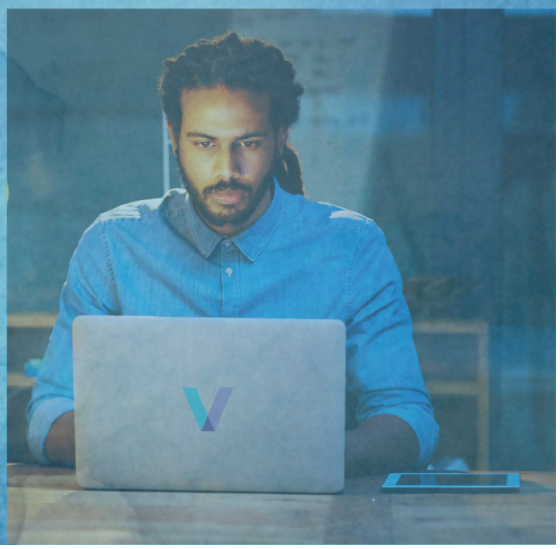
THE ADVOCATE'S GUIDE

to Secure and Efficient Case Management



The Advocate's Guide to Secure and Efficient Case Management

A trauma-informed, compassionate guide for advocacy organizations

Advocates and direct-care providers carry extraordinary responsibility. Every day, you navigate urgent safety needs, build trust with survivors, and balance the emotional weight of trauma with the practical demands of documentation and reporting. At Vela, we understand that this work is both courageous and complex, and the systems you rely on should support you, not slow you down.

This guide was created to honor that reality. Inside, you'll find workflow tips, trauma-informed documentation practices, and a grounded comparison between manual systems and secure digital tools. Our goal is simple: to help you protect survivor information, reduce administrative strain, and reclaim time for human connection.

1. Why Secure, Efficient Case Management Matters

Safety and Confidentiality

Survivors share some of the most sensitive details of their lives. Protecting that information is an act of care and an extension of your advocacy. Limiting access, collecting only what's essential, and maintaining secure practices strengthen the trust that survivors place in you.

Staff Capacity and Well-Being

When workflows are clear and efficient, advocates gain back minutes (and sometimes hours) that can be redirected toward supporting survivors, collaborating with teammates, or simply breathing between crisis moments. Staff deserve systems that lighten their load.

Reporting Readiness

Accurate, timely reporting isn't just a funder requirement. It's how programs tell the story of their impact. Building thoughtful workflows now prevents stress later and ensures that the work you do every day is reflected in the data that sustains your organization.

2. The Confidentiality and Compliance Landscape

Advocacy work exists at the intersection of safety, privacy, and compliance. Even when programs aren't HIPAA-covered entities, the principles of strong security still apply.

VAWA & FVPSA Confidentiality

Survivor information must be treated with the highest level of confidentiality. Sharing personally identifying information (PII) should only occur with informed, time-limited, written consent—and only when absolutely necessary.

Grant Reporting Requirements (VOCA, OVW, STOP)

Capturing the right information at the moment services are delivered reduces rework and protects accuracy. Aligning forms and service definitions with your funders' language ensures clean, consistent reports.

HIPAA Considerations (If Applicable)

When programs fall under HIPAA, secure logins, encryption, and audit trails become essential. Even outside HIPAA, these practices help safeguard survivor information and reduce organizational risk.

3. Trauma-Informed Documentation: Less is Best

Documentation should elevate safety and support, not retraumatize or overwhelm.

Do:

- Record only what is necessary for services, referrals, and required reporting.
- Use neutral, compassionate, non-blaming language.
- Store highly sensitive details in fields with appropriate visibility restrictions.
- Use templates that guide consistency and reduce guesswork.
- Keep notes brief and do not include anything that may be harmful to a survivor if subpoenaed.

Avoid:

- Long narratives or unnecessary details.
- Conjecture, speculation, judgment.
- Copy/paste habits that can spread sensitive information.
- Storing files or screenshots on personal devices.
- Sending personally identifiable information in Email, Slack, Basecamp. They are not protected methods for sending client data.

A Simple, Trauma-Informed Note Pattern

- **Purpose:** What the survivor asked for or needed.
- **Action:** What you provided or facilitated.
- **Next Step:** Follow-ups, referrals, or safety planning.

This structure supports clear, helpful documentation while honoring survivor autonomy and privacy.

4. Practical Workflow Tips for Frontline Teams

Intake & Triage

- Use flexible, conditional forms to avoid overwhelming survivors.
- Capture demographics and required funder data once.
- Always offer survivor-preferred names and communication methods.

Service Delivery

- Customize your referral list to streamline warm hand-offs.
- Store high-risk details in appropriate note categories, password-protected forms, to ensure the data is protected. restricted fields.

Follow-Up & Outcomes

- Use gentle customizable notifications for time-bound check-ins.
- Track outcomes using simple, consistent measures.
- Identify needs, gaps, and opportunities.

Reporting

- Map your services to funder categories early, not during reporting week.
- Run monthly pre-reports to catch missing data.
- Schedule grant reviews each quarter and when a new grant award starts to update your site with new grant conditions and reporting requirements.

5. Security Best Practices for Advocacy Work

Safety extends beyond physical environments.

Digital safety matters too.

- **Role-based access:** Keep information limited to those who truly need it.
- **Strong authentication:** Unique logins, MFA, and automatic timeouts protect against unauthorized access.
- **Encryption:** Data should be encrypted in transit and at rest.
- **Device hygiene:** Full-disk encryption, screen locks, and secure organizational accounts.
- **Audit logs:** Regularly review access for anomalies.
- **Data minimization:** If you don't need it, don't collect it. Permanently delete aggregate data when your data retention mandates have passed.
- **Vendor accountability:** Ask clear questions about hosting, data ownership, retention, and breach response.

These practices don't just reduce risk. They reinforce the trust survivors place in your organization.

6. Quick Checklists

Shift-Start Digital Safety

- Logged in with MFA
- Encrypted device in use
- Wifi is secure

Case Note Check

- Necessary and objective
- No unnecessary identifiers
- Stored appropriately

Monthly Reporting Hygiene

- Review pre-reports
- Merge duplicates
- Follow retention policies

7. Frequently Asked Questions

Do we need long narratives?

No. Clear, objective, short notes often serve survivors best.

Can I email a spreadsheet to finish at a later time?

Avoid exporting survivor data whenever possible. If you must, use secure methods and delete the file immediately after.

Who can see my notes?

Visibility should be based on role and necessity. If unsure, ask your administrator before adding sensitive details.

About Vela

Vela was built alongside advocates, directors, and coalitions who understand the realities of crisis

response and trauma-informed support. Our goal is to create technology that feels like a partner—not another task.

Programs share that Vela helps them reclaim time, strengthen data security, and present clearer stories of the life-changing work they do every day.

What they say:

"We are so grateful to have the opportunity to work with a company that understands what we do so that we can do what we love." *Amy McCarthy, Executive Director*

"Vela has revolutionized everything we do." *Dr. Stephanie Logan, Executive Director*

Want to see what a secure, advocacy-first workflow could look like for your team?

Request a brief, supportive demo with no pressure, just partnership.

This guide is informational and does not constitute legal advice. Always consult your funders' current reporting instructions and applicable laws/regulations in your jurisdiction.

Developed with input from advocates at every stage, Vela by Element 74 is a trauma-informed case management and reporting platform built specifically for domestic violence, sexual assault, and human trafficking organizations.

info@veladirect.com | (573) 332-7474

Manual Systems vs. Secure Case Management Software

A comparison rooted in real-world advocacy needs

Topic	Manual Systems	Secure Case Management Software
Confidentiality	Hard to control who sees paper files; risk of misplacement	Role-based permissions, restricted fields, audit trails
Safety	Sensitive details at risk in physical storage	Encryption, safe contact fields, configurable consents
Consistency	Varied styles and processes	Templates, controlled language, conditional logic
Time & Capacity	Double- entry, end-of-quarter corrections	Quick-click entries, automated summaries
Reporting	Manual tallying, high error potential	Auto-calculated VOCA/STOP metrics
Training	Learning ad-hoc processes verbally	In-app guidance, checklists, micro-lessons
Data Quality	Duplicates and inconsistencies	Required fields, validation, deduping
Continuity	Files scattered across locations	Centralized, backed-up, and searchable