes.

Other privacy-related laws could come into play as well, and some such laws may protect other individuals, including visitors, employees, and vendors. For example, state invasion-of-privacy laws may apply to a wide variety of situations. In addition, the law firm article notes that cameras that record audio may raise risks of violating state eavesdropping or wiretapping laws. While some states allow a conversation to be recorded if one person consents, others require all parties to the conversation to consent for the conversation to be recorded.

Employees have unique privacy rights. According to an UpCounsel article on employee privacy rights, employers may use cameras to monitor their employees for security and employee safety. However, employers are required to notify everyone in range of the camera that their property is

© 2024 ECRI

under video surveillance. According to the article, "surveillance cameras must only be used where there is a legitimate business need to deter violence or theft (including internal theft) or to monitor employee productivity, and they generally may not be used in break rooms, restrooms, locker rooms, or other locations where it is reasonable to expect privacy." Additionally, the National Labor Relations Act bars employers from monitoring employees' union activities. However, hospitals should consider seeking legal advice on which privacy laws apply to their specific circumstances and how they affect security camera use.

Storage and Retention of Recordings

For organizations that record footage, the written policy should address secure storage, maintenance of footage showing incidents, and roles or positions that will manage the system and have access to files in specified circumstances, according to the MedPro Group article. The policy should also include procedures addressing when and how recorded videos may be retained and released. The procedures should address how the organization will respond to legal and patient requests to view or obtain a copy of surveillance recordings, which may vary based on state law. The article suggests consulting an attorney, professional liability carrier, or compliance officer to discuss recording and HIPAA compliance issues.

Additional Suggestions

Additional suggestions from the aforementioned resources include the following:

- When choosing, installing, and maintaining a video surveillance system, consider:
    - Cybersecurity risks
        - As described in a 2021 Fierce Healthcare article, hackers accessed the live feeds of 150,000 surveillance cameras, including cameras inside hospitals.
    - Burden on the hospital's bandwidth
    - The potential for signal interference or transmission between the video surveillance system, medical devices, hospital information systems and networks, and devices brought in by patients (e.g., cell phones, tablets)
    - The need for system redundancy in the event of an outage
- Don't place security cameras in areas where patients and employees have a reasonable expectation of privacy (e.g., exam rooms, other private care areas, bathrooms, employee break rooms).
- Ensure that security cameras are visible, not concealed.
- Ensure that security camera placement will not capture PHI (e.g., on computer monitors, on charts).
- Protect the cameras' physical security (e.g., placement in a locked or tamperproof housing) and electronic security.
- Provide lighting in areas under video surveillance that supports optimal image clarity (e.g., neither too dark nor "washed out").
    - Consider the need for night vision cameras in certain outdoor areas.
- Place video surveillance monitors at nursing stations where indicated (e.g., infant and pediatric care areas).

© 2024 ECRI

- Consider integrating video surveillance with other functions (e.g., access control, infant security, parking access and egress, PHI protection, debit card functions, time and attendance).
- Include access to video surveillance systems in the emergency operations center.

The recommendations contained in Ask ECRI do not constitute legal advice. Facilities should consult legal counsel for specific guidance and develop clinical guidance in consultation with their clinical staff.

TOPICS AND METADATA

Topics

Culture of Safety; Emergency Preparedness; Environmental Health; Equipment and Facility Planning; Facilities and Building Management; Quality Assurance/Risk Management; Security/Safety; Workplace Violence

Roles

Clinical Practitioner; Healthcare Executive; Legal Affairs; Patient Safety Officer; Quality Assurance Manager; Regulator/Policy Maker; Risk Manager; Security Personnel

Information Type

Guidance

Publication History

Published July 24, 2023

RELATED RESOURCES

- Resource Collection: Security
- Photography, Filming, and Other Recording of Patients
- Hospital Security
- Self-Assessment: Hospital Security

© 2024 ECRI