TestLedger™

DOCUMENTATION PLATFORM

Basic User Manual

Operating guidance for the Basic plan

Version 4.2 | April 19, 2026

TestLedger LLC
testledger.io

About This Manual

This manual explains how to use TestLedger Basic to document routine employer workplace drug testing. It covers the record-entry workflow, the cryptographic sealing step, and the public Verify Portal.

Use of TestLedger is governed by the Terms of Service and Privacy Policy. Those documents contain the complete agreement between your organization and TestLedger LLC. Please review them before using the platform.

TestLedger provides documentation workflow, record custody, and sealing tools for customer-submitted records in non-DOT workforce drug testing programs. TestLedger does not create record details, perform testing, provide MRO services, provide legal or regulatory advice, determine whether submitted content is PHI or ePHI, or make compliance, admissibility, or employment determinations. Your organization remains solely responsible for record content, lawful disclosures, regulatory compliance, and employment actions.

TestLedger is a documentation and cryptographic sealing platform. It is not a laboratory, a Medical Review Officer (MRO) service, or a source of legal, medical, or compliance advice. Decisions about testing programs and employment actions are made by your organization and its qualified advisors.

1. Getting Started

TestLedger Basic is designed for organizations that document non-DOT workplace drug testing without placing donor identity fields or evidence file attachments into the sealed record. Each record is protected by a SHA-256 cryptographic seal.

Basic plan includes

- Up to 500 records per billing cycle and up to three team members.
- Seven-tab record entry workflow: Authorization, Donor, Consent, Collection, Result, Evidence, CryptoSeal.
- SHA-256 cryptographic sealing and tamper-evident reference state.
- Public Verify Portal for consistency review of exported records.

If your workflow requires identity-linked records, evidence attachments, or chain-of-custody tracking with supporting documents, use the Professional plan.

Before your first record

On your first sign-in, acknowledge the Before You Begin screen and confirm you have reviewed the Terms of Service and Privacy Policy. Both checkboxes must be confirmed before the workspace becomes available.

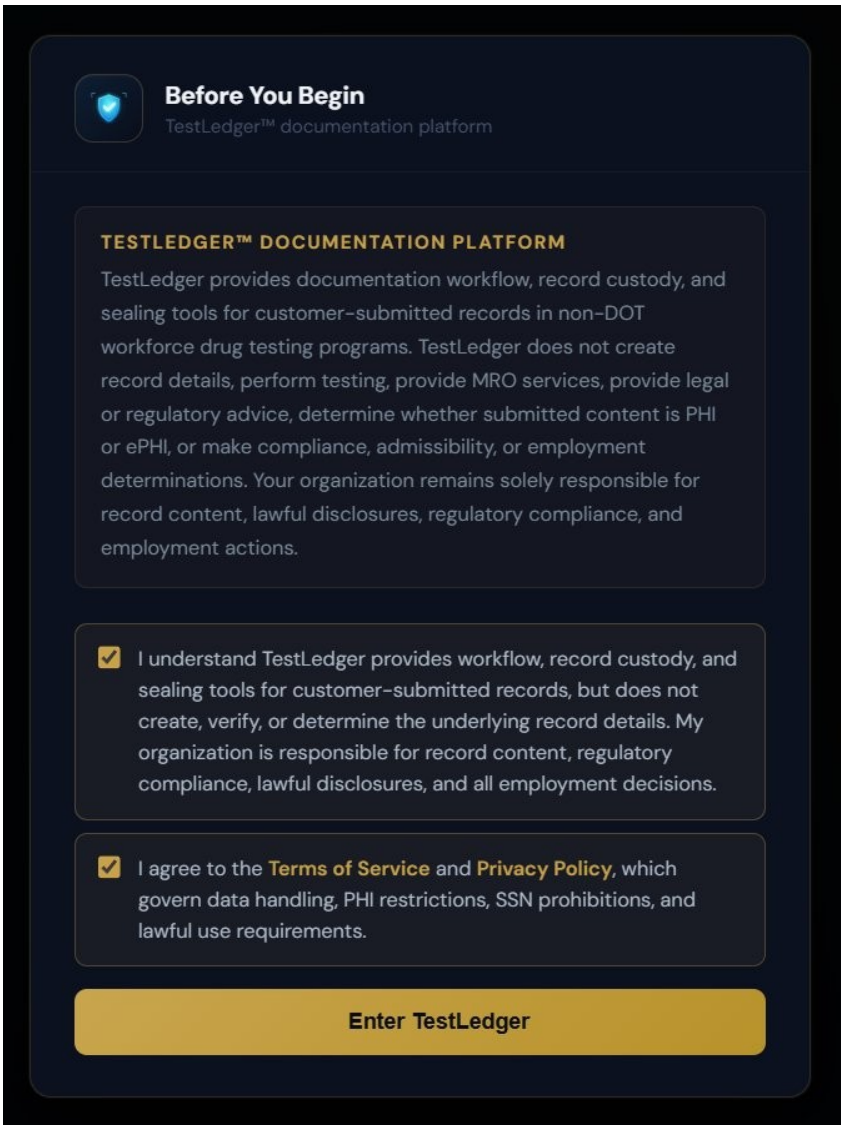

Figure 1. Before You Begin screen.

2. Workspace Dashboard

The workspace dashboard is your main operational surface. It shows monthly record usage, team seats, the next billing date, and the sealed-record list.

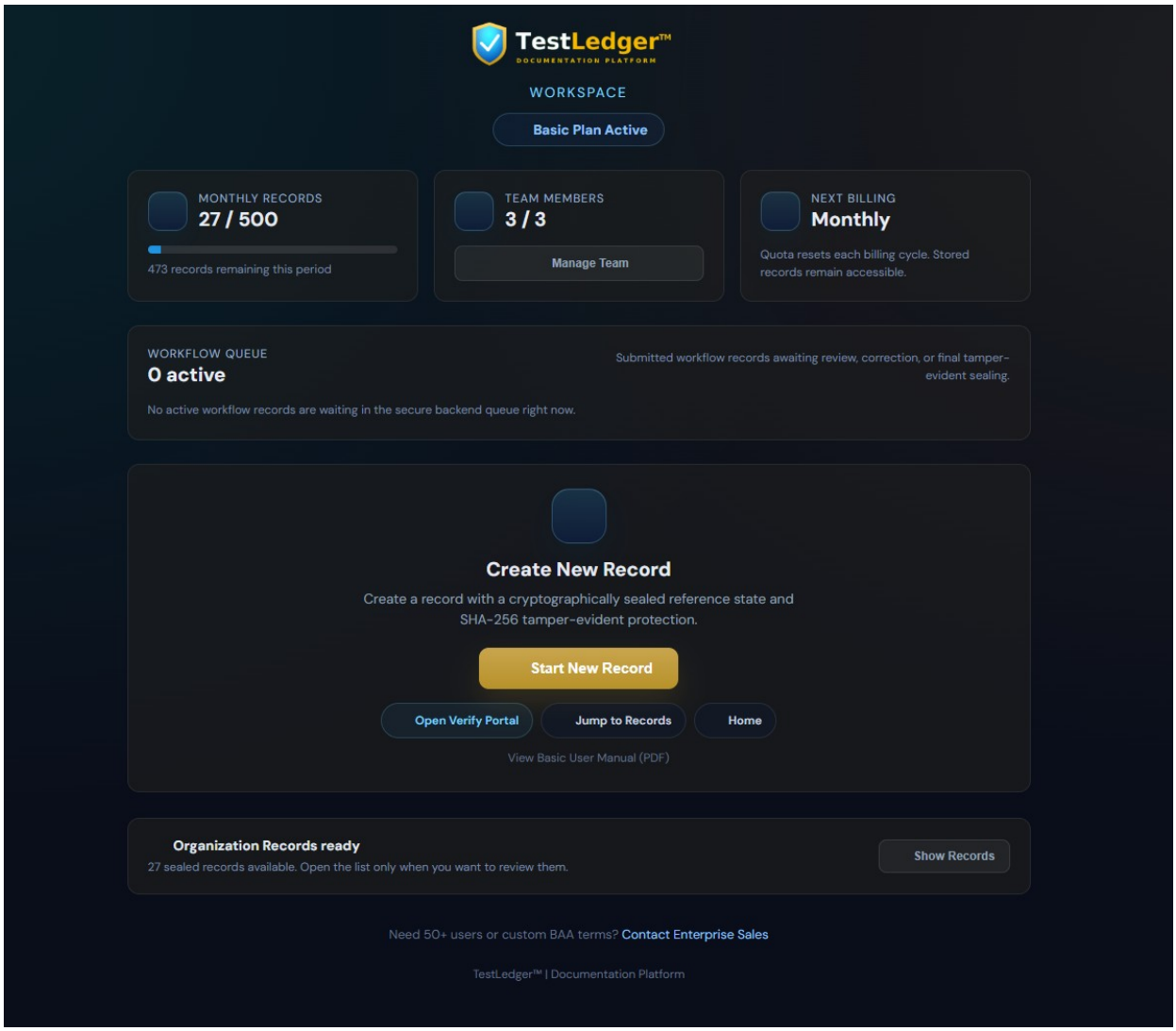

Figure 2. Basic Plan workspace.

What you can do from the dashboard

- Start a new record using the guided seven-tab workflow.
- Open the Verify Portal.
- View the sealed records list.
- View this manual.

Good practice

- Treat the dashboard as a restricted operational surface. Do not screen-share casually.
- Do not place sensitive content in filenames, free-text notes, or screenshots.
- Review access monthly and after any staffing change.

3. Creating a Record

From the workspace, click Start New Record. Complete each tab in order: Authorization, Donor, Consent, Collection, Result, Evidence, and CryptoSeal.

3.1 Authorization

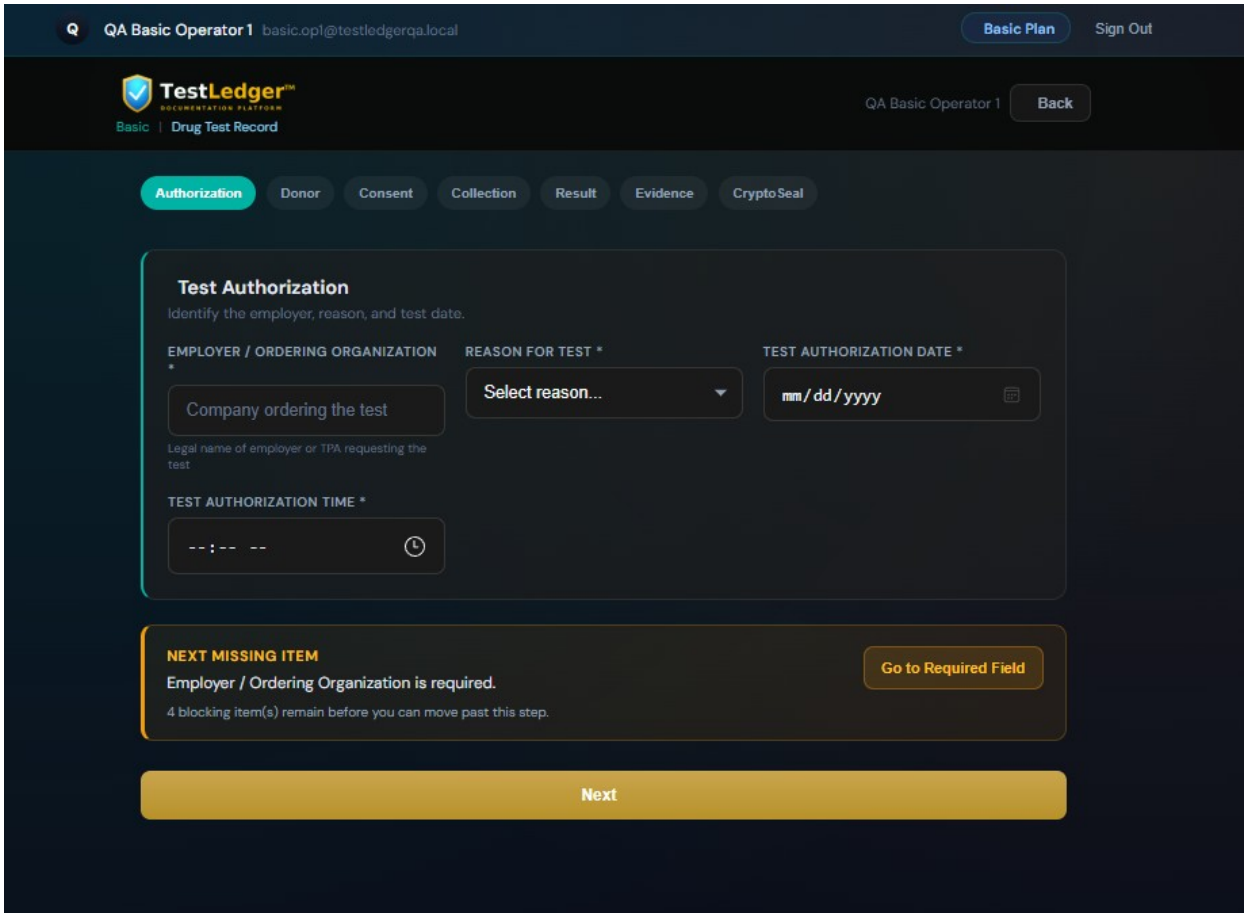

Figure 3. Authorization tab.

Fields

- **Employer / Ordering Organization:** Legal name of the employer or TPA requesting the test.
- **Reason for Test:** Pre-employment, random, post-accident, or other recorded business reason.
- **Test Authorization Date:** Date the test was authorized.
- **Test Authorization Time:** Corresponding time.
- **Additional Details (optional):** Expand when more structured detail is required by your policy.

The Next Missing Item banner identifies the next required field. Use Go to Required Field to jump directly to it.

3.2 Donor

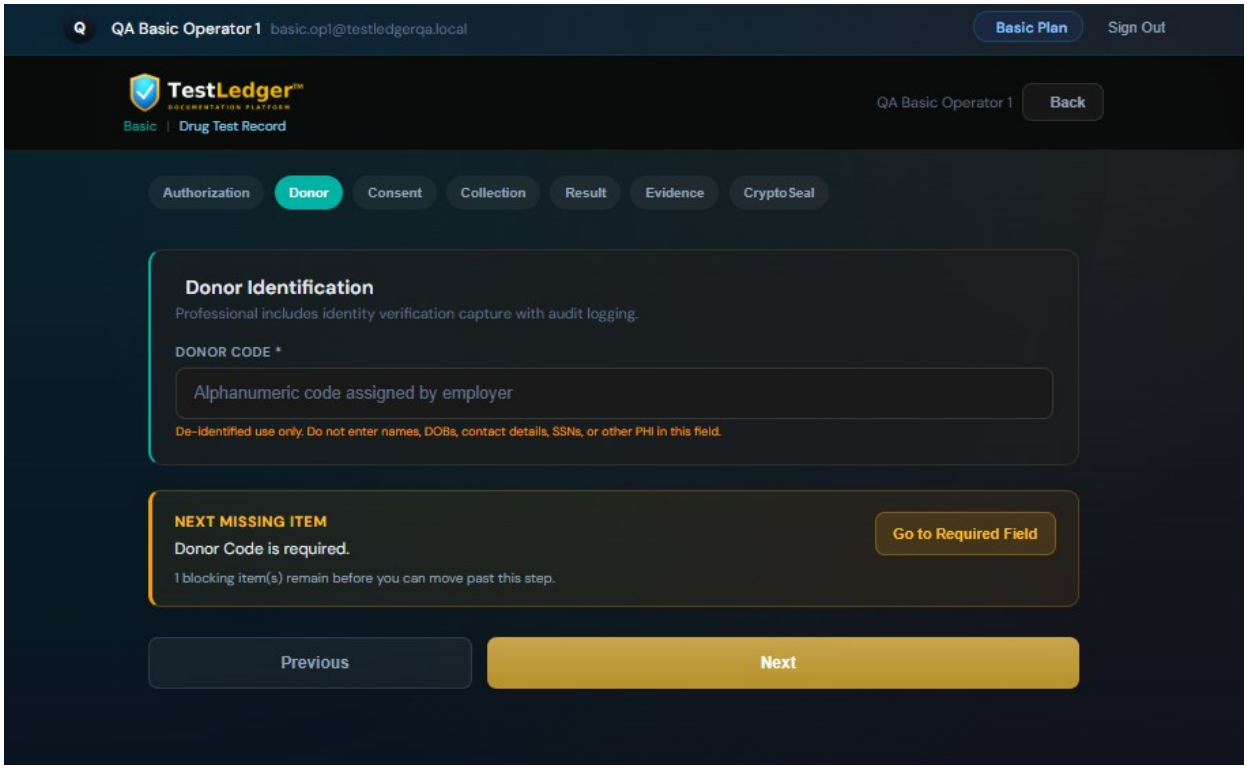

Figure 4. Donor Identification tab.

Fields

- **Donor Code:** Alphanumeric code assigned by the employer.

> **Do not enter in Basic**
>
> - Donor names or dates of birth.
> - Social Security numbers.
> - Contact details or other personally identifiable information.
>
> Use Professional with an active BAA for identity-linked workflows.

3.3 Consent

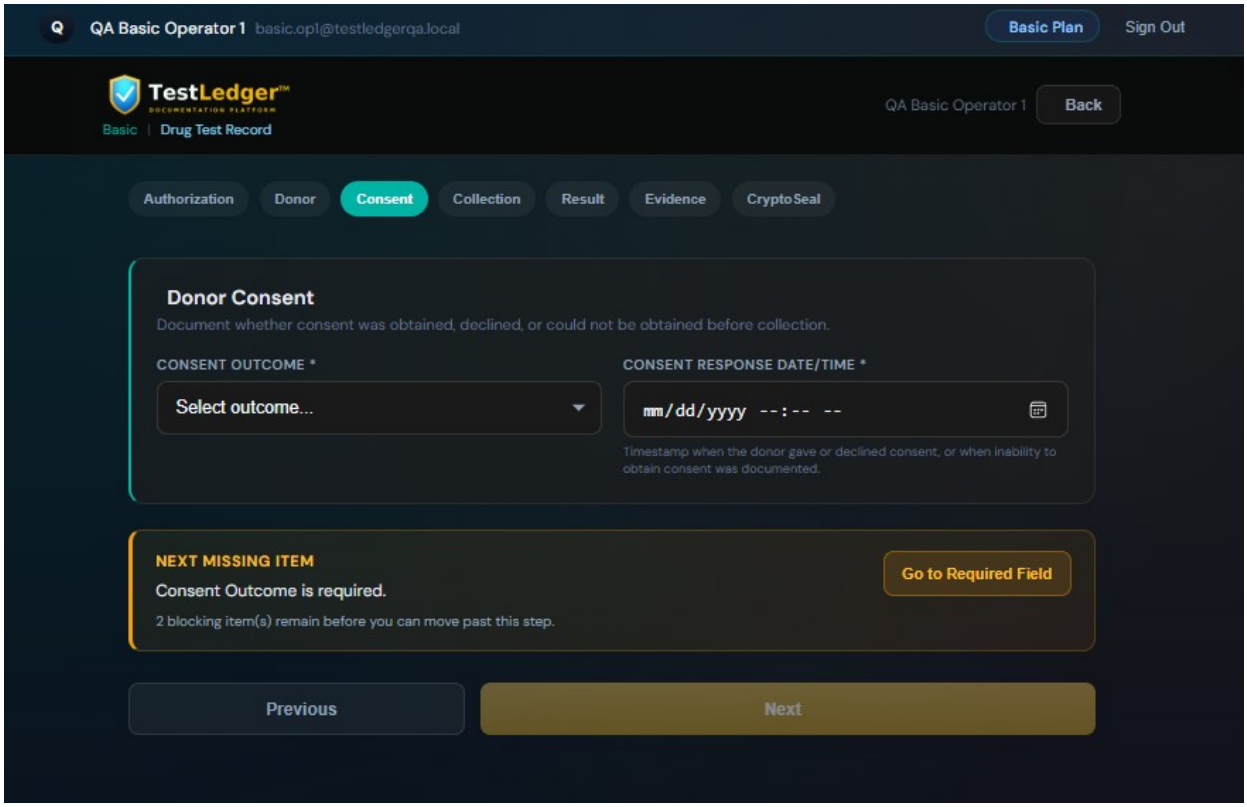

Figure 5. Donor Consent tab.

Fields

- **Consent Outcome:** Obtained, declined, or could not be obtained.
- **Consent Response Date/Time:** Timestamp when consent was given or declined.

3.4 Specimen Collection

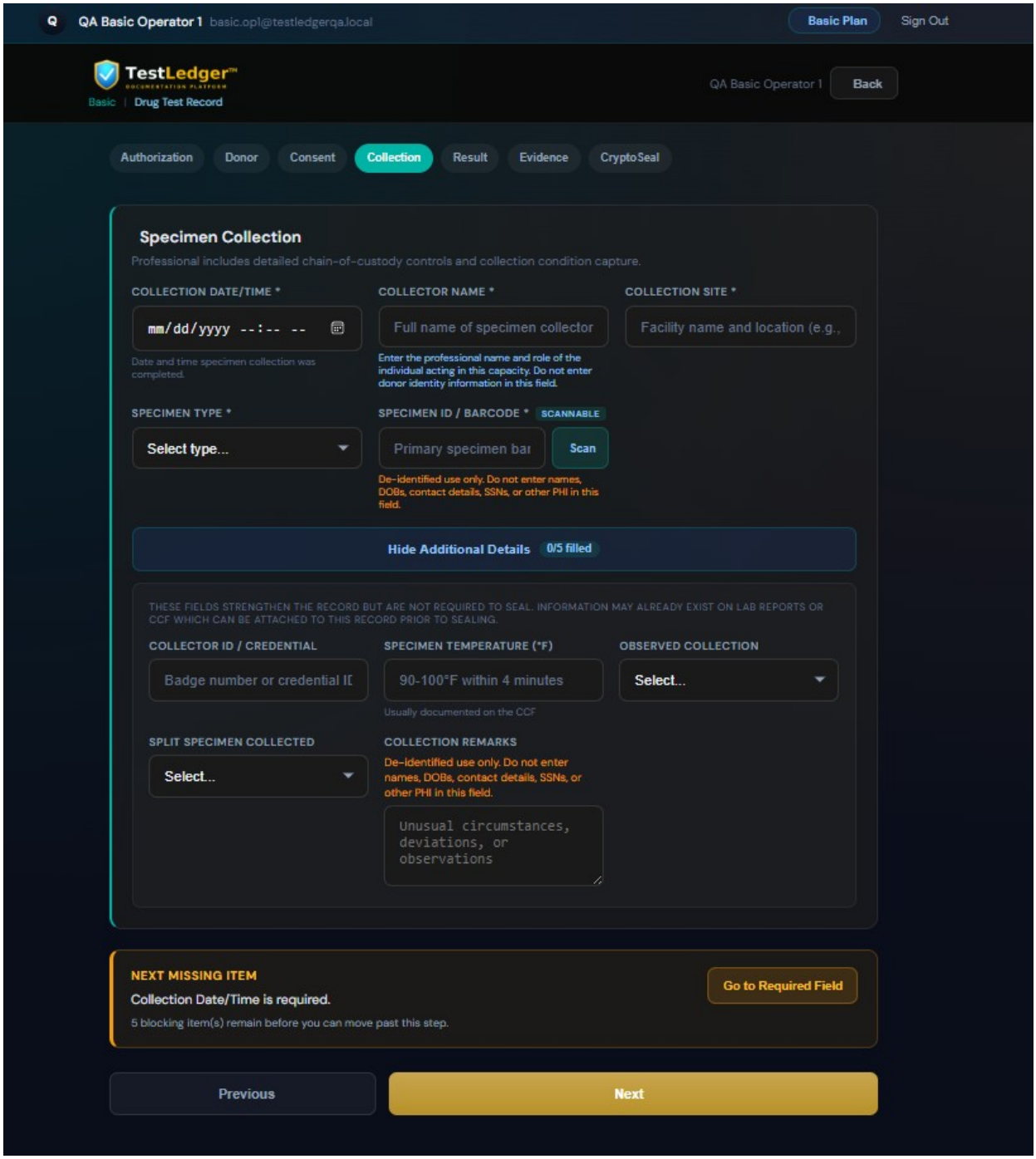

Figure 6. Specimen Collection tab.

Fields

- **Collection Date/Time:** Date and time the specimen was collected.
- **Collector Name:** Full name of the individual who collected the specimen.
- **Collection Site:** Facility name and location.
- **Specimen Type:** Select from available specimen types.
- **Specimen ID / Barcode:** Scannable identifier.
- **Additional Details (optional):** Collector ID, specimen temperature, observed collection, split specimen, collection remarks.

3.5 Test Result

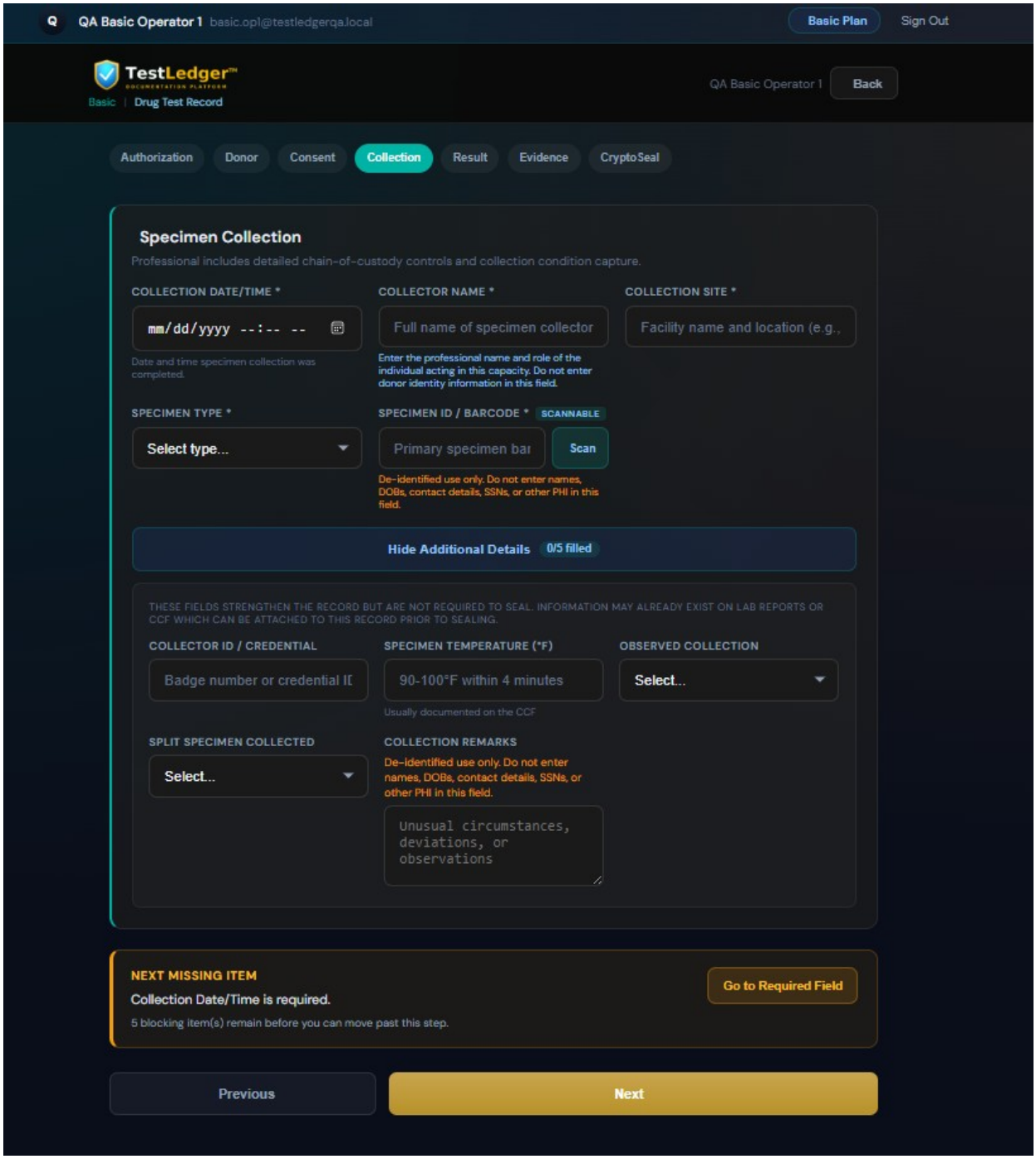

Figure 7. Test Result tab.

Fields

- **Screening Result:** Laboratory-reported screening outcome.

Non-negative results expand additional fields for confirmatory details and laboratory information.

3.6 Evidence

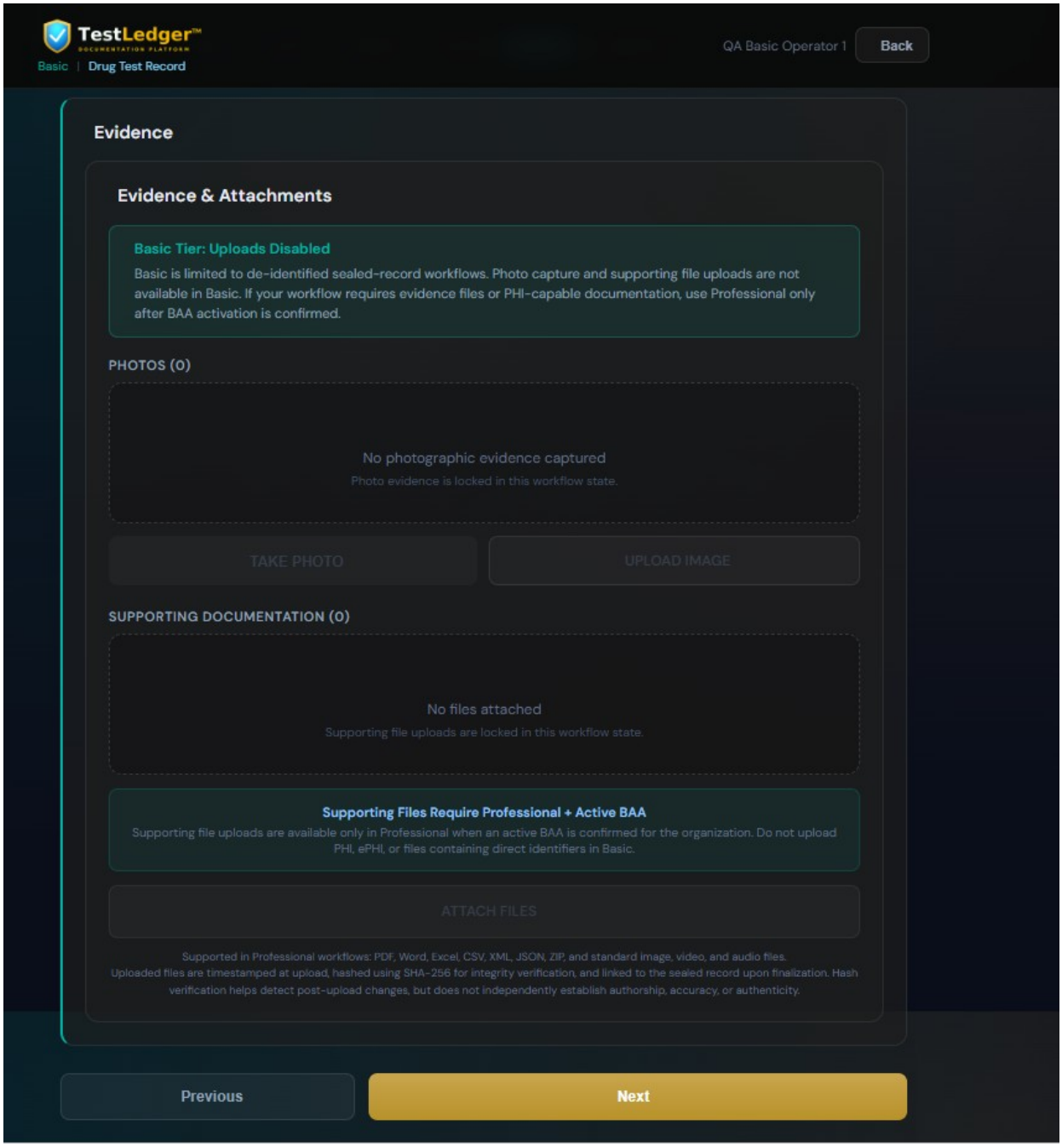

Figure 8. Evidence tab is disabled on the Basic plan.

> **Basic plan note**
>
> Photo capture and supporting file uploads are not available on Basic. If your workflow requires evidence files or laboratory report attachments, upgrade to Professional with an active BAA.

3.7 CryptoSeal

The CryptoSeal tab is the final step in the record-entry workflow. It presents a Chronology Review, a completion map, a pre-seal confirmation, and the seal control.

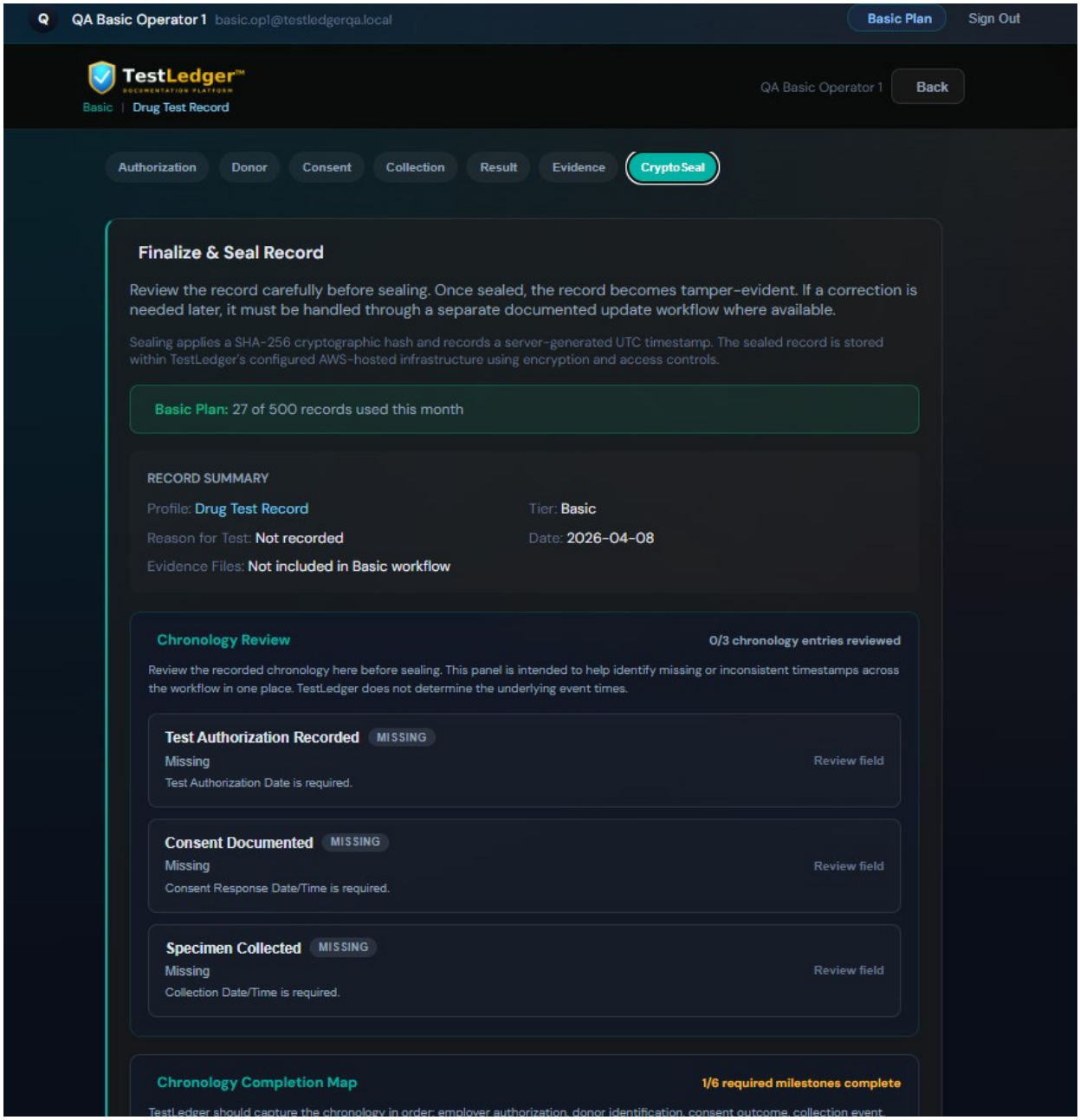

Figure 9. CryptoSeal tab.

Before you seal

- Six milestones must show Complete before the seal control activates.
- Review the Chronology panel. It flags missing or inconsistent timestamps.
- Read and confirm the pre-seal statement acknowledging data entry is complete.
- Once sealed, the record is saved as a reference state for later comparison. Corrections require a new record.

If a correction is needed later

Do not alter a sealed record informally. Create a new record under your organization's corrective-record procedure. The original sealed record remains intact as a reference state.

4. Sealed Records List

After sealing, the record appears in the Organization Records list. Records are synced to TestLedger cloud storage and accessible to authorized team members.

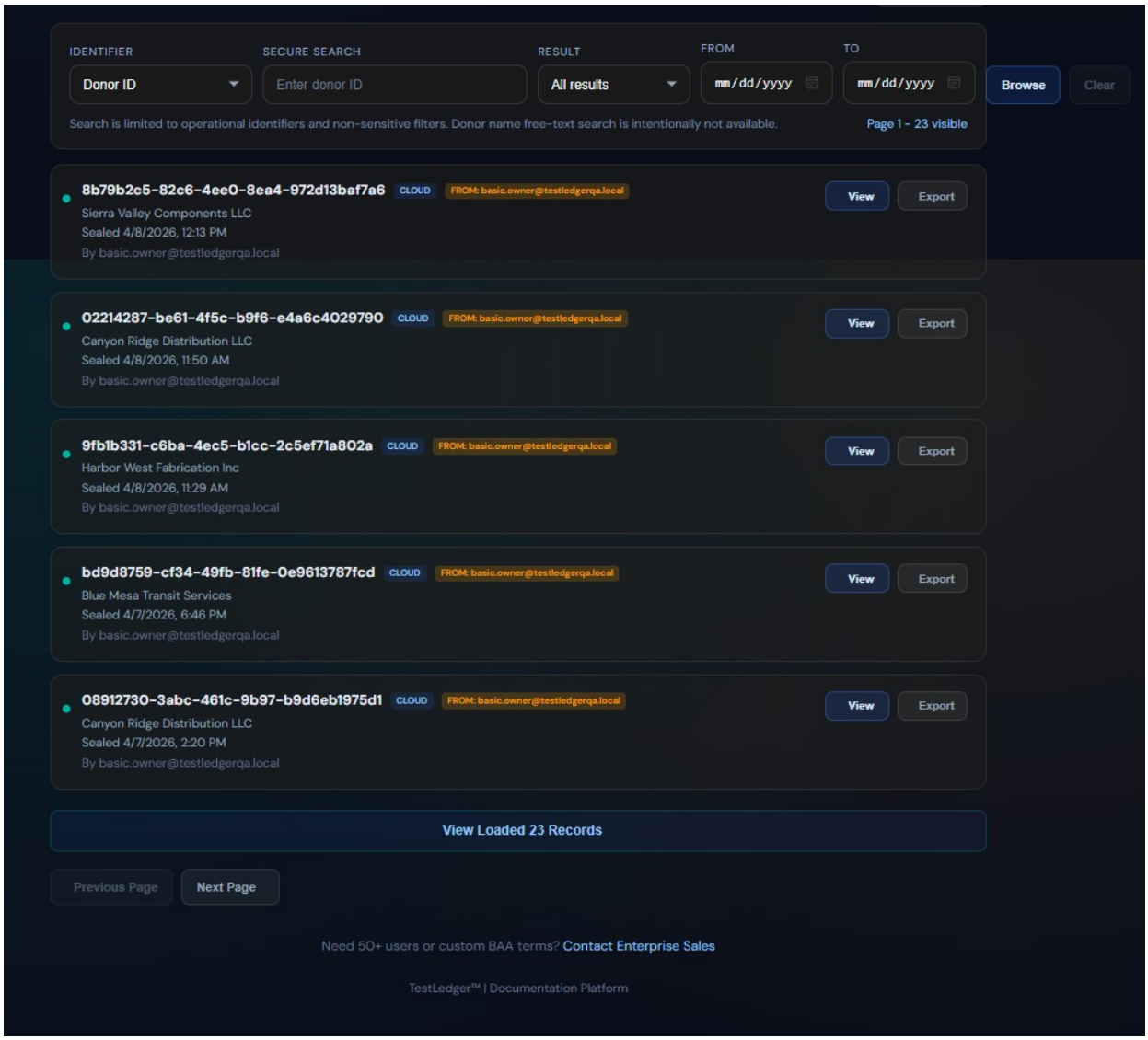

Figure 10. Organization Records list.

Each record row shows

- Record ID, employer name, seal date and time, and the operator who created the record.
- A View action that opens the Secure Record Detail drawer.
- An Export action that downloads the sealed JSON export file.

Search

- Search is limited to operational identifiers.

- Donor name free-text search is intentionally unavailable.

5. Verify Portal

The public Verify Portal checks whether a sealed export is cryptographically consistent with its sealed state. It is available without login at https://testledger.pages.dev/verify.

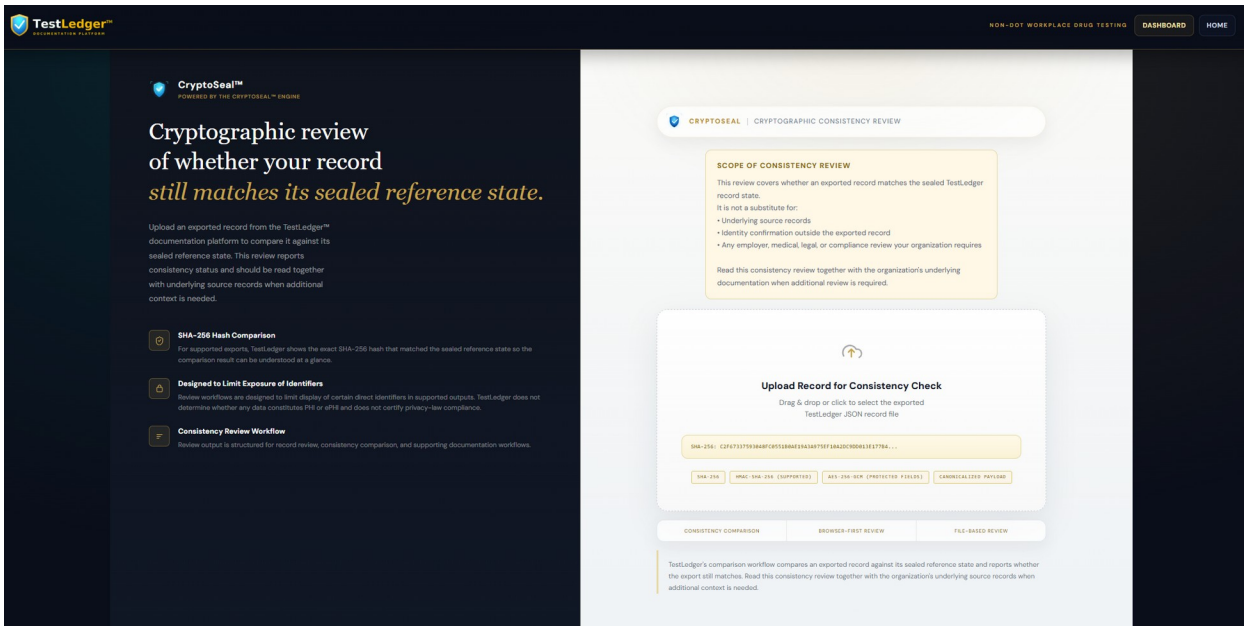

Figure 11. Verify Portal upload screen.

Using the portal

- Upload the exported record.json file. Drag and drop, or click to select.
- Use record.json, not package-manifest.json.
- The portal does not render any personally identifiable information.

5.1 Consistent With Sealed State

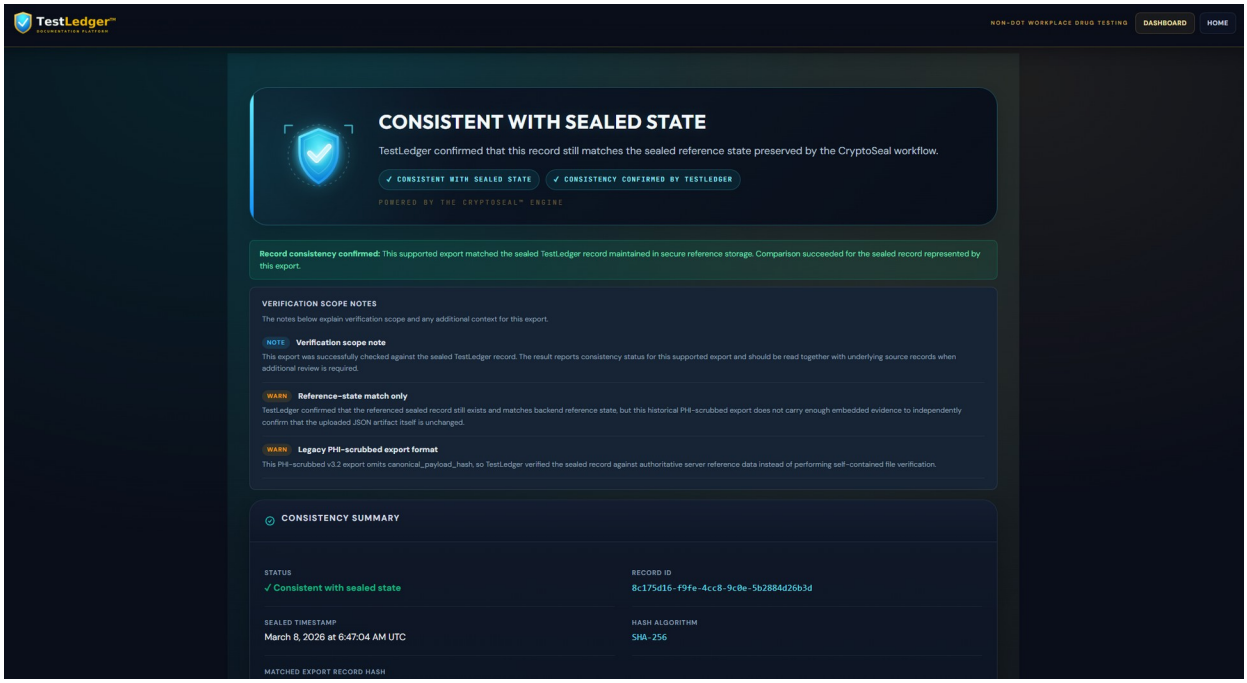

Figure 12. Consistent With Sealed State result.

What the indicators mean

- **Consistent With Sealed State:** The export's canonical hash matches the sealed hash.
- **Hash Match:** The SHA-256 hash of the file content matches the embedded sealed hash.
- **KMS Signed:** The record carries a valid AWS KMS ECDSA signature.
- **TSA Timestamped:** The record carries a valid RFC 3161 trusted timestamp (DigiCert).

5.2 Consistency Check Failed

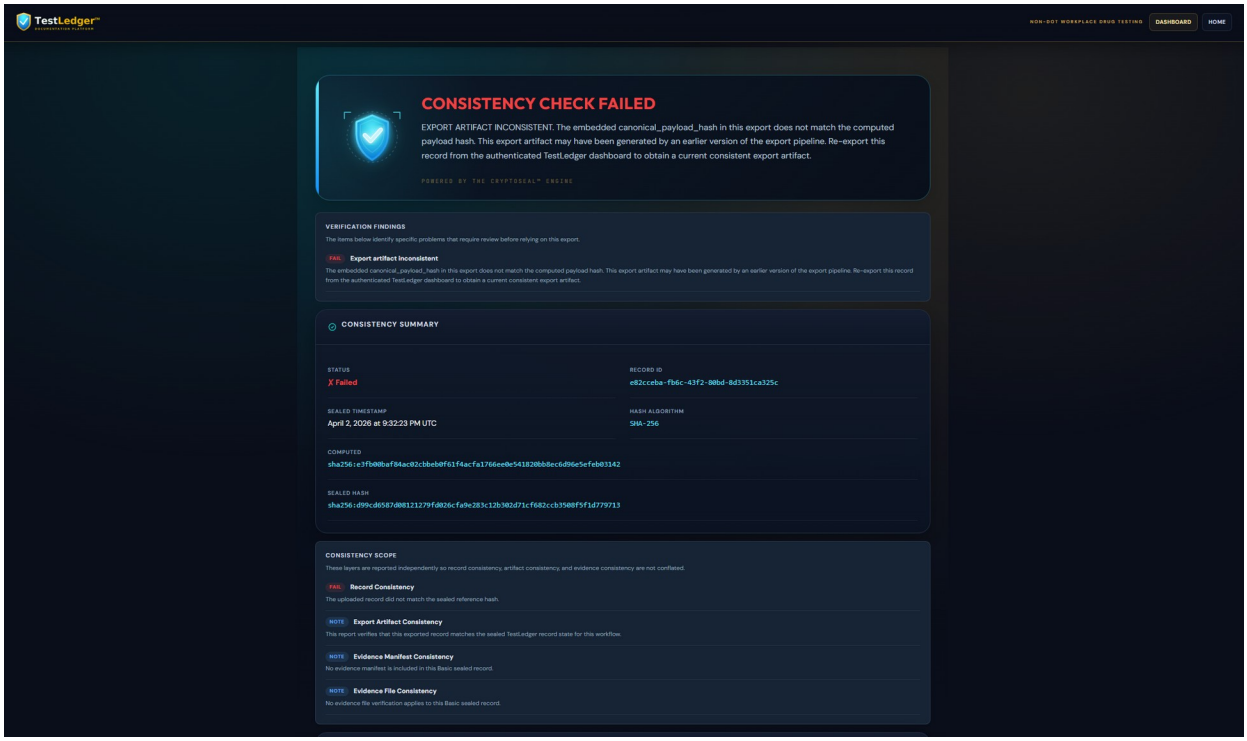

Figure 13. Consistency Check Failed result.

A Consistency Check Failed result means the uploaded file does not match the sealed record reference. The most common causes are a modified export or an export created using an older version of the export pipeline.

> **If a file fails the consistency check**
>
> - Do not rely on a failed export for review purposes.
> - Contact your administrator and review the export source.
> - A tampered or corrupted file will consistently fail the check.

6. Troubleshooting

- **Verification Incomplete:** Confirm you are using https://testledger.pages.dev/verify and not a deployment-specific preview URL.
- **Consistency check fails on package-manifest.json:** Upload record.json instead.
- **File has a Windows duplicate suffix such as (1):** The verifier may still accept it if the SHA-256 hash matches the sealed original.
- **Unsure whether a detail belongs in Basic:** Leave it out and consult your administrator.

- **Sealed record needs correction:** Do not attempt informal alteration. Create a new record under your organization's corrective procedure.

7. Support

For technical support, billing questions, or enterprise sales:

TestLedger LLC

Website: testledger.io

Support: support@testledger.io

Enterprise and BAA: enterprise@testledger.io

For legal terms governing use of the platform, see the Terms of Service and Privacy Policy.

