



VS EVIDENCE MANAGEMENT CASE MANAGEMENT

WHAT YOU NEED TO KNOW BEFORE YOU BUY

Understanding the difference will save you time and money.

If you've ever watched a carpenter show up with only a hammer, you'll notice something interesting.

Every problem starts to look like a nail.

Technology decisions in the justice system sometimes fall into the same trap. A team adopts a system that solves one part of the problem well, and suddenly it's expected to solve everything. Before long, people are stretching tools beyond what they were built to do, and the work starts getting harder instead of easier.

At Guardify, we see this most often when organizations try to force a **case management system (CMS)** to act like a **digital evidence management system (DEMS)** – or vice versa.

They are related.

They should connect.

But they serve very different purposes.

And understanding that difference is one of the most important technology decisions a justice-focused organization can make.

First, Let's Get the Definitions Right

A **Case Management System (CMS)** is exactly what it sounds like; software that helps you manage the entire lifecycle of a case. Who's involved, what

services were provided, what documents exist, what the outcomes were. It's your operational command center. It's where workflows live, reports get generated, and your team coordinates across disciplines. For CACs, this is where you're tracking forensic interviews, therapy referrals, MDT coordination, and outcome data.

A **Digital Evidence Management System (DEMS)** is something different. It's a secure, purpose-built platform for storing, managing, and sharing digital evidence; primarily video. Think forensic interview recordings, body cam footage, court exhibits. The job of a DEMS isn't workflow. Its job is to make sure that evidence is protected, controlled, admissible, and accessible to the right people at the right time.

Think about how a hospital operates. It runs on two distinct systems; one that manages patients and care workflows (admissions, treatment plans, appointments, records), and another that handles diagnostic imaging and clinical evidence (X-rays, MRIs, lab results). You wouldn't ask the patient scheduling system to store MRI scans. And you wouldn't ask the imaging system to run the hospital's patient workflow. The justice system works exactly the same way.

“You wouldn't store sensitive child interview recordings in the same system you use to schedule therapy appointments. And you wouldn't try to generate compliance reports out of a video library. These are different tools, built for different purposes.”

The good news is that a great technology stack has both; and they integrate well. The better news is that knowing exactly what to look for in each makes your vendor conversations a lot sharper.

What to Demand from a Digital Evidence Management System

Let me start here because this is where I see the most risk. Evidence is sacred in the justice system. How your platform handles it isn't just a product feature;

it's a legal and ethical responsibility.

Security and Compliance, Full Stop

Your evidence platform needs to be fully compliant with relevant data protection standards. It needs to meet the security requirements of your accrediting bodies and your state. And here's something we feel very strongly about at Guardify:

your data should never be used to train AI models. Full stop.

This is not a hypothetical concern. Many platforms are building AI features by pushing customer data to large language models; sometimes without clearly disclosing it. In a justice context, that's unacceptable. The platform you choose should have an explicit, contractual commitment that your evidence is not pushed to LLMs, not used to train any AI model, and not sold or shared with third parties. Ask for it in writing. If they hesitate, walk.

⚠️ ASK EVERY VENDOR

Is our data used to train AI models? Is it ever shared with or sold to third parties? Get the answer in writing; not just on a webpage.

Recording Device Integration

Your DEMS should connect natively to the recording equipment you already use, or come fully integrated with a recording solution. Manually transferring interview recordings is a chain-of-custody risk. If your vendor makes you export files to a USB drive and drag them into their system, that's a problem. Look for direct integration or a fully native recording environment.

Streaming Playback; The Right Way

Evidence needs to be viewable without being downloadable by default. That means streaming playback; not download-and-open. This is a critical distinction. Streaming means you control access at all times. The wrong hands never get a local copy they can forward, share, or lose.

Evidence shouldn't travel through email attachments or flash drives. It should stay protected while still enabling the right people to access it; and every single view needs to be logged. Who watched it. When. From where. A

complete, tamper-proof audit trail isn't optional; it's what makes the evidence trustworthy and the chain of custody defensible in court.

Admissibility and Court Readiness

This one sounds obvious, but I can't tell you how many organizations have discovered; late in the process; that their evidence platform didn't have a clear pathway to court verification. The system should be able to generate a verified, court-ready export that demonstrates the evidence hasn't been tampered with. Ask the vendor directly: "Has your platform been used in court proceedings? How does verification work?" If they can't give you a clear answer, that's your answer.

Access Controls and Download Restrictions

Granular permissions aren't a nice-to-have; they're non-negotiable. You should be able to control who can view evidence, who can share it, who can download it, and under what circumstances. Prosecutors need different access than law enforcement. Law enforcement needs different access than advocates. The platform should support that without requiring a workaround.

Nice-to-Have DEMS Features

Once you've covered the essentials, there's a second tier of features that can genuinely transform how your team works: automated transcripts that save hours of manual work, AI-generated insights from video content, the ability to redact sensitive information, in-platform messaging between case stakeholders, tagging and notes for easy organization. These are table-stakes differentiators among the better platforms; but they should never distract from whether the fundamentals are solid.

What to Demand from a Case Management System

Case management is where your team actually works every day. The bar here isn't just "does it have the features"; it's "can my team actually use it without wanting to throw their laptop out the window."

Roles-Based Workflows That Actually Simplify Things

A CMS that shows everyone everything is not a CMS; it's chaos. Your forensic interviewers, therapists, advocates, MDT coordinators, and administrators all have different jobs, different data access needs, and different workflows. The system should reflect that automatically. Role-based access and role-based views are essential, not add-ons.

Customization Without Complexity

Every center is a little different. Your intake process, your service categories, your required fields; they're not identical to the center two states over. A good CMS lets you configure it without hiring a developer. A great CMS lets you do it without even calling support. If a vendor's answer to customization is "we can build that for you," build in a cost and timeline and think hard about whether that's the right partner.

Reporting and Data Querying; This Is the One

I've talked to more center directors than I can count who have told me their previous system couldn't run the reports they needed for grant compliance. This is a disaster. Your CMS needs to be able to collect and organize all the data required for NCA reporting, grant requirements, state requirements, and internal metrics; and it needs to let you run custom queries without calling your vendor every time.

Can you generate a report on all clients served in a given county, by age, by service type, over a rolling 12-month window? Can you do that yourself, today, without a ticket? That question alone will tell you a lot about whether a CMS is actually built for your needs.



TEST THIS IN THE DEMO

During any CMS demo, ask them to run a custom report on the spot using a filter combination you specify. How they respond; and how long it takes; tells you more than any feature sheet.

The Things That Matter for Both

Systems

Real Humans, Real Support; Fast

This might be the thing I care most about, because I've seen it break organizations. When your system goes down at 8am before a scheduled forensic interview, you need a human on the phone; not a ticket queue with a 48-hour SLA. At Guardify, our standard is: a real human responds within 15 minutes. Engineers are on call for technical emergencies. Our field teams have actually worked in CACs and know what a morning like that feels like.

Ask every vendor: What's your first-response SLA? Is it automated or human? What's the escalation path for critical issues? And ask for references who've experienced an urgent support situation; not just references who love the product.

Cloud-Native, Not Cloud-Optional

If a vendor's pitch includes "on-premise options," take note. In 2026, a system that isn't built cloud-first is a system carrying technical debt that will slow you down. Cloud means your team accesses it from anywhere. It means updates happen automatically. It means you're not managing a server in a closet. Mobile apps and desktop apps built on top of a cloud backbone are table stakes; not selling points.

(I asked our IT team if they missed managing on-premise servers. They said they had a lot of feelings about it, but they couldn't access them remotely.)

Onboarding That Actually Sticks

The best system in the world is worthless if your team doesn't use it correctly. Onboarding needs to cover every role; not just your IT admin. Your front desk staff, your interviewers, your advocates, your supervisors, your prosecutors who will access evidence remotely. A vendor that offers "train the trainer" and calls it done isn't set up to actually support your team. Look for structured onboarding with accountability, follow-up, and field experience behind the people delivering it.

The Bottom Line

Case management and evidence management are not the same thing. The best technology outcomes I've seen in this space come from organizations that understand exactly what problem they're solving, ask the right questions, and demand vendors prove their answers; not just assert them.

The checklist below is designed to be your starting point. Print it out. Bring it to every vendor call. And if a vendor can't check every box in the "critical" column, keep looking.

The work you do is too important for technology that lets you down. And when the right systems are in place; built thoughtfully, connected properly, supported by people who actually know this work; the technology fades into the background. **Which is exactly where it belongs.**

The Case Management & Evidence Management Evaluation Checklist

DIGITAL EVIDENCE MANAGEMENT (DEMS)

SECURITY & COMPLIANCE

- Meets applicable compliance standards (HIPAA, CJIS, SOC2, state requirements) **[CRITICAL]**
- Data is never pushed to LLMs or used to train AI models **[CRITICAL]**
- Vendor does not sell or share your data with third parties **[CRITICAL]**
- Evidence is safely stored with documented security controls **[CRITICAL]**

ACCESS & CONTROL

- Granular access controls and permissions by role **[CRITICAL]**
- Ability to restrict or disable downloading by user/role **[CRITICAL]**
- Streaming playback (evidence viewed, not downloaded by default) **[CRITICAL]**
- Full audit logs; who viewed, when, from where **[CRITICAL]**

INTEGRATION & COURT READINESS

- Direct integration with or native support for recording devices **[CRITICAL]**
- Evidence verified and accepted in court proceedings **[CRITICAL]**

NICE TO HAVE

- Automated transcription **[NICE TO HAVE]**
- AI-generated video insights **[NICE TO HAVE]**
- Redaction tools **[NICE TO HAVE]**
- In-platform messaging between stakeholders **[NICE TO HAVE]**
- Tagging, notes, and clip editing **[NICE TO HAVE]**

CASE MANAGEMENT SYSTEM (CMS)

WORKFLOW & USER EXPERIENCE

- Roles-based access and views by user type **[CRITICAL]**
- Highly customizable workflows without developer support **[CRITICAL]**
- Intuitive navigation; customizable but not clunky **[CRITICAL]**

DATA & REPORTING

- Accurate tracking of all required person, service, and case data **[CRITICAL]**
- Run custom queries and ad-hoc reports without vendor help **[CRITICAL]**
- Pre-built reports for grant, NCA, and compliance requirements **[CRITICAL]**
- Document collection and organization within cases **[CRITICAL]**

APPLIES TO BOTH SYSTEMS

SUPPORT & ONBOARDING

- Real human support response within 15 minutes **[CRITICAL]**
- Engineers on call for critical technical issues **[CRITICAL]**
- Field-experienced support team familiar with CAC/LE workflows **[CRITICAL]**
- Full onboarding for all users across all roles **[CRITICAL]**

PLATFORM

- Cloud-native architecture (not just “cloud optional”) **[CRITICAL]**
- Mobile app available **[NICE TO HAVE]**
- Desktop app available **[NICE TO HAVE]**

