

Clinic CCTV footage is a sensitive data asset that requires careful handling to balance privacy, compliance, and operational needs. One of the trickiest situations comes when a patient requests their footage just before the system's automatic overwrite cycle erases it. This is a high-stakes moment, demanding swift action following established protocols to ensure footage is preserved securely, privacy is maintained, and the incident is properly documented.

Understanding the Scenario: The Overwrite Risk Check

CCTV systems in clinics often operate with limited storage capacity, following data minimization [redact patient info on video](#) principles to avoid keeping footage longer than necessary. A common policy might be to overwrite video files after 7-14 days unless flagged or exported. This data retention strategy reduces unnecessary exposure of sensitive information and helps keep us compliant with privacy laws like HIPAA.



However, if a patient requests footage near the end of this retention period, staff must perform an **overwrite risk check** immediately. Simply put, you need to verify how much time is left before the relevant files are erased and then take rapid steps to preserve that footage.

What Incident Are We Trying to Solve?

Before jumping to technical solutions, it's critical to understand the nature and purpose of the footage request. Is the patient requesting footage to confirm an incident, investigate a complaint, or verify an event? Knowing this helps apply the principle of *purpose-first camera justification* that guides when and how we save footage.

- Does the camera footage capture the necessary event or area?
- Is the requested footage relevant to the patient's specific request?
- Are we preserving video beyond what's needed, risking over-collection?

This focused approach aligns with **data minimization** – collecting and retaining only what is necessary to resolve the incident.



Step-by-Step Guide: Preserve Footage Step When Request Is Just Before Overwrite

1. **Perform Overwrite Risk Check** Immediately check the system's timestamp for the requested footage. Identify how soon it will be overwritten.
2. **Determine Camera Field-of-View Suitability** Review the documented camera placement and their field of view to confirm which camera angles are relevant. Avoid preserving footage that does not capture the incident or patient's presence.
3. **Escalate Immediately** Notify the designated privacy officer or security lead right away. They should have direct access to export footage quickly and securely.
4. **Export and Preserve Footage Securely** Use on-premises visual redaction and anonymization software like **Gallio PRO** to mask any unrelated individuals or sensitive information within the footage before sharing.
5. **Log Incident Details** Record a short incident note describing the request, overwrite risk, actions taken, and persons involved. This note provides an audit trail and accountability.
6. **Follow Up With Patient** Confirm with the patient how the footage will be used, ensuring compliance with clinic privacy guidelines and obtain any necessary consent.

Why Gallio PRO Helps

Gallio PRO is a critical tool in this workflow because it supports *privacy-safe workflows*. Instead of sharing raw footage with hard-to-blur identities or background paperwork visible, Gallio PRO allows you to:

- Apply automated or manual redaction to protect patient and staff privacy
- Anonymize faces not involved in the incident
- Ensure that only the footage relevant to the incident remains visible
- Export footage in a secure, controlled way to authorized individuals

This approach addresses one of my pet peeves: reception or waiting-room cameras pointed at monitors or paperwork. With Gallio PRO, you can blur those elements so protected health information isn't exposed inadvertently.

Role-Based CCTV User Accounts: No More Shared Passwords

One crucial security and privacy practice is implementing **role-based CCTV user accounts**. Clinic staff should never use shared passwords to access the CCTV system. Instead, assign named accounts with specific permissions based on roles. Benefits include:

- Clear accountability — you know who accessed footage and when
- Limits on who can export or delete files
- Reduces risk of unauthorized access or accidental sharing
- Easier audits when responding to requests or incidents

By mandating named accounts, the clinic enhances operational security and builds trust with patients about how their data is protected.

Camera Placement, Field-of-View Reviews, and Documentation

Prevention is as important as response. Regular audits of **camera placement** and **field-of-view documentation** help minimize over-collection and unnecessary data exposure.

- **Avoid pointing cameras at:** monitors, front desks with patient information, staff badges, or private conversations
- **Ensure cameras cover only areas necessary for safety and security:** entrances, waiting rooms, hallways
- **Maintain up-to-date diagrams and field-of-view reviews** documenting what's visible, updated after any relocations or equipment changes

This ongoing diligence supports privacy by design principles, reducing the likelihood that irrelevant information is captured or saved.

Summary Table: Key Actions When Patient Requests Footage Near Overwrite

Action	Description	Why Important	Overwrite Risk	Check	Check time left before footage is auto-erased	Determines urgency and whether footage is salvageable
Field-of-View Review	Confirm which cameras recorded relevant footage	Prevents over-collection and privacy violations	Escalate Immediately	Notify privacy/security lead to act fast	Ensures footage is preserved before deletion	Use Gallio PRO
Redact and anonymize footage before export	Protects privacy of unrelated individuals	Log Incident Notes	Document request and response details	Creates audit trail and accountability	Role-Based User Accounts	Use named accounts, no shared passwords
Improves security and tracks access						

Conclusion

When a patient footage request arrives right before the system overwrites files, the clock is ticking. Staff must act swiftly with a clear, purpose-driven process to preserve only what's necessary, maintain privacy, and follow compliance protocols.

Implementing tools like **Gallio PRO** for visual redaction, enforcing **role-based user accounts**, and conducting regular **field-of-view reviews** dramatically improve the clinic's ability to protect sensitive information while responding effectively to patient requests.

Remember always to ask at the outset: *“What incident are we trying to solve?”* This question guides thoughtful data collection, minimizes privacy risks, and keeps clinic operations running smoothly during even the busiest shifts.