

TestLedger™
DOCUMENTATION PLATFORM

Professional User Manual

Version 1.4.3 | April 19, 2026

TestLedger LLC
testledger.io

About This Manual

This manual explains how to use TestLedger Professional to document non-DOT workplace drug testing. It walks through each tab of the record-entry workflow, the sealing and verification process, and the administrative tools available to organization administrators.

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, including data handling terms, service limitations, and obligations relating to protected information. 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, employment actions, and regulatory compliance are made by your organization and its qualified advisors.

Contents

1. Getting Started
2. Roles and Permissions
3. Business Associate Agreement (BAA)
4. Identity Protection Key
5. Workspace Dashboard
6. Creating a Record
 - 6.1 Authorization
 - 6.2 Donor Identification
 - 6.3 Donor Consent
 - 6.4 Specimen Collection
 - 6.5 Test Result
 - 6.6 THC Context (when applicable)
 - 6.7 Employment Action
 - 6.8 Evidence Vault
 - 6.9 Seal and Workflow Queue
7. Working With Sealed Records
8. Exporting and Sharing Records
9. Verify Portal
10. Identity Verification Tool
11. Support

1. Getting Started

TestLedger Professional provides a structured workflow for creating, sealing, and verifying non-DOT workplace drug testing records. Each record is protected by a SHA-256 cryptographic seal, giving your organization a tamper-evident reference state that can be independently checked for cryptographic consistency.

Professional plan includes

- Up to 10 team members and 2,000 records per billing cycle.
- Donor identity protection using HMAC-SHA-256 hashing and AES-256-GCM narrative encryption, with keys held exclusively by your organization.
- Evidence vault with per-file SHA-256 hashing and S3 Object Lock storage.
- Business Associate Agreement (BAA) execution workflow.
- Workflow Queue with separation of duties between Record Creator and Administrator roles.
- Chronology engine that checks timestamp sequencing before a record can be sealed.
- Employment action documentation tab and conditional THC Context tab.

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.

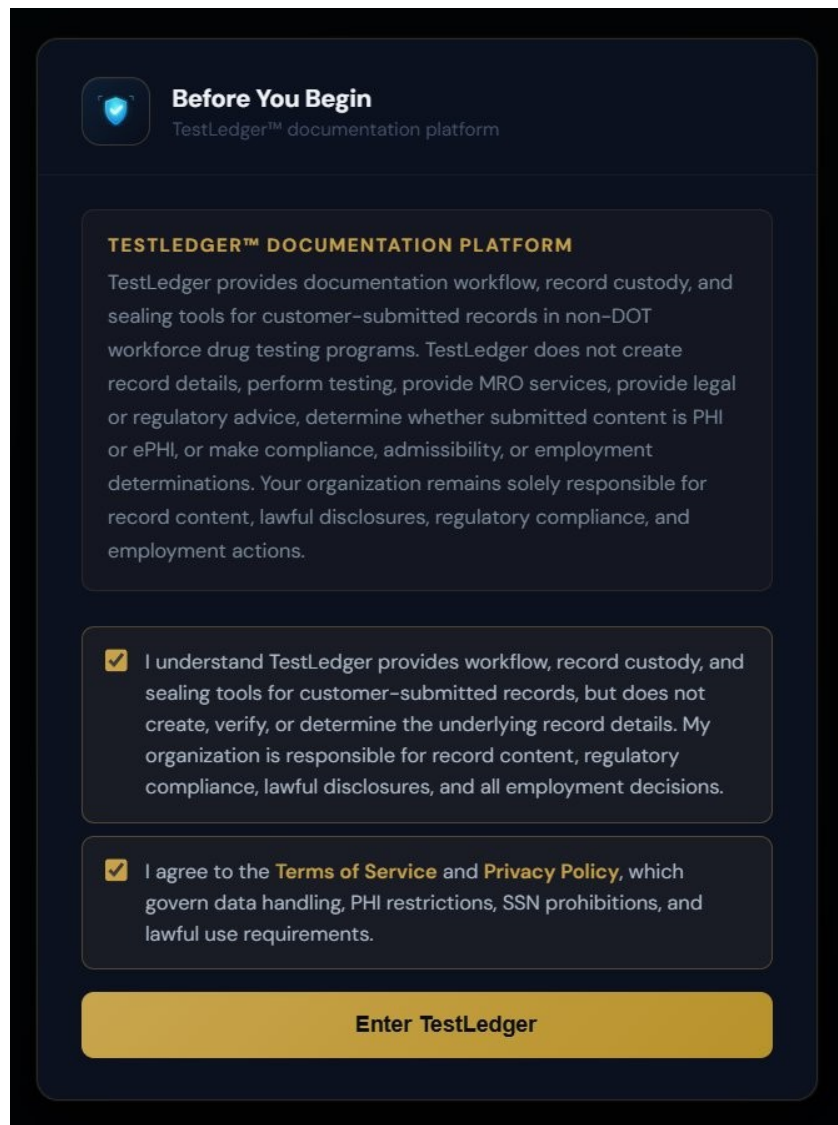


Figure 1. The Before You Begin screen is shown on first sign-in.

2. Roles and Permissions

Professional supports two organizational roles. Role assignment and record access scope are configured from the Team Management screen.

Capability	Administrator	Record Creator
Create records	Yes	Yes
Fill all record tabs	Yes	Yes
Submit for Sealing	Yes	Yes
Review Workflow Queue	Yes	No
CryptoSeal records	Yes	Submit only
Manage team members	Yes	No
Assign record access scope	Yes	No

Capability	Administrator	Record Creator
View org-wide records	Yes	Per admin assignment

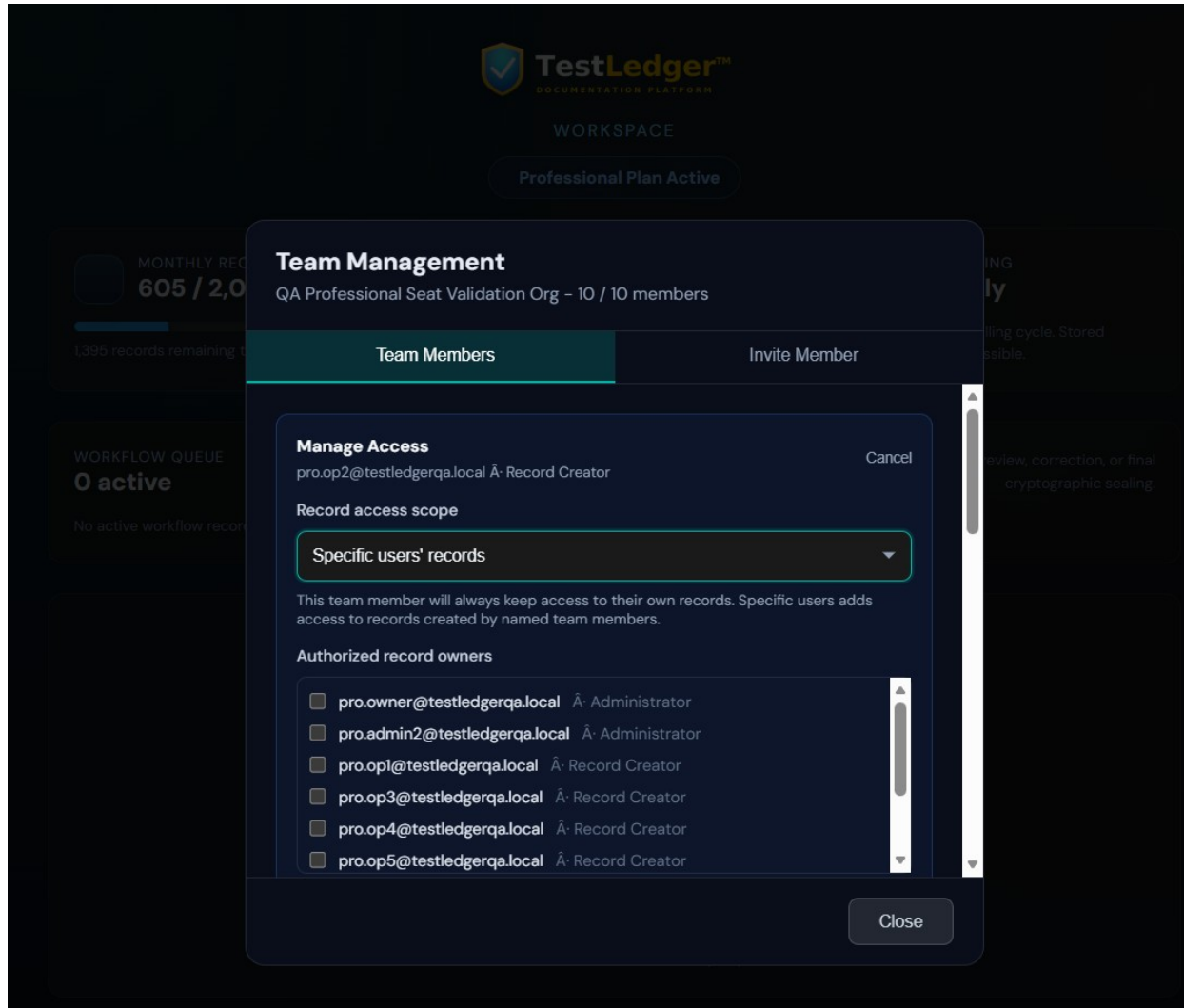


Figure 2. Team Management with role assignment and record access scope.

Record access scopes

- **Organization-wide records:** The user can view all records in the organization.
- **Specific users' records:** The user can view records owned by selected team members.
- **Own records only:** The user can view only the records they created.

Good practice

- Do not use shared accounts.
- Review access after any staffing change and remove access promptly when roles change.
- Restrict evidence review, export, and protected-field reveal to the smallest set of users that need them.

3. Business Associate Agreement (BAA)

If your organization’s workflow involves protected health information (PHI), you can execute a Business Associate Agreement with TestLedger LLC directly from the dashboard. BAA status is scoped at the organization level and applies to all team members.

Features unlocked when BAA status is Active

- Donor Full Name and Date of Birth fields on the Donor tab.
- Evidence Vault uploads, including photo capture and supporting documents.
- Identity protection key entry at seal time for HMAC-SHA-256 donor identity hashing.

Execute Business Associate Agreement

Required to access PHI fields. HIPAA 45 CFR 164.502(e)

✓ Execution of a BAA is required only if you intend to enter or process PHI. Records may be created, saved, and sealed without PHI.

1 Covered Entity Information

ORGANIZATION LEGAL NAME *
Full legal entity name

ORGANIZATION TYPE *
Select organization type...

AUTHORIZED SIGNATORY NAME *
Full legal name

TITLE / POSITION *
e.g., Privacy Officer, CEO

BUSINESS EMAIL *
name@organization.com

PHONE *
(555) 000-0000

STREET ADDRESS *
Street address

CITY *
City

STATE *
CA

ZIP *
00000

2 Regulatory Confirmations

I confirm that my organization has determined that execution of a Business Associate Agreement is appropriate for its intended use of the TestLedger platform, and that an authorized signatory is executing this agreement. TestLedger makes no determination as to whether HIPAA applies to your organization or your intended use. Consult qualified legal counsel before executing this agreement.

Cancel Execute BAA Agreement

Figure 3. BAA Execution modal.

Before entering PHI

- Confirm that BAA Active status is displayed on the dashboard.
- Never enter Social Security numbers anywhere in TestLedger. Use employee identifiers only.
- If BAA status is inactive, contact your account administrator or TestLedger support before proceeding.

4. Identity Protection Key

The identity protection key is a 64-character hexadecimal value generated and controlled by your organization. When supplied at seal time, it enables HMAC-SHA-256 hashing of donor identity fields and AES-256-GCM encryption of designated narrative fields. The key is processed in the browser and is never transmitted to or stored on TestLedger servers.

Key behavior

- A 12-character key fingerprint is displayed for client-side confirmation.
- The same key is required later to reconstruct donor identity linkage in the Identity Verification Tool.
- If the key is lost, protected fields in previously sealed records cannot be decoded by TestLedger or any third party.

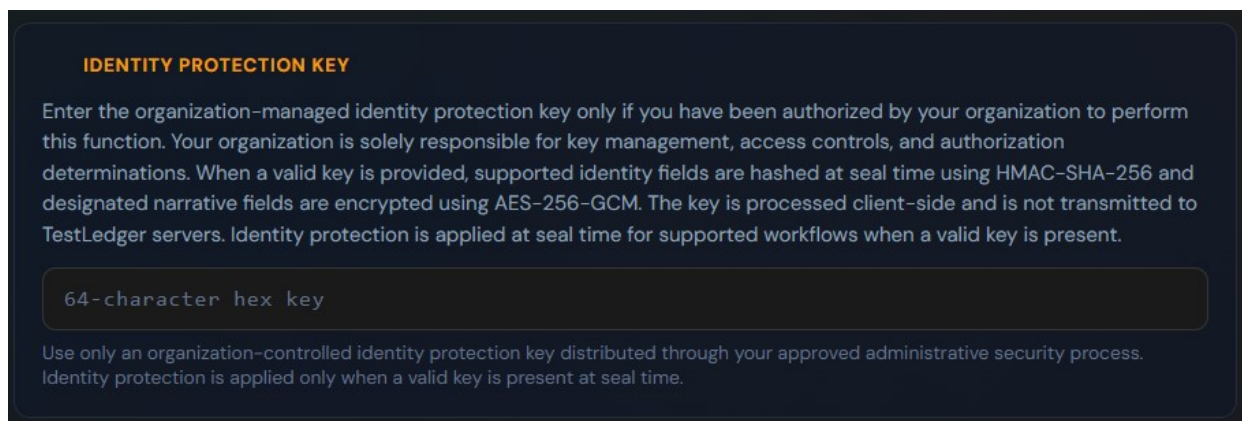


Figure 4. Identity protection key entry, processed entirely in the browser.

Key custody checklist

- Store the key in an organization-controlled password vault or key management system.
- Never store the key in TestLedger, in support tickets, or in unencrypted files.
- Limit access to the smallest set of authorized administrators.
- Maintain an internal key-custody, recovery, and rotation procedure before production use.

5. Workspace Dashboard

The workspace dashboard is the main operational surface. It shows monthly record usage (up to 2,000), team seats (up to 10), the billing cycle, the Workflow Queue, and the Organization Records list.

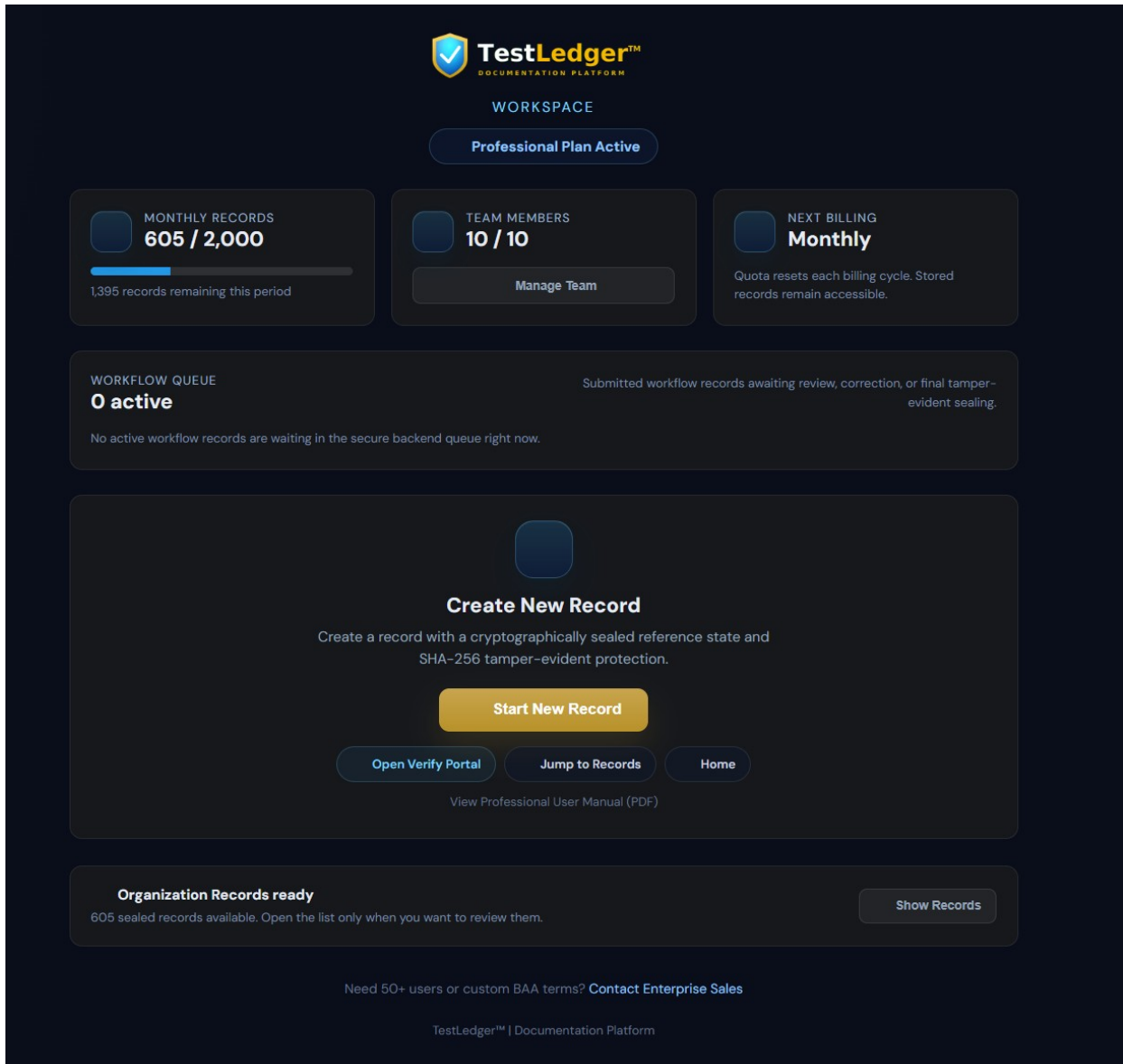


Figure 5. Professional workspace dashboard.

What you can do from the dashboard

- Start a new record using the 8-tab guided workflow (expands to 9 tabs when a non-negative THC result is entered).
- Open the Workflow Queue to review records awaiting seal.
- Open the Verify Portal.
- Open the Organization Records list to search, view, export, or download a record package.

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.

- Export every sealed record after sealing. Exports, combined with your identity protection key, give your organization a self-contained copy of the record.

6. Creating a Record

From the workspace, click Start New Record. The entry interface has eight tabs: Authorization, Donor, Consent, Collection, Result, Decision, Evidence, and CryptoSeal. A ninth tab, THC Context, is inserted between Result and Decision when a non-negative THC result is entered. Complete each tab in order.

6.1 Authorization

The screenshot shows the 'Test Authorization' form in the TestLedger Professional interface. At the top, the user is identified as 'QA Professional Owner' with the email 'pro.owner@testledgerqa.local'. The interface includes a 'Professional Plan' badge and a 'Sign Out' link. The TestLedger logo and 'Professional | Drug Test Record' are also visible. The 'Authorization' tab is selected among other tabs like Donor, Consent, Collection, Result, Decision, Evidence, and CryptoSeal. The form contains several input fields: 'EMPLOYER / ORDERING ORGANIZATION *' with a text input 'Company ordering the test'; 'REASON FOR TEST *' with a dropdown menu 'Select reason...'; 'TEST AUTHORIZATION DATE *' with a date input 'mm / dd / yyyy'; 'TEST AUTHORIZATION TIME *' with a time input '-- : -- --' and a clock icon; and 'TEST PANEL *' with a dropdown menu 'Select panel...'. A button 'Hide Additional Details 0/2 filled' is present. Below this, a note states: 'THESE FIELDS STRENGTHEN THE RECORD BUT ARE NOT REQUIRED TO SEAL. INFORMATION MAY ALREADY EXIST ON LAB REPORTS OR CCF WHICH CAN BE ATTACHED TO THIS RECORD PRIOR TO SEALING.' There are two more fields: 'POSITION / JOB TITLE' with 'Job title used in the organization record' and 'COMPANY POLICY REFERENCE' with 'e.g., Policy #HR-DT-2025 v3.2'. A 'NEXT MISSING ITEM' section indicates 'Employer / Ordering Organization is required.' and '5 blocking item(s) remain before you can move past this step.' with a 'Go to Required Field' button. A large yellow 'Next' button is at the bottom.

Figure 6. Authorization tab.

Fields

- **Employer / Ordering Organization:** Legal name of the employer or TPA requesting the test.
- **Reason for Test:** Pre-employment, random, reasonable suspicion, or post-accident.
- **Test Authorization Date:** Date the test was authorized under your organization’s SOP.

- **Test Authorization Time:** Corresponding time.
- **Test Panel:** 5-panel, 10-panel, or custom.
- **Additional Details (optional):** Position / Job Title and Company Policy Reference.

6.2 Donor Identification

The screenshot shows the 'Donor Identification' tab in the TestLedger Professional interface. The user is logged in as 'QA Professional Owner'. The form includes the following fields and options:

- DONOR CODE ***: Text input with placeholder 'Alphanumeric code assigned by'. A note below indicates 'BAA Active. PHI permitted for this field.'
- DONOR FULL NAME ***: Text input with placeholder 'First and Last Name'. A note below indicates 'BAA Active. PHI permitted for this field.'
- DATE OF BIRTH ***: Date picker with placeholder 'mm / dd / yyyy'.
- ID VERIFICATION METHOD ***: Dropdown menu with 'Select method...'.
- ID VERIFICATION OUTCOME ***: Dropdown menu with 'Select outcome...'.
- EMPLOYEE IDENTIFIER (LAST 4, NON-SSN)**: Text input with placeholder 'Last 4 of employee ID, not SSN'. A note below says 'Do not enter SSN.'

A 'Next Missing Item' alert box is present, stating: 'Donor Code is required. 5 blocking item(s) remain before you can move past this step.' A 'Go to Required Field' button is located next to the alert. At the bottom of the form are 'Previous' and 'Next' navigation buttons.

Figure 7. Donor Identification tab with PHI fields unlocked (BAA Active).

Fields

- **Donor Code:** Alphanumeric code assigned by the employer.
- **Donor Full Name:** First and last name of the donor. Available only when BAA status is Active.
- **Date of Birth:** Donor date of birth. Available only when BAA status is Active.
- **ID Verification Method:** For example, government-issued photo ID or employer badge.
- **ID Verification Outcome:** Verified, unable to verify, or refused.
- **Employee Identifier (Last 4, Non-SSN):** Optional. Last four digits of the employee ID. Never enter an SSN.

Donor Identification
Professional includes identity verification capture with audit logging.

DONOR CODE *
Alphanumeric code assigned by
De-identified use only. Do not enter names, DOBs, contact details, SSNs, or other PHI in this field.

DONOR FULL NAME *
This field unlocks only after a signed BAA is confirmed for Professional PHI-capable workflows. **Execute BAA**
For chain-of-custody only. Do not enter SSN or other identifiers.

DATE OF BIRTH *
This field unlocks only after a signed BAA is confirmed for Professional PHI-capable workflows. **Execute BAA**
Do not enter SSN or other identifiers.

ID VERIFICATION METHOD *
This field unlocks only after a signed BAA is confirmed for Professional PHI-capable workflows. **Execute BAA**
Locked by tier and PHI access policy.

ID VERIFICATION OUTCOME *
This field unlocks only after a signed BAA is confirmed for Professional PHI-capable workflows. **Execute BAA**
Locked by tier and PHI access policy.

Expand Additional Details 0/1 filled

NEXT MISSING ITEM
Donor Code is required. **Go to Required Field**
1 blocking item(s) remain before you can move past this step.

Previous **Next**

Figure 7a. Donor tab before BAA activation: identity fields are locked with an Execute BAA prompt.

Heads up

- Do not enter names, dates of birth, or other PHI until BAA Active status is confirmed.
- Never enter Social Security numbers.

6.3 Donor Consent

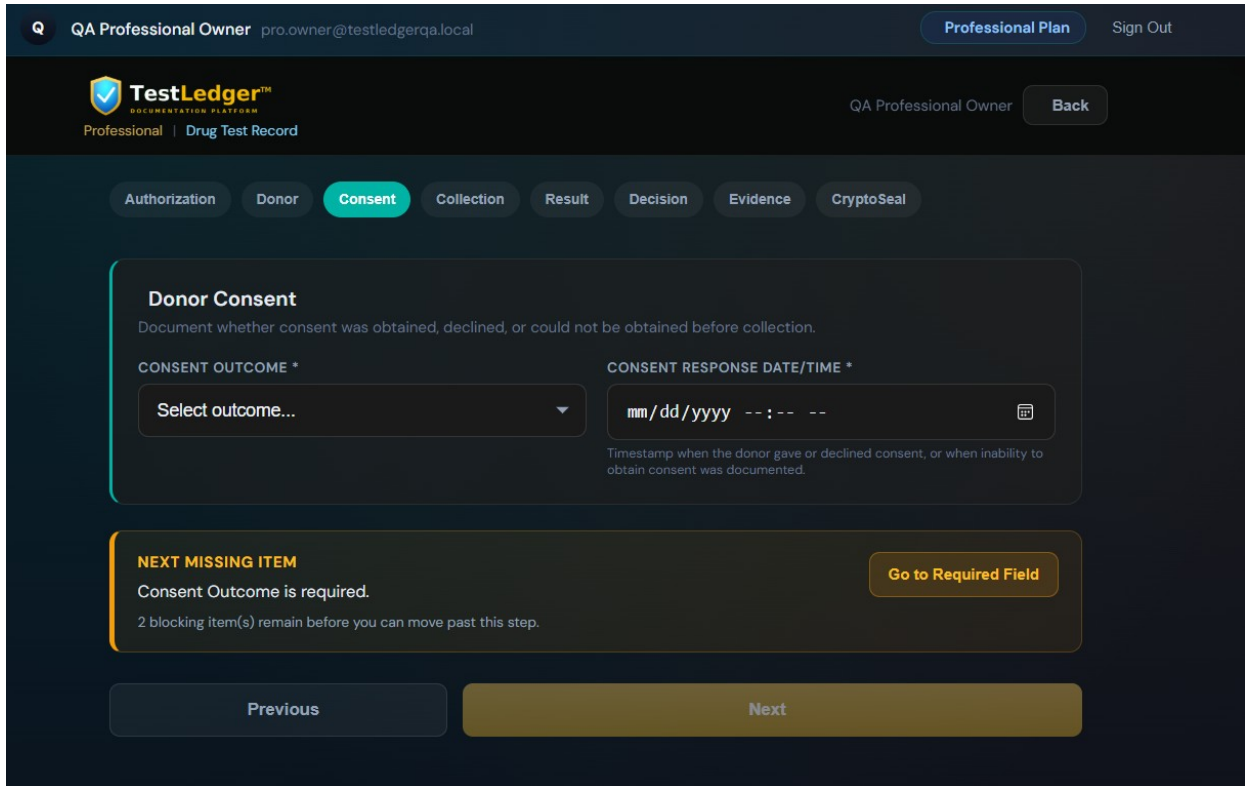


Figure 8. Donor Consent tab.

Fields

- **Consent Outcome:** Obtained, declined, or could not be obtained.
- **Consent Response Date/Time:** Timestamp associated with the consent outcome.

6.4 Specimen Collection

Specimen Collection
Professional includes detailed chain-of-custody controls and collection condition capture.

COLLECTION DATE/TIME *
mm/dd/yyyy --:-- --
Date and time specimen collection was completed.

COLLECTOR NAME *
Full name of specimen collector
Full legal name of individual who collected the specimen.

COLLECTION SITE *
Facility name and location (e.g.,

SPECIMEN TYPE *
Select type...

SPECIMEN ID / BARCODE * SCANNABLE
Primary specimen bar **Scan**
Links this record to the physical specimen and lab report. Must be at least 3 characters.

TEMPERATURE WITHIN ACCEPTABLE RANGE *
Select...

SPLIT SPECIMEN COLLECTED *
Select...

SEALS INTACT AT HANDOFF *
Select...

I CERTIFY THAT THIS SPECIMEN WAS COLLECTED IN ACCORDANCE WITH APPLICABLE PROCEDURES AND THAT CHAIN OF CUSTODY WAS MAINTAINED WITHOUT DOCUMENTED DEVIATION. *

Hide Additional Details 0/5 filled

THESE FIELDS STRENGTHEN THE RECORD BUT ARE NOT REQUIRED TO SEAL. INFORMATION MAY ALREADY EXIST ON LAB REPORTS OR CCF WHICH CAN BE ATTACHED TO THIS RECORD PRIOR TO SEALING.

COLLECTOR ID / CREDENTIAL
Badge number or credential IC

SPECIMEN TEMPERATURE (°F)
90-100°F within 4 minutes
Usually documented on the CCF

SPECIMEN VOLUME ADEQUATE
Select...

OBSERVED COLLECTION
Select...

COLLECTION REMARKS
Unusual circumstances, deviations, or observations

NEXT MISSING ITEM
Collection Date/Time is required.
9 blocking item(s) remain before you can move past this step.

[Go to Required Field](#)

Figure 9. Specimen Collection tab with collection-condition fields and the Chain-of-Custody Attestation.

Fields

- **Collection Date/Time:** Date and time specimen collection was completed.
- **Collector Name:** Full legal name of the collector. Do not enter donor information in this field.
- **Collection Site:** Facility name and location.
- **Specimen Type:** Select the specimen type.
- **Specimen ID / Barcode:** Primary specimen barcode. Scannable.
- **Temperature Within Acceptable Range:** Collector’s determination regarding specimen temperature.

- **Split Specimen Collected:** Whether a split specimen was collected.
- **Seals Intact at Handoff:** Collector’s observation regarding seal integrity at handoff.
- **Chain-of-Custody Attestation:** Checkbox capturing the collector’s statement regarding specimen handling.

6.5 Test Result

Test Result
Professional includes confirmation lifecycle tracking and recorded laboratory review details.

SCREENING RESULT * LABORATORY NAME * SAMHSA-CERTIFIED LABORATORY (IF APPLICABLE)

Select result... e.g., WestCoast Toxicology Lab

LAB ACCESSION NUMBER * LABORATORY CLIA / ID *

Links this record to the lab report e.g., CLIA-CA-55555

Found on the laboratory report. Must be at least 3 characters.

Hide Additional Details 0/2 filled

THESE FIELDS STRENGTHEN THE RECORD BUT ARE NOT REQUIRED TO SEAL. INFORMATION MAY ALREADY EXIST ON LAB REPORTS OR CCF WHICH CAN BE ATTACHED TO THIS RECORD PRIOR TO SEALING.

FINAL RESULT REPORT DATE LABORATORY RESULT NOTES

mm/dd/yyyy Supplemental factual notes from the source record if not fully captured above.

Structured fields above are primary; use this only for additional factual context from source documentation.

NEXT MISSING ITEM Go to Required Field

Screening Result is required.
4 blocking item(s) remain before you can move past this step.

Previous Next

Figure 10. Test Result tab with laboratory fields.

Fields

- **Screening Result:** Laboratory-reported screening outcome.
- **Substances Flagged:** Substances with presumptive positive results. Required when the screening result is non-negative.
- **Confirmation Result:** Confirmation result if available from the laboratory report.
- **Laboratory Name:** Name of the laboratory that performed the analysis.

- **SAMHSA-Certified Laboratory:** Check if the laboratory holds SAMHSA certification.
- **Lab Accession Number:** At least three characters. Links the record to the lab report.
- **Laboratory CLIA / ID:** CLIA certificate number for the reporting laboratory.
- **Final Result Report Date:** Optional. Date the final result was issued.
- **Laboratory Result Notes:** Optional. Supplemental notes transcribed from the source report.

Note

If the screening result includes a non-negative THC finding, a THC Context tab is inserted before the Decision tab. See Section 6.6.

6.6 THC Context (when applicable)

This tab appears only when a non-negative THC result is entered on the Result tab. When present, the workflow expands from eight tabs to nine.

The screenshot shows the TestLedger Professional interface. At the top, there's a header with the TestLedger logo and 'Professional | Drug Test Record'. On the right, it says 'QA Professional Owner' and a 'Back' button. Below the header is a navigation bar with tabs: Authorization, Donor, Consent, Collection, Result, **THC Context** (highlighted), Decision, Evidence, and Crypto Seal. The main content area is titled 'Recorded State Context' and contains the following text: 'Document recorded state context applicable to this THC-related result. This section preserves information recorded at the time of testing and review. It does not represent legal conclusions.' Below this are two dropdown menus: 'EMPLOYEE PRIMARY WORK STATE AT TIME OF TEST *' with a 'Select state...' option, and 'RECORDED STATE CANNABIS CONTEXT *' with a 'Select recorded context...' option. Below these is a 'NEXT MISSING ITEM' section with a yellow background, stating 'Employee Primary Work State at Time of Test is required.' and '2 blocking item(s) remain before you can move past this step.' There is a 'Go to Required Field' button. At the bottom are 'Previous' and 'Next' navigation buttons.

Figure 11. THC Context tab.

Fields

- **Employee Primary Work State at Time of Test:** Recorded primary work state of the employee when the test was conducted.
- **Recorded State Cannabis Context:** Descriptor selected for the cannabis regulatory context of that state.

6.7 Employment Action

The Decision tab captures the employment action as your organization has recorded it, along with the result referenced in that action.

The screenshot shows the 'Employment Action Documentation' tab in the TestLedger Professional interface. The form is titled 'Employment Action Documentation' and includes the following fields and sections:

- RECORDED EMPLOYER ACTION DATE/TIME ***: A date and time input field with a calendar icon.
- RECORDED EMPLOYER ACTION ***: A dropdown menu labeled 'Select recorded action...'.
- RECORDED RESULT REFERENCE ***: A dropdown menu labeled 'Select recorded result...'.
- DECISION MAKER ROLE ***: A dropdown menu labeled 'Select role...'.
- RECORDED BASIS / POLICY REFERENCE**: A text area with a placeholder 'Document the organization-recorded basis for this action as it was recorded at' and a 'Record the organization-documented basis for this action. TestLedger does not evaluate, validate, or advise on the sufficiency of any employment decision or justification.' note.
- RECORDED DECISION MAKER NAME**: A text input field with a placeholder 'e.g., Pat HR-Manager'.
- Hide Additional Details**: A button with a '0/1 filled' indicator.
- NEXT MISSING ITEM**: A notification box stating 'Recorded Employer Action Date/Time is required.' and '5 blocking item(s) remain before you can move past this step.' with a 'Go to Required Field' button.
- Navigation**: 'Previous' and 'Next' buttons at the bottom.

Figure 12. Employment Action Documentation tab.

Fields

- **Recorded Employer Action Date/Time:** Date and time the action was recorded.
- **Recorded Employer Action:** Return to duty, removal from safety-sensitive position, termination, or other.
- **Recorded Result Reference:** The result referenced for the action.
- **Decision Maker Role:** Role of the individual who recorded the decision.
- **Recorded Basis / Policy Reference:** Organization-supplied basis for the action.
- **Recorded Decision Maker Name:** Optional. Name and title of the decision maker.

Good practice

- Records that include employment action documentation may later be reviewed by management, counsel, auditors, or regulators. Treat the record as a controlled case file before sealing.

6.8 Evidence Vault

The Evidence Vault is available in Professional with an active BAA. It accepts photo capture and supporting documents up to 250 MB per record. Every file is hashed with SHA-256 at upload and recorded in the evidence manifest, which links to the parent record at seal time.

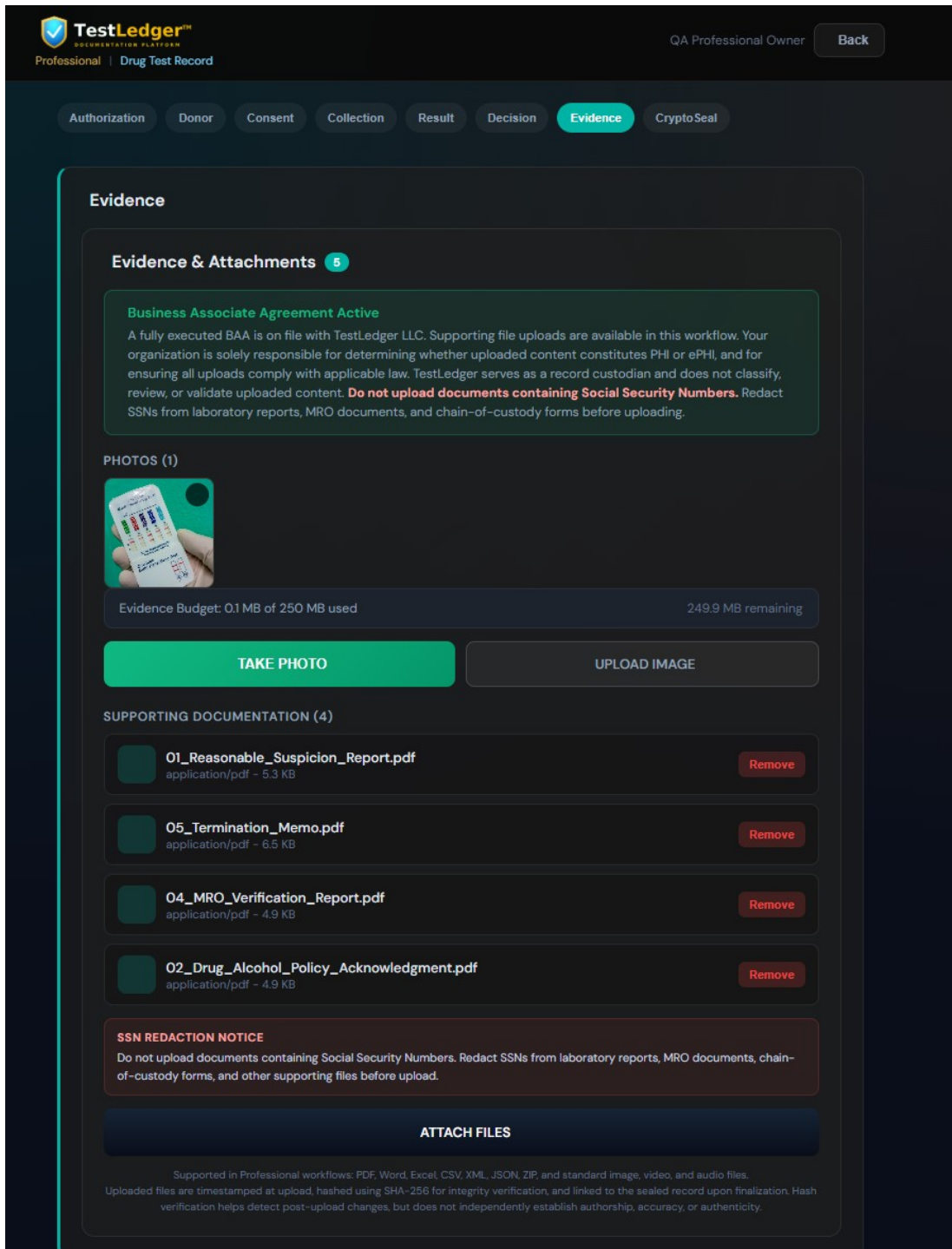


Figure 13. Evidence tab with the BAA Active banner.

What you can attach

- **Photos:** Captured or uploaded photographic evidence, hashed at upload.
- **Supporting documents:** PDF, Word, Excel, CSV, XML, JSON, ZIP, and standard image, video, and audio files.
- **Evidence budget:** Up to 250 MB per record. The remaining budget is shown in the tab.

Before upload

- Redact SSNs from laboratory reports, MRO documents, and chain-of-custody forms before uploading.
- Do not upload files that your organization has not authorized for storage in TestLedger.

6.9 Seal and Workflow Queue

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

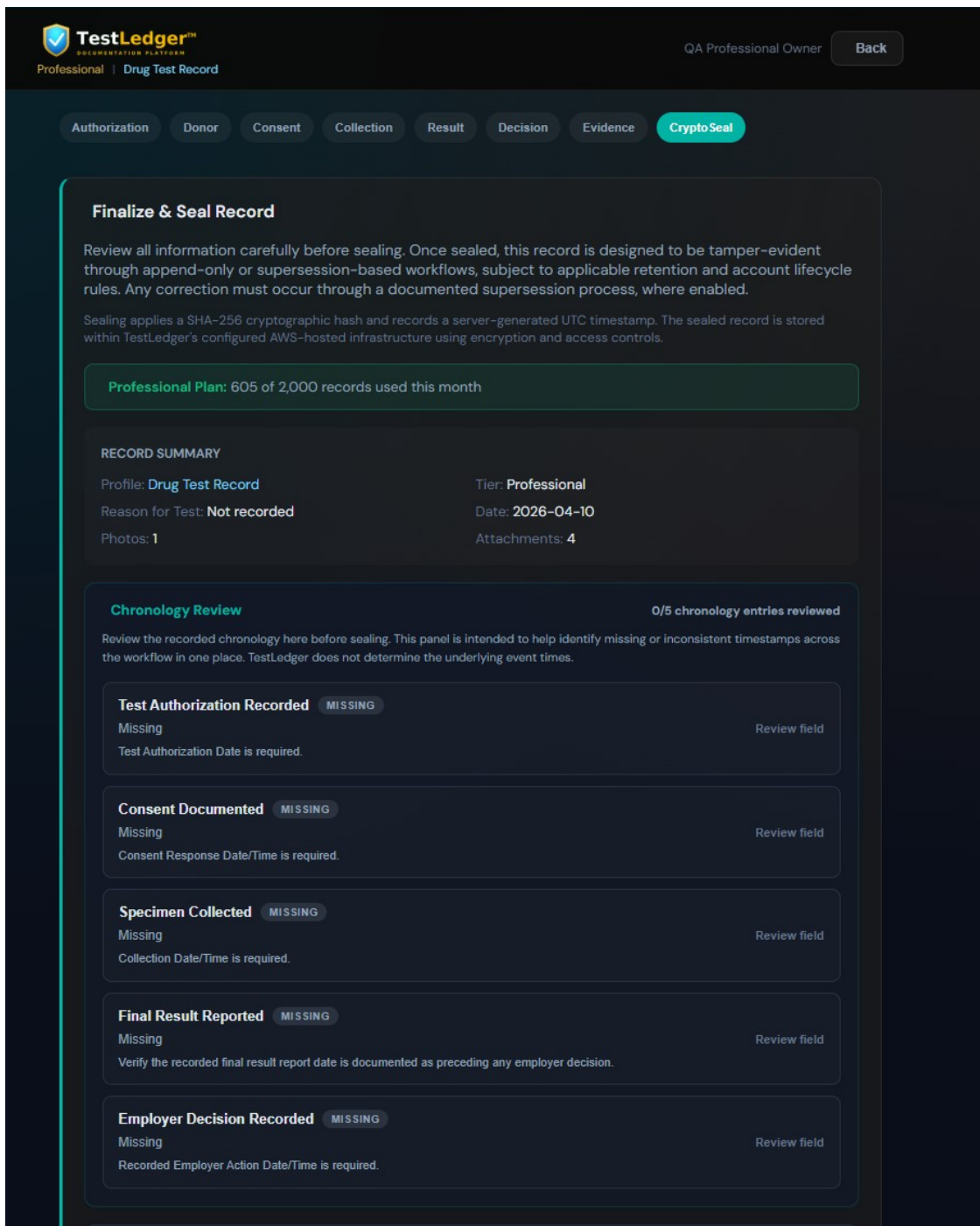


Figure 14. CryptoSeal tab with Chronology Review and completion map.

Separation of duties

- **Record Creator:** Fills all tabs and clicks Submit for Sealing. The record enters the Workflow Queue in pending_seal state.
- **Administrator:** Reviews the submitted record from the Workflow Queue and clicks CryptoSeal This Record to apply the seal. Administrators can also seal records they created themselves.

Chronology engine

The chronology engine compares timestamps across the record before the seal control activates. When a sequence issue is detected, a message is displayed with the specific problem.

Chronology Completion Map 6/8 required milestones complete

TestLedger records the chronology in the order documented by your organization. The following milestones are reviewed for completeness and consistency: employer authorization, donor identification, consent outcome, collection event, laboratory screening status, confirmation / mro review, final result reported to employer, hr decision, optional evidence attachment when used, and finally the CryptoSeal server timestamp.

REQUIRED TO SEAL

Employer authorization
Chronology issue: Specimen collection precedes test authorization. Verify workflow accuracy. Add a sequence deviation note before sealing if this sequence is confirmed by your organization's source records.
Blocked

Donor identification
Complete Complete

Consent outcome
Complete Complete

Collection event
Chronology issue: Specimen collection precedes test authorization. Verify workflow accuracy. Add a sequence deviation note before sealing if this sequence is confirmed by your organization's source records.
Blocked

Figure 14a. A chronology issue blocking seal until resolved.

- Hard blocks prevent sealing when collection precedes authorization, consent precedes collection, or the employer decision precedes the final result report.
- Tier 2 issues require a Sequence Deviation Note before sealing can proceed. The note is captured in the record and is not displayed on the public verify surface.

Before you seal

- Eight milestones must show Complete before the seal control activates.
- Read and confirm the pre-seal statement acknowledging data entry is complete.
- Once sealed, the record is tamper-evident. The platform does not provide an edit function for sealed records.

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.

7. Working With Sealed Records

Sealed records appear in the Organization Records list and are synced to TestLedger cloud storage with encryption at rest and in transit. Authorized team members see records within their assigned record access scope.

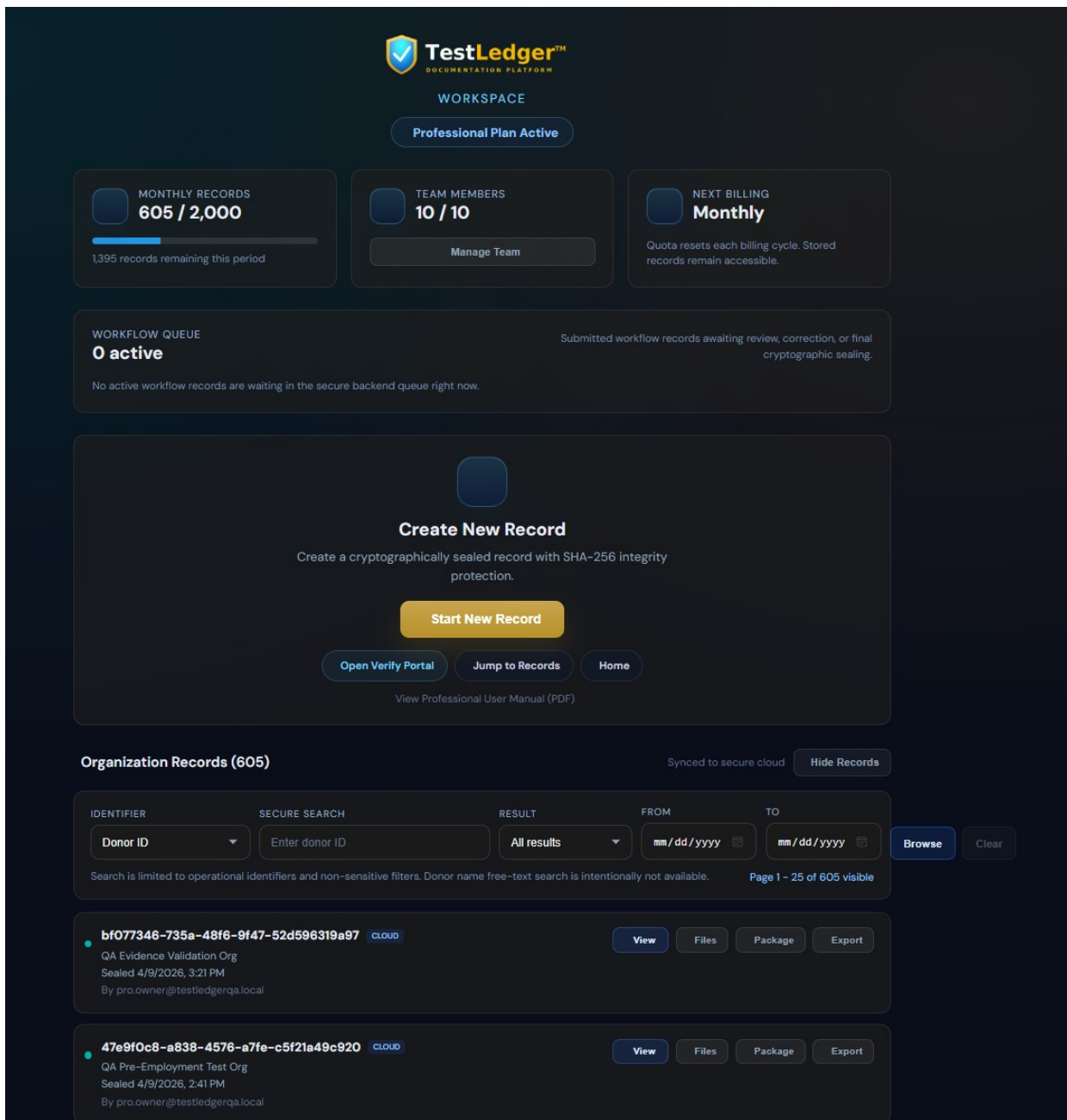


Figure 15. Organization Records list.

Actions on each record

- **View:** Opens the Secure Record Detail drawer.
- **Files:** Opens evidence files associated with the record.
- **Package:** Downloads the complete record package including the evidence manifest.
- **Export:** Downloads the sealed JSON export file used for verification.

Search

- Search is limited to operational identifiers and non-sensitive filters.
- Donor name free-text search is intentionally unavailable.
- The CLOUD badge indicates the record is synced to cloud storage.

Recommended retention practice

- Export every sealed record immediately after sealing.
- Store exports in a secure, organization-controlled location separate from TestLedger (for example, an encrypted network drive or records management system).
- For records with identity protection enabled, the exported JSON combined with your 64-character identity protection key lets your organization independently check the record for cryptographic consistency.
- Treat sealed record exports with the same retention schedule and access controls as other employment records.

8. Exporting and Sharing Records

Before exporting or producing a record for external review, confirm the purpose, the authorized recipient, the transfer method, and the destination storage location. Record the reason for export as part of your organization's documentation.

Recommended controls

- Use a controlled transmittal method appropriate to the sensitivity of the record.
- Minimize duplicate working copies. Apply local encryption where your policy requires it.
- Apply retention, legal-hold, and restricted-access rules immediately after download.
- Keep the record package together when external review is expected (the record, the evidence manifest, and the evidence files).

Reminder

- Once a file is downloaded, your organization's safeguards control what happens next.
- Do not transmit exported files by unencrypted personal email or consumer messaging channels.
- Do not place sensitive outcomes in filenames or exported file metadata.

9. 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>.

For exports that carry a `canonical_payload_hash`, the portal first performs a client-side canonical consistency check, then queries the server to compare against the sealed reference stored by TestLedger.

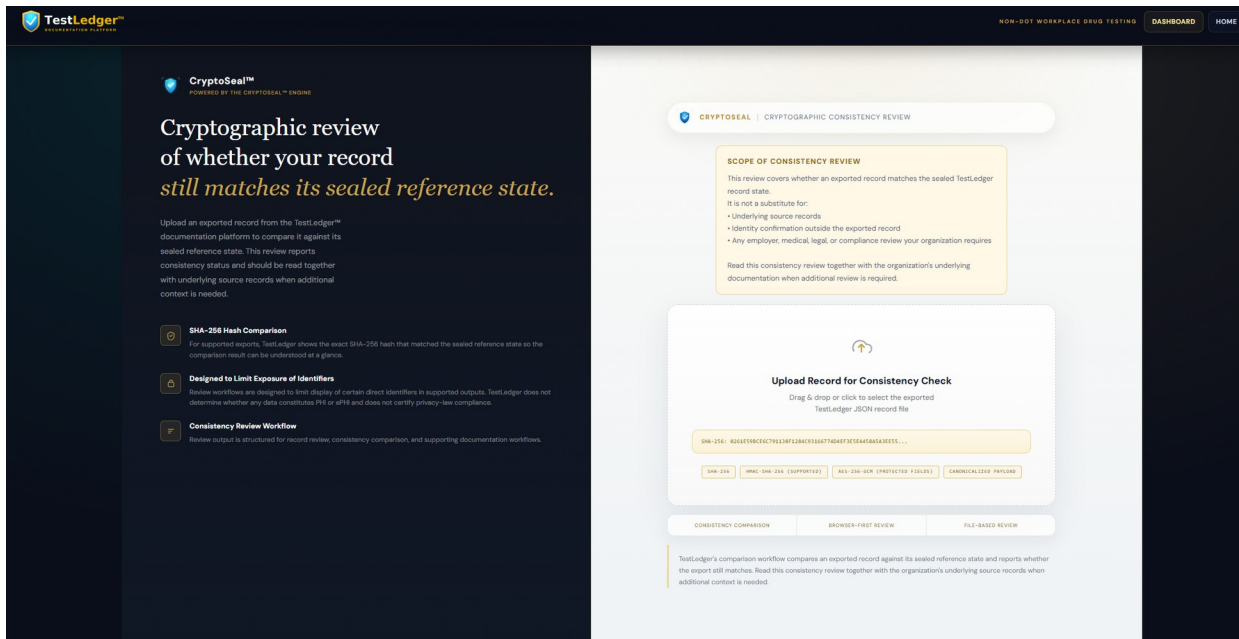


Figure 16. Verify Portal upload screen.

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 PHI or evidence files. It reports consistency status only.
- Professional exports include an Evidence Exhibit Register listing per-file SHA-256 hashes when an evidence manifest is present.

9.1 Consistent With Sealed State

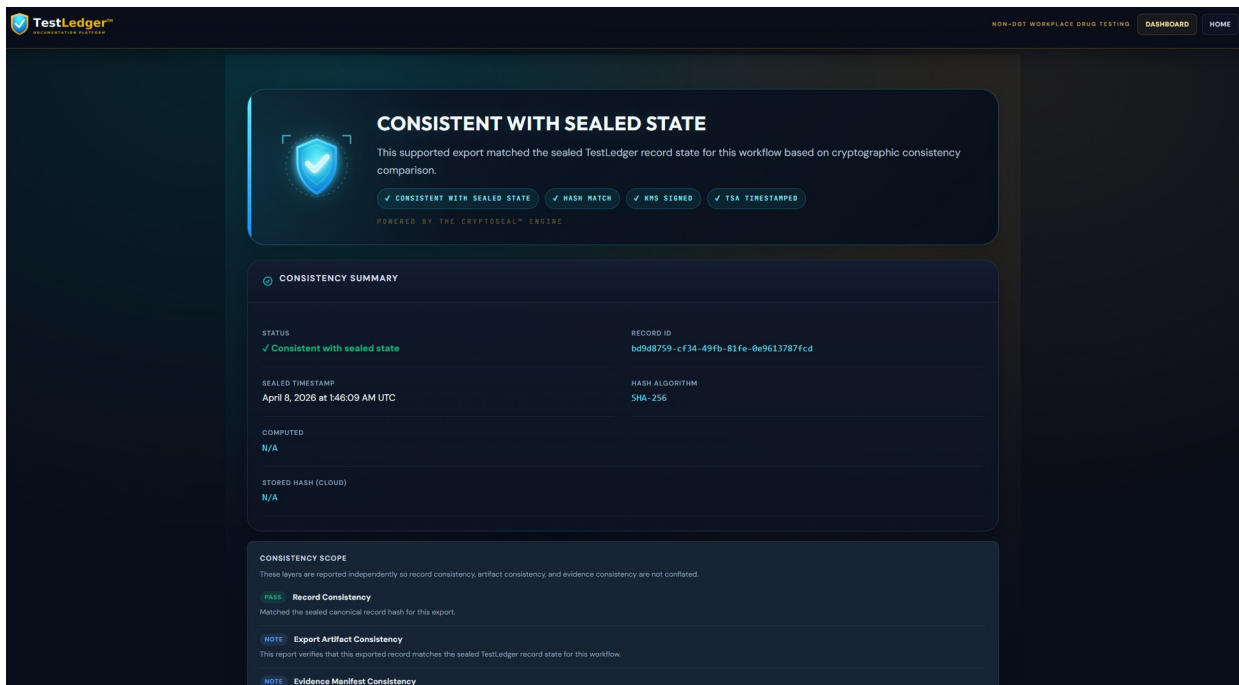


Figure 17. Consistent With Sealed State result.

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 export carries a valid AWS KMS ECDSA signature.
- **TSA Timestamped:** The export carries a valid RFC 3161 trusted timestamp (DigiCert).

9.2 Consistency Check Failed

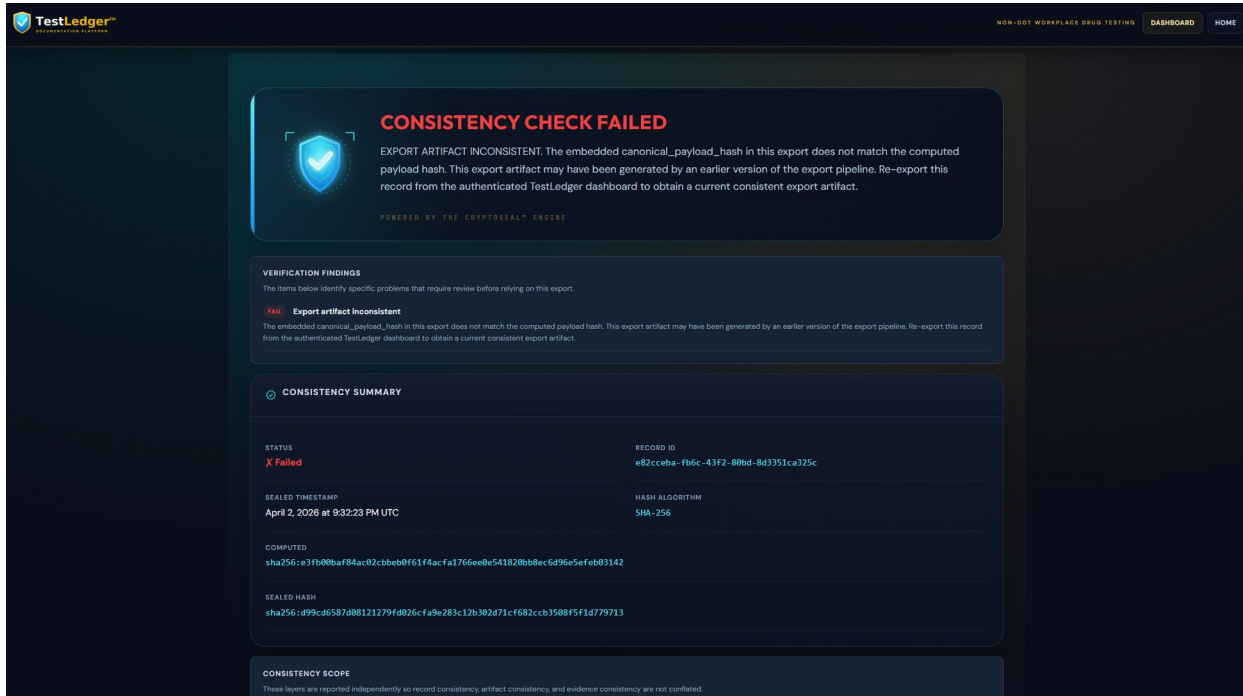


Figure 18. Consistency Check Failed result.

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 any review purpose.
- Contact your administrator and review the export source.
- A tampered or corrupted file will consistently fail the check.

9.3 Export Artifact Inconsistent

The failure screen may report EXPORT ARTIFACT INCONSISTENT when a record was exported using an earlier version of the export pipeline. Re-export the record from the authenticated dashboard using the current Export function. The re-exported file uses the current canonical format and should return Consistent With Sealed State.

10. Identity Verification Tool

The Identity Verification Tool is a standalone browser utility that reconstructs donor identity linkage from sealed Professional records. It runs entirely in the browser using the Web Crypto API. Nothing is transmitted or logged.

The tool is available at <https://testledger.pages.dev/identity-verify-tool.html>.

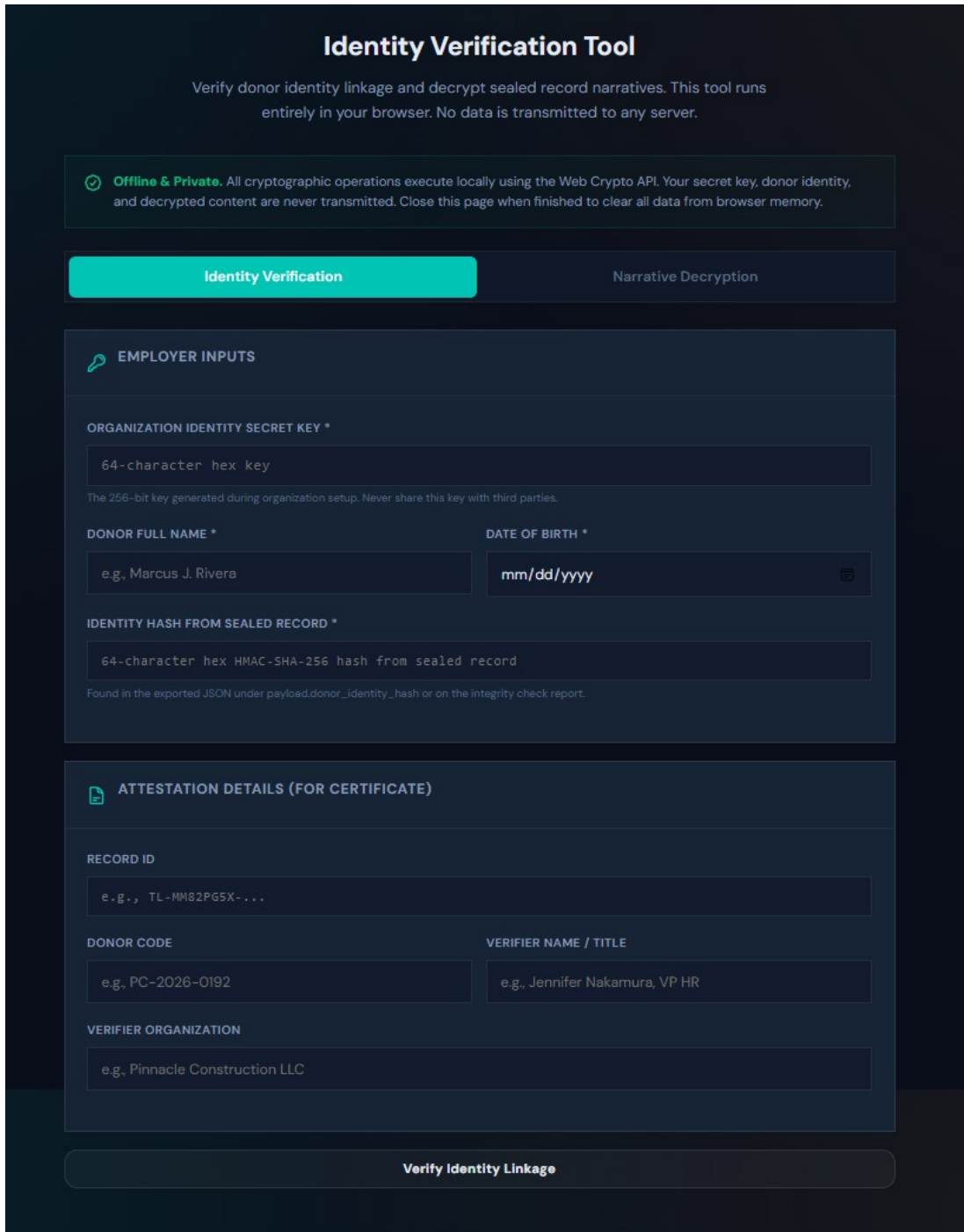


Figure 19. Identity Verification Tool.

Typical use cases

- An auditor or HR reviewer needs to compare a stored identity hash against a candidate name and date of birth.

- Internal QA is checking a stored identity hash against a candidate identity for a specific test event.
- Your organization is presenting a computational comparison as part of a broader evidentiary showing.

How to use it

- Supply your organization's 64-character identity protection key. TestLedger does not hold this key.
- Enter the candidate name and date of birth and the stored identity hash from the sealed record.
- Use the Narrative Decryption tab to decrypt AES-256-GCM encrypted narrative fields using the same key.
- Close the page when finished to clear all data from browser memory.
- Use the Attestation Details section to generate a verifier certificate documenting the comparison.

11. 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](#).