BINDER ESSENTIALS

Privacy Policy

Document ID	PRV-01
Version	1.2
Last updated	11/06/2026
Provider	Stacked Innovations, LLC
Applies to	binderessentials.com, app.binderessentials.com and the demonstration environment

1. What This Policy Covers

This policy explains how Stacked Innovations, LLC ("we", "us") collects, uses, shares and protects personal information about the people who use Binder Essentials and visit our websites: customer users, people who sign up, prospective customers requesting or using the demonstration, and website visitors.

It does not cover protected health information. Information about residents and patients that our customers store in Binder Essentials is handled under each customer's Business Associate Agreement with us, and under that customer's own privacy practices. We act on the customer's behalf for that information, and do not use or disclose it except as the Business Associate Agreement permits. Questions about it should go to the facility.

References in this policy to “records” or to activity in the Service mean the operational and security metadata we keep about user actions, not the content of resident or patient health information, which remains governed by the applicable Business Associate Agreement and the facility’s own privacy practices.

2. Information We Collect

Category	What, and from where
Account information	Name, email address, password (stored only as a one-way hash), role, and the facility you belong to -- from you at signup or registration, or from the Facility Administrator who invites you. If you sign up, whether you chose to receive product news from us.
Customer and facility details	The legal entity name, facility name, facility address, time zone and, if provided, CMS Certification Number.
Acceptance records	The version of these documents and of our Terms of Service you accepted, when, and the network address you accepted from.
Security and activity records	Sign-in events (successful and failed), sign-outs, the network address and time of each, and a record of actions taken in the Service, such as creating, changing, uploading, viewing or downloading records.

Category	What, and from where
Billing information	Payment is handled by Stripe. We receive a customer reference, subscription status and billing period -- not full card numbers.
Communications	Emails and support requests you send us, and the transactional emails we send you.
Demonstration use	In the demonstration environment, a temporary account and the actions taken in it. Each demonstration copy, with its activity, is deleted automatically.
Demo and early-access requests	Name, email address, role, facility name, state, CMS Certification Number and your early-access preference, from the form on our website.
Website information	Information our websites collect automatically, such as browser type and pages visited, and any cookies or analytics used.

3. How We Use It

- To provide the Service: creating and managing accounts, applying each user's role, and delivering the features you use.
- To secure the Service: authenticating users, detecting and investigating misuse, and keeping security records.
- To bill for subscriptions and keep financial records.
- To send transactional email: verification, invitations, security notices, and account and billing notices. **Our emails contain links, never document content or resident information.** We do not send marketing email to customer users without their consent.
- To keep records of acceptance of our terms and of executed Business Associate Agreements.
- To respond to demo requests and, if you ask, to consider you for early access.
- To send occasional product news to people who have opted in to receive it. Every such email includes a way to unsubscribe.
- To support you when you ask, and to meet our legal obligations.
- To improve the Service, using information that does not identify you where we can.

We do not sell personal information, and we do not use it for advertising.

4. How We Share It

We share personal information only with:

- **Your facility.** Your Facility Administrator can see your account, role and activity within the facility.
- **Service providers** that operate parts of the Service for us, under contracts that limit their use of it to providing those services, and under business associate terms where they may handle protected health information:

Service	Provider
Application hosting and databases	Render
Document storage	Amazon Web Services
Website and application front end	Vercel
Domain and network services	Cloudflare
Payments	Stripe
Email	Google Workspace; Postmark
Artificial intelligence features	Anthropic

- **Email-marketing providers,** for people who have opted in to product news: Constant Contact, which receives the name, email address, organization, and facility name and address of each person who opted in, and which we use only to send those emails.
- **A buyer of a facility,** when a customer sells a facility and instructs us in writing to transfer its records, after the buyer has entered into a Business Associate Agreement with us.
- **A successor** to our business in a merger, acquisition or sale of assets, subject to this policy.
- **Authorities,** when the law requires it, or when necessary to protect the rights, property or safety of our customers, their residents, users or others.

5. How Long We Keep It

Information	Kept for
Account information	While the account exists, and then as the customer's offboarding provides
Security and activity records	30 days
Acceptance records and Business Associate Agreement records	Six years after the relevant agreement ends
Billing records	As tax and accounting law requires
Demonstration copies and their activity	Deleted automatically, within hours
Demo requests	12 months after our last contact with you
Product news subscriptions	Until you unsubscribe
Communications	As needed to support you, and no longer than 30 days

6. How We Protect It

We use administrative, physical and technical safeguards, including encryption in transit, passwords stored only as one-way hashes, role-based access limited to each facility, automatic sign-out after inactivity, separate environments with separate credentials, multifactor authentication on our internal consoles, and activity logging. No system is perfectly secure; we will notify affected customers of a breach as the law and our agreements require.

7. Your Choices and Rights

- **Access and correction.** You can view and update your account details in the Service, or ask your Facility Administrator or us.
- **Deletion.** Your account is removed when your Facility Administrator removes you, or when your facility's subscription ends. Some records are kept as Section 5 describes.
- **State privacy rights.** Depending on where you live, you may have additional rights, such as to know, delete or correct personal information. To exercise them, contact us at the address below.
- **Residents and patients** should contact their facility about their health information.

8. Children

The Service is for professional use and is not directed to anyone under 18. We do not knowingly collect personal information from children.

9. Changes to This Policy

Each version of this policy carries a version number and date. **When a change is material, users must accept the new version at their next sign-in**, and we record that acceptance**. A user who does not accept cannot continue to use the Service**. Other changes take effect on publication.

10. Contact

Stacked Innovations, LLC, 424 Barons CT, Venetia PA 15367. Privacy questions: privacy@binderessentials.com. Our HIPAA Security Officer can be reached at the same address.