

Client Brief

August 4, 2026

Topic: Surveillance cameras

Background: Property owners' use of video surveillance cameras in and around businesses and homes has become increasingly more prevalent over the last decade as the cost of these cameras continues to decrease, and more and more owners begin to realize the benefits of detecting (and recording), suspicious activity, crimes, accidents, etc. around their property. Businesses, and especially medical practices, must be careful, however, with respect to the placement of video surveillance cameras and how/where the recorded video footage is stored.

Benefits: I have triaged several claims over the last few years where video surveillance cameras recorded, for example, (i) the theft of an office HVAC system (helping the police catch the suspect), (ii) a patient tripping over a sidewalk curb (thwarting a potential trip & fall claim against the facility), and (iii) a patient reaching through the front desk, check-in window, grabbing stacks of patient records in anger when the receptionist left to get a manager because the patient was becoming increasingly more belligerent about the status of her prescription. In this last example, the practice shared the video footage with the local police, including outside footage of the patient leaving the practice and getting into her car, helping them locate and arrest her just a few hours later. This quick response also helped the practice recover all of the stolen patient information (i.e., the records that the patient grabbed from the receptionist's desk) and, consequently, mitigate their HIPAA breach claim.

Camera

Considerations: You should not place video surveillance cameras in, or facing, a location where there is an expectation of privacy. In Georgia, “[i]t shall be unlawful for ... [a]ny person, through the use of any device, without the consent of all persons observed, to observe, photograph, or record the activities of another which occur in any private place and out of public view...” [emphasis added].¹ Therefore, you should not place cameras in patient examination rooms, bathrooms, changing areas, lactation rooms, etc. You should also take into consideration the public relations aspect of installing cameras, both with your patients and office staff. For example, your employees could construe having their daily activities video recorded as distrustful and perceived dishonesty, leaving them disgruntled and prompting them to look elsewhere for employment. Similarly, patients may find it distasteful that “Big Brother” is recording them in a place that they presumed was very private and confidential.

Video

Storage: The recorded video images of your patients at your medical office are Protected Health Information (PHI) and thus subject to HIPAA rules. Because it would be difficult, if not impossible, to separate the video recordings of patients from non-patients, you should treat all video recordings as PHI and protect it accordingly. Moreover, to the extent that a video recording captures relevant treatment information about a patient (e.g., a patient is observed on video limping after telling the provider that they have no issues ambulating), that footage must be placed in the patient's medical chart, either through saving a clip of the actual video or transcribing the recording.

¹ O.C.G.A. § 16-11-62 (2).

Advice:

Develop a video surveillance recording and storage policy that addresses, among other things: (i) the purpose of the surveillance; (ii) how many surveillance cameras will be used and where they will be located and facing; (iii) where the video recordings will be kept (e.g., the cloud, on a hard-drive, etc.); (iv) how long the recordings will be stored (e.g., 30 days) and how they will be deleted - automatically or manually; (v) who within the practice has the right to access the recordings and how; and (vi) which vendor(s) will be involved in the installation of the video cameras and the storage of the video recordings (closely review the vendor agreements and make sure that you have a Business Associate Agreement with the video storage vendor).

You should also place signs around the office (inside and outside) informing patients, visitors, and others that certain areas around the medical office are under video surveillance, and provide a reason for same (e.g., staff and patient safety, and to prevent theft).

If you have questions about this Client Brief, please feel free to contact:

*Brent Reece
Director of Risk Management and Claim Advocacy
Email: breece@sspins.com
Phone: (706) 300-2033*

Disclaimer: Nothing herein should be considered, construed, or interpreted as legal advice. Rather, this material was developed strictly as a risk management resource pursuant to your insurance broker agreement with Sterling Seacrest Pritchard. You should consult with an attorney concerning this matter and any advice, suggestions, and comments provided herein. We do not make any guarantees, express or implied, that following this guidance will prevent or protect you against an invasion of privacy claim or cyber/regulatory violation, or mitigate the outcome of same.