

Evidence Sharing Best Practices

Practical guidance for managing, sharing, and tracking digital evidence with FileSworn.

1. Temporary Access vs Preserved Evidence

Temporary Access

Files shared with temporary access auto-expire after a set period. Use this for opposing counsel review during negotiations, witness deposition prep, expert preliminary evaluation, or any situation where permanent third-party access is undesirable.

Expiration options: **24 hours** (quick review), **7 days** (standard review), **30 days** (complex productions), or a **custom date** for specific deadlines. Best practice: set the shortest reasonable expiration to minimize the exposure window.

Preserved Evidence

Files stored as preserved evidence remain permanently until manually deleted. This mode supports litigation hold, which prevents deletion even by the file owner. Use this for preservation obligations under FRCP 37(e), long-term archives, files needed across multiple proceedings, and evidence requiring tamper-evident records.

Using Litigation Hold

1. Upload the file in preserved evidence mode
2. Enable Litigation Hold from the file actions menu
3. The file is protected from deletion. Hold status is recorded in the access audit trail.
4. To release, disable from file actions. The release is also logged.
5. While active, the file cannot be deleted through the dashboard or API.

2. Organizing Evidence

Cases and Matters

- Create cases from the dashboard to group files by litigation
- Each case gets its own Bates numbering sequence
- Assign files to cases during or after upload

Tags

- Add custom tags to any file (e.g., "Exhibit A", "Deposition", "Body Cam", "Surveillance")
- Use tags alongside cases for cross-case categorization

Search and Filter

- Search by filename, SHA-256 hash, or tag
- Filter by file type, upload date, status, and storage mode
- Find specific files quickly even with large libraries

Bates Numbering

- Automatic sequential numbering per case
- Numbers locked once assigned (cannot be changed)
- Follows standard legal document identification format
- Referenced in production logs and certificates

Naming Conventions

Even with cases and tags, consistent file naming helps when working outside of FileSworn:

- Prefix with case number: "2024-CV-1234_surveillance_video.mp4"
- Include dates when relevant: "2024-03-15_deposition_exhibit_A.pdf"
- Use consistent naming across all files in a matter

3. Sharing and Watermarking

Creating Effective Share Links

- Set appropriate expiration based on recipient need
- Enable recipient identity verification for sensitive materials
- Choose watermark detail level based on case sensitivity:

Level	Shows	Best For
Standard	Viewer email	Routine sharing, basic attribution
Detailed	Email + timestamp	Sensitive materials, time-based attribution
Full	Email + timestamp + IP hash	Highly sensitive, IP-level attribution

Batch Sharing

- Share one file with multiple recipients in a single workflow
- Each recipient gets a unique share link with their own watermark
- Access tracked independently per recipient
- Useful for multi-party discovery or multiple expert reviews

Watermark Best Practices

- Inform recipients that content carries a viewer identity watermark. This acts as a deterrent.
- If a leak occurs, compare leaked content against the access audit trail to identify the likely source.
- Use watermarked sharing for sensitive or confidential materials.
- Combine watermarking with short expiration for maximum security.
- Choose Full detail level for materials where you may need to prove exactly when and from where content was accessed.

4. Discovery Productions

What Production Tracking Does

Production tracking documents formal evidence transfers to opposing counsel. It covers the handoff moment: what was sent, to whom, when, and whether received. It is not e-discovery software and does not handle document review or filtering.

Creating a Production

1. Navigate to Productions in the sidebar (Professional and Enterprise)
2. Click "Create Production"
3. Select files from your evidence library
4. Assign a production number (auto-suggested or custom)
5. Specify recipient name and email
6. Review file list with Bates numbers and SHA-256 hashes

Sending and Confirming

- Click "Send" to deliver watermarked share links to the recipient
- Each file gets a unique share token with 30-day expiration
- FileSworn automatically confirms delivery when the recipient accesses the files
- Production status updates: Draft, Sent, Confirmed

Production Log PDF

- Download a complete production log documenting the transfer
- Includes: production number, date, recipient, file list with Bates ranges, SHA-256 hashes, and access status per file
- Use as a cover sheet for formal discovery productions

5. Monitoring and Documentation

View Activity Tracking

- Every shared file has a view activity panel
- Each access event shows: viewer email, timestamp, device info, IP address
- Expandable per-share history for files with multiple links

Downloadable Receipts

- PDF receipt for each individual view event
- Documents specific access details for court filings
- Proves opposing counsel received and viewed evidence

Access Notifications

- Email alerts sent when evidence is viewed
- **Essential:** 10 notifications per month
- **Professional and Enterprise:** unlimited notifications

For questions or help implementing these practices, contact anthony@filesworn.com or schedule a walkthrough at calendly.com/anthony-kulick/filesworn-demo.