



The Finer Points of Video Surveillance in an Urgent Care Center

Urgent message: The increasing use of video surveillance in urgent care requires an awareness of the risks and restrictions of such systems used for patient and employee safety.

■ ALAN A. AYERS, MBA, MAcc

Security is one of the most significant concerns in the operation of an urgent care facility. In this instance, it's not data security or HIPAA compliance, but rather the physical security and safety of employees and patients that leads some operators to install surveillance systems. In doing so, it's essential to recognize both the benefits and the potential risks involved.

Benefits

A digital video surveillance system can capture images and videos stored or delivered offsite via a communication network.¹ Typically, these systems allow for recording via a digital video recorder (DVR) for archiving and the review of specific time frames and incidents. Plus, now with smart technology, many video surveillance systems have the ability to live "stream" footage and to be managed from a mobile device.

A digital video surveillance system can be used to safeguard employees and patients, and to deter theft or other unwanted or illegal behavior.

Urgent care centers in larger communities may have issues with unwelcome solicitors, vagrants, or potential criminals.² Whether by a simple IP (internet protocol) camera network or a more elaborate CCTV (closed circuit television) set-up, an urgent care center will see the benefits in employee and patient safety.

A digital video surveillance system gives an urgent care operator the ability to remotely monitor a center and provide evidence for investigations into crimes and safety incidents. In addition,

there is an operational benefit of implementing a system, as managers and owners can monitor customer service flow and wait times, as well as employee productivity and behavior.³

Legal Considerations

There are special considerations that exist for the use of video surveillance in healthcare settings when compared to another retail property or service environments. The primary legal concern is *patient privacy*. For example, a California healthcare facility may have violated HIPAA when it released video surveillance footage to an attorney. In that case, the hospital placed *hidden* cameras in the operating room. Neither the staff nor the patients were notified of surveillance cameras in use to record surgical procedures.⁴ Although the administration installed the cameras in an attempt to thwart drug theft by doctors and staff, the surreptitious way in which the hospital used the surveillance system resulted in legal problems, both in terms of civil liability and state and federal agency investigation.^{5,6} Such conduct may result in the imposition of sanctions by the Health and Human Services Office of Civil Rights for HIPAA infractions.

The laws of California, New York, and Rhode Island prohibit hidden video cameras in locations where individuals expect complete privacy, and Connecticut and Delaware statutes require businesses to notify employees and customers of video cameras in bathrooms and changing rooms.⁷

Other privacy concerns

Beyond HIPAA, patients who visit an urgent care center have a reasonable expectation of privacy in a public place.

Likewise, staff members also have privacy rights. Surveillance cameras should be placed only in common or public areas, such as the facility lobby, hallways, and other public spaces like en-



Alan A. Ayers, MBA, MAcc is Chief Executive Officer of Velocity Urgent Care and is Practice Management Editor of *The Journal of Urgent Care Medicine*.

trances and parking lots. Cameras should not be placed in treatment rooms, offices, conference rooms, and break areas.

While video surveillance may be helpful in monitoring staff behavior, owners should recognize that employees still have privacy expectations at work. To that end, cameras at the entrance may be permitted to monitor employees on smoke breaks or at the reception area to observe their interactions with the public, but surveillance cameras in treatment rooms, break areas, and bathrooms will certainly run afoul of state law.

Using a surveillance system that records audio may also be considered eavesdropping or wiretapping, depending on the circumstances of the conversation.⁸ Many states make a distinction between audio and video recordings, requiring “dual consent,” or permission from the person being recorded, before audio recording is permitted.

Another concern for owners of urgent care facilities is whether there is a requirement for signage where video surveillance is being used. Typically, video surveillance systems that are used by businesses are coupled with a video surveillance notice (for example, a sign saying “All activities monitored by video surveillance”). However, there is little guidance from state and federal governments on the issue of notification.⁹ Currently, a business owner is not legally required to post these signs for public area surveillance.¹⁰ But note that posting signs will not excuse an urgent care owner from liability for installing cameras or video recording in areas or circumstances where it’s prohibited by law.

Risks of Video Surveillance

There are several risks with implementing a video surveillance system in an urgent care facility. Owners and operators should recognize these and plan their security programs accordingly.

Access to the footage should be limited to key personnel, such as the owner, HR manager, and operations director. As with electronic medical records and other health and business information, access should be based on a demonstrated need, and only to the specific footage needed to address a patient, safety, or compliance concern. Access should be via a company device on a secured network. Any other personal access to either the live stream or archived footage should be restricted. Access privileges assigned to one individual may not be delegated to anyone else, and dual presence should be considered when reviewing archived footage.

Video surveillance can be a critical component of an urgent care’s security plan; however, it should not be a substitute for physical security on the premises. Owners run the risk of an overreliance on technology, and they shouldn’t be tempted to eliminate other security policies and procedures in place, ranging from physical locks to hired security guards.

Other technological issues may be concerns. They include people tampering with security cameras—repositioning camera

“While video surveillance may be helpful in monitoring staff behavior, owners should recognize that employees still have privacy expectations at work.”

angles, erasing stored footage, and damage to the systems hard drive and other components. Urgent care owners should take steps to physically safeguard the system to be certain of an uninterrupted signal.

Finally, circuitry, the internet, and smart technology all are susceptible to bugs, power outages, software glitches, and other anomalies. A back-up system and redundancies can help an urgent care center maintain uninterrupted monitoring and recording of its operations.

Takeaway

While there are some laws concerning video surveillance, much of its use centers upon common sense and reasonable privacy expectations for urgent care employees and patients.

An urgent care center may consider creating a written policy and informing its employees about the existence of cameras. Frequently, this type of notice will defeat an invasion of privacy claim, as employees are less apt to pursue such an action if they’ve been warned. ■

References

1. Techopedia. Digital video surveillance system. Available at: <https://www.techopedia.com/definition/4703/digital-video-surveillance-system>. Accessed January 7, 2019.
2. Videosurveillance.com. Video surveillance for offices. Available at <https://www.videosurveillance.com/office.asp>. Accessed January 7, 2019.
3. Videosurveillance.com. Video surveillance for hospitals. Available at: <https://www.videosurveillance.com/hospital.asp>. Accessed January 7, 2019.
4. HCPro. Unauthorized video surveillance may lead to HIPAA violation. June 3, 2016. Available at: <http://www.hcpro.com/HOM-327029-6962/Unauthorized-video-surveillance-may-lead-to-HIPAA-violation.html>. Accessed January 7, 2019.
5. Clark C. Sharp hospital apologizes for privacy breach as video sting provokes backlash. KPBS Radio News. May 19, 2016. Available at: <https://www.kpbs.org/news/2016/may/19/sharp-hospital-apologizes-privacy-breach-video-sti/>. Accessed January 7, 2019.
6. Clark C. Physician’s lawsuit says Sharp Grossmont endangered patients, reinstalled secret video cameras. inewssource. February 2, 2017. Available at: <https://inewssource.org/2017/02/02/physicians-lawsuit-points-to-unsafe-hospital-practices/>. Accessed January 7, 2019.
7. Videouniversity.com. Video surveillance laws. Available at: <https://www.videouniversity.com/articles/video-surveillance-laws/>. Accessed January 7, 2019.
8. Smith ML. Video surveillance in patient care areas. *Advance for Respiratory Care and Sleep Medicine*. July 26, 2012. Available at: <http://respiratory-care-sleep-medicine.advanceweb.com/Columns/Legally-Speaking/Video-Surveillance-Patient-Care-Areas.aspx>. Accessed January 7, 2019.
9. My Security Sign. When to post video surveillance signs. Available at: <https://www.mysecuritysign.com/mss/posting-video-surveillance-signs.aspx>. Accessed January 7, 2019.
10. Spengler T. If I put up surveillance cameras, do I need to post a sign? *LegalBeagle*. Updated December 12, 2018. Available at: <https://legalbeagle.com/7452958-put-do-need-post-sign.html>. Accessed January 7, 2019.