

In busy multi-provider clinics and urgent care suites, reception areas bustle with staff juggling phone calls, insurance questions, and patient check-ins. Cameras installed for safety and compliance are meant to protect patients and staff—but when the reception camera angle includes the computer monitor, it poses a serious privacy risk.

So how do we stop reception CCTV from capturing confidential information visible on computer screens? In this post, I'll walk you through key strategies for **camera angle exclude screen** setups, using tools like *Gallio PRO* for automatic redaction, and why *role-based CCTV user accounts* matter. Plus, we'll cover best practices in **data minimization** and ongoing **field-of-view documentation** to keep your clinic compliant and respectful of patient privacy.

What Incident Are We Trying to Solve?

Before re-angling cameras or buying new software, ask: *why is the monitor appearing in footage, and what risk does it pose?*

- Are patient names, insurance numbers, or other PHI (Protected Health Information) visible on the screen?
- Could unauthorized users access this video and see sensitive data?
- Is the "just in case" footage retention increasing clinic liability?
- Are shared CCTV passwords making audit trails impossible?

Knowing exactly what risk the clinic faces—excessive data capture exposure and poor access controls—helps shape practical fixes.

Purpose-First Camera Justification: Why Is Reception CCTV There?

Reception cameras serve many legitimate purposes like:

- Documenting security incidents
- Protecting staff from verbal or physical abuse
- Monitoring workflow to improve efficiency

But the purpose doesn't extend to capturing computer screens full of sensitive data. According to data minimization principles, the footprint of CCTV should only cover what's necessary.

Example Purpose Statement

"Camera 2 at front desk is positioned solely to observe the patient queue and reception interactions while excluding the computer monitors and paperwork to avoid capturing sensitive information."



Data Minimization: How to Avoid Over-Collection

“Over-collection” means capturing more video than needed, increasing risk and complicating privacy compliance.

- **Avoid aiming cameras at screens.** Adjust the physical **camera angle to exclude the monitor** entirely.
- **Use privacy filters on monitors.** Privacy screen protectors reduce the viewing angle so only the receptionist can see sensitive info.
- **Mask areas in CCTV footage.** When re-positioning isn’t enough, software tools can blur or blackout sensitive sections.

Case Study: Camera 2 Field-of-View Adjustment

Step Action Outcome
1 Reviewed Camera 2 view with staff to identify monitor visibility Confirmed monitor screen is visible in default placement
2 Physical camera angle changed slightly downward and sideways Monitor screen no longer visible in live view
3 Privacy filter added to reception computer screen Screen unreadable from all other angles except receptionist’s chair
4 Footage reviewed and recorded for documentation Filed with system logs as part of compliance record

Field-of-View Reviews and Documentation

Ask yourself this: it’s not enough to fix the angle once and forget it. Regular reviews ensure the camera view stays compliant, especially if desks or equipment are moved.

- **Quarterly camera angle audits:** Check and document current field-of-view for all reception cameras
- **Record findings:** Store screenshots and notes tied to specific camera IDs (e.g., “Camera 2 – cash drawer angle”)
- **Update SOPs:** Include instructions for maintaining “monitor excluded” angles during setup changes or new hires

Good documentation also prepares you for audits or incident investigations with clear evidence of privacy-safe design.

Leveraging Gallio PRO for Visual Redaction

If a camera angle adjustment alone can't exclude the screen—say because space is tight or reception layout is unusual—use **Gallio PRO**, an on-premises video redaction and anonymization tool expressly designed for healthcare environments.

- Automatically **mask areas in CCTV** footage like computer monitors, name badges, or paperwork
- Ensures **no PHI** can be accessed by unauthorized CCTV users
- Processes footage quickly onsite—no data leaves the clinic's secure network
- Allows exporting redacted videos for investigations or reporting with confidence

Gallio PRO helps clinics meet HIPAA and local privacy regulations by removing human error from manual masking.

Role-Based CCTV User Accounts: Stop Shared Passwords

Let me tell you about a situation I encountered learned this lesson the hard way.. One of my pet peeves is seeing clinics use shared passwords for CCTV systems. This practice creates accountability gaps and increases risks.

Instead, set up named user accounts with **role-based permissions** like:

- **Reception supervisor:** Can view live feeds but not export footage
- **Compliance officer:** Can export redacted video clips through Gallio PRO
- **IT admin:** Manages system settings and user access

Benefits of this approach include:



- Clear audit trails showing who accessed or exported footage
- Limiting sensitive footage access to trained personnel only
- Enabling quick user revocation or permission changes when staff roles evolve

Step-by-Step Clinic Workflow Fix Summary

1. **Identify the problem:** Monitor appears in reception camera view (Camera 2)
2. **Confirm what sensitive info is at risk:** Patient data, insurance info, staff badges?
3. **Re-position the camera angle:** Adjust Camera 2 to exclude monitor from view
4. **Add privacy filters:** Place a privacy screen on the monitor for added protection
5. **Review the footage field-of-view:** Document and save screenshots for audit logs
6. **Implement Gallio PRO redaction:** Automatically mask any remaining PHI in video
7. **Enforce role-based accounts:** Set up named users with distinct access rights to CCTV systems
8. **Schedule recurring audits:** Keep camera placement and access permissions in check quarterly

FAQs About Reception Cameras and Monitor Privacy

Do privacy filters really help block screen visibility from cameras?

Yes. Privacy filters narrow the visible angle so only the receptionist can view content clearly. From side angles or cameras, the screen appears black or distorted, protecting sensitive data effectively.

Is it enough to rely on software auto-blur features to protect monitor content?

No. Auto-blur functions are often imperfect and can miss detail, especially for close-up screens. Physical camera angle adjustments paired with dedicated redaction tools like Gallio PRO provide stronger privacy safeguards.

How often should we review camera angles and views?

At minimum, conduct **quarterly reviews**. Any time reception desk layouts change or new equipment is added, immediately reassess camera views.

Can I save “just in case” unedited footage indefinitely?

Absolutely not. Saving excess footage increases the risk of privacy breaches. Retain footage only as long as required by regulation or incident response policies, and use redaction to minimize stored sensitive data.

Conclusion

Reception CCTV is a valuable tool for security and securitysenses.com workflow management, but it must be thoughtfully managed to comply with privacy laws and respect sensitive patient information. The problem of reception cameras catching computer monitors can be fixed through a combination of strategic **camera angle exclude screen** placement, physical **privacy filters for monitors**, and technology like **Gallio PRO to mask areas in CCTV** footage.

Don't overlook **field-of-view documentation** and **role-based CCTV user accounts**—these administrative controls make sure your clinic remains protected and audit-ready.

With these practical steps, clinics can maintain a privacy-safe environment that staff can follow even during busy shifts, avoiding common pitfalls like shared CCTV passwords or excessive data retention. If your reception camera keeps catching the computer monitor, now you know exactly how to fix it.