

Security cameras are a critical part of clinic safety and security protocols. They help deter theft, monitor patient and staff safety, and provide valuable evidence in incidents. However, with their increasing use comes a responsibility to handle recorded footage thoughtfully, balancing security needs against privacy and data protection concerns.

In this post, we'll explore how clinics can define an effective **rolling retention clinic** policy for their **cctv retention period**. We'll look at best practices like *data minimization*, *purpose-first camera justification*, *smart camera placement*, and keeping clear documentation of *field-of-view reviews*. We'll also highlight tools such as **Gallio PRO** for on-premises visual redaction and the importance of **role-based CCTV user accounts** instead of shared passwords to improve security and accountability.

Understanding the Importance of a Delete Footage Policy

First things first: if your clinic doesn't have a **delete footage policy** in place, it's time to make one. Retaining CCTV footage indefinitely "just in case" it might be needed later is a significant privacy risk and can lead to larger data management headaches.



A delete footage policy clarifies:

- How long footage is kept before being automatically deleted or overwritten.
- Who can access and review footage, and under what circumstances.
- The process for securely deleting footage when retention periods expire.
- Guidelines around redacting sensitive information when sharing or archiving footage.

Having a documented policy also supports compliance with privacy regulations and reassures patients and staff that their data is handled responsibly.

Data Minimization: Collect Only What You Need

Data minimization is a foundational privacy principle: collect and keep only the data you absolutely need for your defined security purposes.

How Does This Apply to Clinic CCTV?

- **Limit recording to public, common areas**—avoid positioning cameras where private conversations, patient paperwork, or computer screens are routinely visible.
- **Review camera angles regularly** to ensure they focus strictly on required areas (e.g., entrances, waiting rooms, reception), rather than overshooting into private zones.
- **Consider the minimum quality and frame rate** needed to identify subjects or incidents without capturing unnecessary detail.

This helps prevent inadvertent capture of Protected Health Information (PHI) or confidential discussions and reduces the amount of footage you must manage and safeguard.

Purpose-First Camera Justification

Before installing new cameras or expanding coverage, ask: *What incident are we trying to solve?* Every camera should have a clear security or safety purpose tied to a documented clinic risk.

- For example, a camera monitoring the medication dispensing area to deter theft.
- A camera near the main entrance to monitor visitor flow and access control compliance.
- A camera at the cash drawer angle to reduce the risk of theft or cash handling disputes.

Documenting camera purposes ensures that each recording is justified, reduces unnecessary surveillance, and helps configure retention settings appropriately.

Best Practices in Camera Placement

Proper camera placement directly impacts your compliance with privacy rules and reduces the risk of over-collection of data.



Tips for Clinic Camera Placement:

- **Avoid pointing cameras at monitors or paperwork:** Reception cameras should be angled to observe the reception area—not the computer screens or patient forms.

- **Prevent capturing badges or ID details:** Design angles so that name tags or badges are not easily readable, unless absolutely necessary for investigations.
- **Label your cameras clearly:** Use staff-friendly labels like “Camera 2 - Front Desk Entrance” or “Cash Drawer Angle” to avoid confusion during footage retrieval or audits.
- **Limit the field of view:** Use physical barriers or adjust zoom to exclude sensitive zones from visible areas.

Field-of-View Reviews and Documentation

It’s not enough to set up cameras and forget them. Regular *field-of-view reviews* help ensure ongoing compliance with policy and adapt to clinic layout changes.

These reviews should be documented thoroughly, including:

Date	Camera Label	Reviewer	Field-of-View Description	Adjustments Needed	Notes
2024-05-15	Camera 2 - Front Desk Entrance	Operations Manager	View covers entrance and waiting area; no display screens visible	None	Clear view maintained, privacy preserved
2024-05-15	Cash Drawer Angle	Security Lead	Focuses on cash drawer; badge details partially visible	Adjust angle to reduce badge visibility	Scheduled adjustment for next quarter

Keeping detailed logs improves [waiting room camera height](#) accountability, aids audits, and provides evidence of ongoing privacy efforts.

Choosing the Right Retention Period

So, what is a reasonable **cctv retention period** for clinics? While regulations vary by jurisdiction, here are common considerations to guide your decision:

- **Purpose-driven retention:** Footage should be kept only as long as necessary for its intended security use, such as incident investigation or compliance review.
- **Typical retention ranges:** Many clinics keep footage for 14 to 30 days on a rolling basis before automatic deletion or overwriting.
- **Extended retention for incident footage:** If an incident occurs, relevant footage must be saved securely until the case is resolved; this should be documented.
- **Reduce ‘just in case’ retention:** Avoid indefinite keeping of footage “just in case.” Establish clear rules and deletion schedules.

Example Rolling Retention Schedule

Footage Type	Retention Period	Notes
Routine daily footage	21 days (rolling)	Automatically deleted after 3 weeks unless flagged
Incident footage	90 days (or until resolution)	Manually flagged by authorized user; securely archived
Footage with sensitive patient info	Varies, minimize retention	Use redaction tools (see below) before storage

Leveraging Gallio PRO for Privacy-Safe Video Handling

When your footage does capture sensitive information accidentally — such as faces of patients, badges, or paperwork — using tools like **Gallio PRO** can help minimize privacy risks.

- **On-Premises Visual Redaction:** Gallio PRO enables clinics to automatically anonymize video data on-site before storage or sharing.

- **Precise Anonymization:** Faces, badges, and documents can be blurred or pixelated to maintain privacy.
- **Simplified Compliance:** This approach facilitates compliance with HIPAA and other privacy regulations by reducing exposure of personal health information.
- **Staff Training:** Train designated users to perform redactions easily when incidents require footage review or sharing.

Role-Based CCTV User Accounts: Security and Accountability

Another common problem in clinic CCTV management is the use of shared passwords for systems. This practice reduces security and prevents accurate audit trails.

Why Role-Based Named Accounts Matter:

- **Individual Accountability:** Each user logs in with their own credentials, making access traceable.
- **Granular Access Control:** Permissions can be set based on staff roles—view-only for some, download rights for investigators, etc.
- **Password Management:** Users can update their credentials without disrupting workflow.
- **Audit Logs:** Comprehensive logs of who accessed what footage and when improve security.

Implementing role-based user accounts is a low-effort, high-impact way to improve your clinic's CCTV governance.

Summary: Practical Steps to Implement Effective CCTV Retention

1. **Define the purpose** of every camera before installation and document it.
2. **Review and adjust camera placement** regularly to avoid unnecessary coverage of private areas or monitors.
3. Adopt **data minimization** principles by limiting footage captured and quality settings.
4. Create a clear **delete footage policy** with defined rolling retention periods (commonly 14-30 days), and extended retention for flagged incidents.
5. Utilize tools like **Gallio PRO** for on-premises visual redaction to protect sensitive info before storage or sharing.
6. Replace shared passwords with **role-based CCTV user accounts** to enhance security and accountability.
7. Conduct and document **field-of-view reviews** at regular intervals.
8. Train your staff on privacy-safe workflows that can be realistically followed during busy shifts.

Final Thoughts

Balancing security needs and privacy protection is challenging but achievable. A thoughtful approach to CCTV retention, coupled with practical tools and clear policies, safeguards your clinic's patients and staff while staying compliant with regulations.

Remember: *What incident are we trying to solve?* Asking this simple question before every camera decision and footage retention policy ensures your operations remain focused, safe, and privacy-aware.

For clinics looking to upgrade or audit their CCTV workflows, these tips and tools can serve as a practical, privacy-safe framework to manage recorded footage effectively without over-retention or unnecessary data risk.