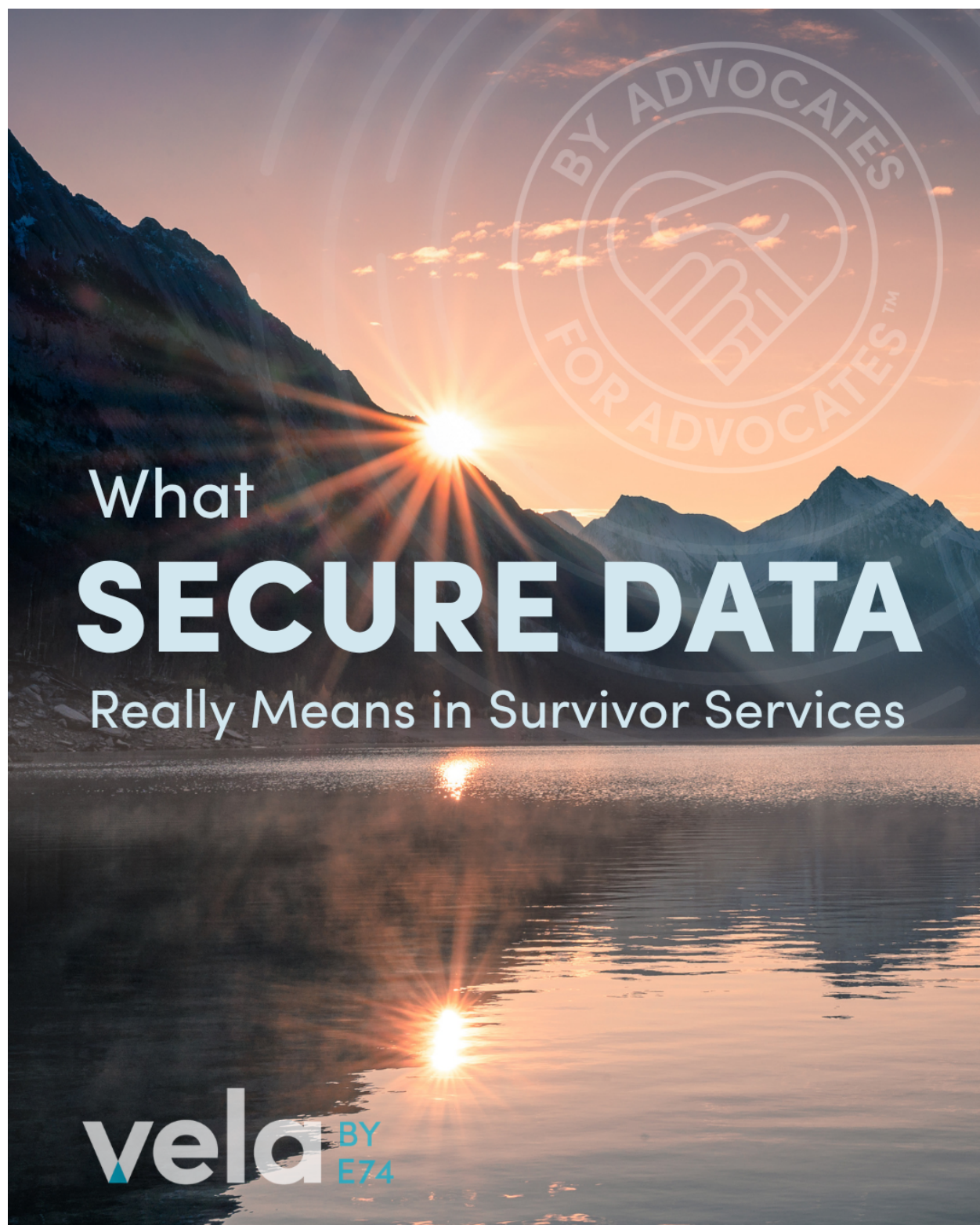




What **SECURE DATA** Really Means in Survivor Services

vela BY
E74

What Secure Data Really Means in Survivor Services

While *secure data* can sound like just a tech buzzword, in survivor services, it's a matter of trust, dignity, and safety. Trauma survivors hold some of the most sensitive information imaginable. Protecting their information isn't just about meeting compliance checkboxes; it's about ensuring every detail shared is handled with the utmost care.

Let's break down what secure data really means in this field.

1. Encryption: Locking the Doors (and the Windows)

Encryption is like putting your data in a locked safe. When information like service notes, contact details, or intake forms is stored or sent, encryption scrambles it into a code that only someone with the right digital key can unlock.

There are two main types:

- **Data “at rest”** encryption protects stored information (like files on a server or in a database).
- **Data “in transit”** encryption secures information as it moves from one place to another (like when a survivor fills out a secure form online).

Without encryption, data travels in plain text and becomes easy for hackers or bad actors to read. With encryption, even if someone intercepts the data, all they'd see is a jumble of meaningless characters.

2. Access Controls: Keeping the Right Eyes on the Right Data

Encryption locks the information, but access controls decide *who* gets the key. In survivor services, that often means:

- **User roles and permissions:** A therapist might have access to client notes, while a volunteer only sees basic contact information. Permissions can also determine whether a staff member can view all clients or only the clients they themselves added to the system. This also means that staff can only access data connected to programs they are authorized to see. For example, survivor advocates cannot see data entered into a BIP program or legal program.
- **Two-factor authentication (2FA):** With 2FA, logging in requires more than just something you *know* (like a username and password). It also necessitates something you *have* (like a phone or app code).

- **Audit logs:** Every access, edit, or view can be tracked, which creates accountability and transparency.

These controls help ensure that confidential survivor data isn't accidentally shared or accessed by someone without a legitimate reason. The goal is simple: *only the right people see the right information at the right time.*

3. Privacy Standards: Following Rules That Protect Real People

Privacy standards are the guardrails that organizations follow to keep survivor data safe and ethical. Some of the most relevant include:

- **HIPAA (Health Insurance Portability and Accountability Act):** HIPAA protects health-related information, including counseling notes or referrals.
- **VOCA and VAWA confidentiality requirements:** These limit how and when personally identifying information about survivors can be shared, even with partner agencies.
- **Data minimization:** The principle of data minimization holds that organizations should collect only what's necessary and nothing more. Vela encourages organizations to keep only the data absolutely necessary to provide the victim services and to take care ensuring survivors have

provided informed consent. For example, survivors *are not required* to have their immigration status logged in the database to receive victim services.

Meeting these standards isn't just about legal compliance; it's about building a culture of respect and trust. Survivors deserve to know that their information is not only protected but handled with empathy and utmost care.

4. Beyond the Technology: The Human Side of Security

Even the best encryption or privacy policy can't protect data if people aren't trained to handle it responsibly. True security includes:

- Regular staff training on recognizing phishing attempts and safe data practices.
- Clear policies for reporting and responding to breaches.
- A culture that reinforces confidentiality as a shared responsibility, not just an IT concern.

Secure Data = Safe Survivors

When survivor service organizations talk about "secure data," they're really talking about protecting lives and stories. Encryption keeps the information safe, access controls keep it in the right hands, and privacy standards ensure it's treated with care.

More than just a technical requirement, security is a commitment to the survivors who trust you to care well for their stories.

Innovation That Protects What Matters Most

At Vela, innovation is more than building better software.

It means continually asking how our technology can better protect survivor safety, strengthen confidentiality, and support the advocates doing this critical work. Our team is committed to evolving alongside the needs of survivor service programs, maintaining strong security practices while designing tools that are practical, thoughtful, and trauma-informed.

We believe that when technology is built with both innovation and care, it becomes more than a system for managing data. It becomes part of a safer, more trustworthy foundation for serving survivors.

Vela is driven by our core values to support survivor-serving organizations with compassion, integrity, innovation, collaboration, and gratitude.

Want to learn new ways to simplify your work or explore features you may not be using yet? Visit veladirect.com or reach out to our team. We're always here to help.



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