Clinic operations managers and staff often grapple with the tricky balance between safety, privacy, and practical surveillance. A common question we get: *"Can I place a CCTV camera at the entrance if it also shows the whole waiting room?"* While it might seem efficient to have a single camera covering both areas, the answer depends heavily on privacy principles, regulatory standards, and practical tech use. This post breaks down the key considerations and best practices for effective, privacy-safe clinic CCTV setup.

Why Data Minimization Matters in Clinic CCTV

Before we even talk about camera angles, let's get one principle crystal clear: **Data minimization.** This is a core privacy concept which says you should only collect what's necessary for your specific purpose — nothing extra. For clinics, that means avoiding unnecessary capture of patient faces, badges, or paperwork.

- **Over-collection risks:** Privacy breaches, complaints, unnecessary storage costs.
- **Legal compliance:** Health Information Privacy laws often require minimization and secure handling of video data.
- **Staff trust:** Protecting your team's privacy improves morale and reduces risk.

In practice, this means thinking carefully before pointing that camera in just anywhere. Does your monitoring genuinely need to include the entire waiting room, or can a narrow focus on the entrance suffice?

Purpose-First Camera Justification

Always start with the question: *"What incident are we trying to solve or prevent?"* Common reasons for camera placement include:

1. Monitoring clinic entry and exit points to prevent unauthorized access.
2. Identifying individuals causing safety or security concerns.
3. Tracking patient flow to improve operational efficiency.

If your primary purpose is to keep an eye on the entrance door — for example, to verify who comes in and out — then the camera's field of view should be limited as much as possible to just that area. Extending coverage to the whole waiting room introduces potential risks:

- Capturing detailed images of patients in various states of privacy.
- Recording sensitive conversations or information exposed by proximity.
- Over-collection beyond what's necessary to meet your stated purpose.

This is where *entrance only coverage* and a *narrow field of view* come retain footage after incident into play.

Camera Placement Tips to Avoid Over-Collection

Strategic camera placement reduces privacy risks and helps ensure you only collect what's necessary. Here are some practical tips from the field:

- **Use zoom and angle adjustments:** Make sure "Camera 2" or whichever camera is focused on the entrance doesn't show the whole waiting room. Zoom in on the doorway, avoid aiming at reception monitors or paperwork.
- **Check for close-up faces:** Cameras should not capture people waiting except those entering/exiting within a very narrow angle. Avoid wide-angle lenses here.
- **Regular field-of-view reviews:** Set calendar reminders to review camera angles quarterly or if the clinic lobby layout changes.
- **Document placement and purpose:** Maintain clear notes on why each camera is placed, what it covers, and who has access.

Remember: aim for the minimum field of view needed for your defined security purpose. Less is more.

Field-of-View Reviews and Documentation: A Must-Do

Don't set it and forget it. Camera coverage can creep over time if nobody checks it regularly. We recommend formalizing your reviews as part of your security and privacy policy:

1. **Frequency:** Every 3 to 6 months, or after layout updates.
2. **Checkpoints:** Confirm entrances are clearly covered without unnecessary spill into waiting areas or staff desks.
3. **Update purpose and coverage documentation:** Keep it simple and use plain language that reflects how staff describe areas (e.g., "Camera 2 – cash drawer angle," "Front entrance only").

This practice not only supports compliance but also helps during privacy audits and incident investigations.

Leveraging Technology To Support Privacy

Even with best practices in placement, sometimes you'll need to handle footage where patient faces or sensitive info appear. This is where tools like **Gallio PRO** shine. It's an on-premises software for visual redaction and anonymization that helps clinics mask faces and other private info before footage is accessed or shared.

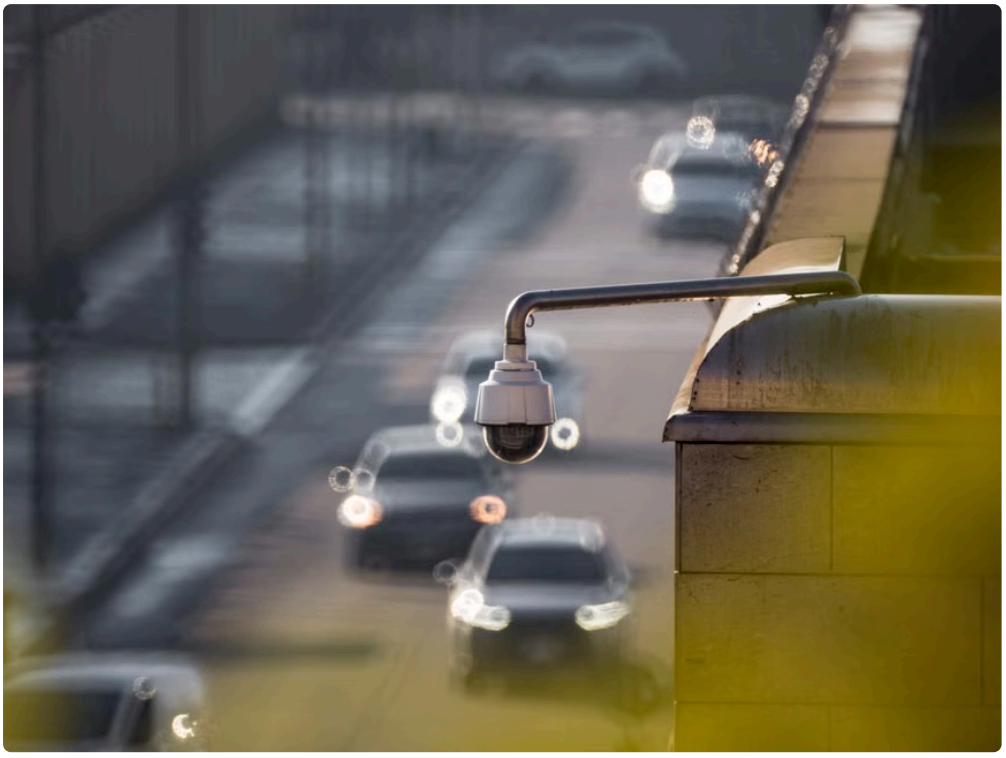
- **Gallio PRO** allows you to:
    - Blur or block faces automatically or manually in recorded videos.
    - Protect badges, documents, and screens showing patient info.
    - Operate fully on-premises—no cloud upload, minimizing data privacy risks.

Combine this tech with good physical placement and you have a privacy-safe CCTV environment.

Role-Based CCTV User Accounts: Why Shared Passwords Don't Cut It

One of the biggest headaches we see in clinic CCTV management is **shared system passwords**.

Why is this bad?



- Accountability evaporates—if something goes wrong, who can you investigate?
- Increased risk of unauthorized access.
- Difficult to enforce data access policies.

Best practice is role-based user accounts with **named users**. This means:

- Each staff member has their own login tied to their role and responsibilities.
- Access rights are limited to only what's needed (e.g., receptionists don't see footage from staff-only areas).
- Audit trails exist showing who accessed which footage and when.

If you want to improve your clinic's camera system today, start by ditching shared passwords and setting up proper role-based access.

Summary Table: Good vs Bad CCTV Practices for Entrance Camera Placement

Aspect Good Practice Bad Practice Camera Field of View Narrow field of view focused on entrance only Wide-angle covering entrance plus whole waiting room Data Minimization Only capture necessary areas, avoid close-up faces in waiting room Record entire waiting room including nearby faces and documents Access Control Role-based, named CCTV user accounts Shared passwords across multiple staff Review & Documentation Regular field-of-view reviews with documented camera purpose One-time setup, no ongoing evaluation or records Privacy-Enhancing Technology Use on-premises tools like Gallio PRO for redaction No anonymization—raw footage shared freely

Final Takeaway

Simply put: it's usually **not okay** to point a camera at the entrance if it also shows the whole waiting room unless you have a very clear purpose and strong privacy safeguards. The key is to minimize data collection, focus the camera's field of view narrowly, regularly review placement, and use technology like Gallio PRO to redact footage before sharing. Also, make sure your CCTV system has role-based user accounts—no shared passwords—so access is secure and auditable.

Following these steps ensures your clinic CCTV protects safety without compromising the privacy your patients and staff rightly expect.

Have questions or want to review your clinic's camera setup? Drop a note with "what incident are we trying to solve?" for custom advice tailored to your situation.