Don't let the data walk out the door: Aligning legal, HR, and IT at employee exit

By Tara Lawler, Esq., Matthew Hamilton, Esq., and Lindsey Bonafede, Esq., Morgan Lewis

MARCH 31, 2026

Employee departures represent a critical inflection point in data preservation. Without a documented, coordinated departing employee process for individuals subject to legal hold, the company may risk inadvertent spoliation of evidence through the loss, deletion, or alteration of potentially relevant data during offboarding. This can lead to court sanctions, adverse inference instructions, and increased litigation costs if remedial data recovery efforts are needed.

A proactive, cross-functional strategy not only protects against litigation exposure but also demonstrates a culture of defensible information governance.

Departing employees: a predictable preservation risk

Employee departures trigger cascading technical and administrative changes. HR initiates offboarding; IT disables credentials and reallocates licenses; collaboration platforms may update ownership; and retention clocks begin counting down toward deletion.

In remote and hybrid environments, the departing employee's digital footprint may span numerous systems: email, cloud storage, collaboration tools, mobile devices, and personal devices under BYOD policies.

If that employee is subject to an active legal hold, any uncoordinated action can compromise preservation, and knowledge of that employee's data storage habits may be lost. Mailboxes may be deleted after a retention window. Documents from OneDrive or Google Drive accounts may be transferred to a successor altering metadata. Devices may be reimaged before relevant data is secured. Messaging content may disappear when mobile accounts are reset.

Courts closely scrutinize preservation efforts, particularly when data is lost during employee departures. Increasingly, they expect organizations to maintain mature, integrated workflows that address these risks proactively. While perfection is impossible, that is not the legal standard — the law requires reasonable and proportional efforts. A well-designed structured process can help meet that standard, whereas its absence may be viewed not merely as an oversight, but as a broader governance lapse.

The case for strategic guidance

Designing and implementing a defensible departure preservation framework requires more than internal coordination. It demands a sophisticated understanding of litigation risk, data architecture, regulatory obligations, and evolving judicial expectations.

Without a documented, coordinated departing employee process for individuals subject to legal hold, the company may risk inadvertent spoliation of evidence through the loss, deletion, or alteration of potentially relevant data during offboarding.

Engaging experienced e-discovery and information governance advisors can transform a reactive offboarding process into a defensible preservation framework. From policy development and process engineering to technical implementation and defensibility documentation, experienced counsel can help ensure that departure events do not become litigation liabilities.

Governance should be intentional and structured

Effective preservation during employee departures is best supported by thoughtful coordination, clearly defined roles, and disciplined execution across relevant teams.

Legal: oversight and strategic control

The Legal department should have real-time visibility into all custodians subject to active legal holds.

When notified of a pending departure, Legal could consider taking steps such as:

- Confirming the individual's hold status.
- Reissuing preservation instructions, as appropriate.
- Coordinating promptly with IT regarding any necessary technical controls.
- Ensuring that custodian tracking systems are integrated with HR's departure workflows.

Human resources: the gatekeeper

Because HR is often the first to receive notice of resignations or terminations, organizations may benefit from implementing a standardized notification workflow that promptly alerts Legal and IT.

Offboarding procedures may also be strengthened by incorporating a legal hold check before accounts are modified or deleted. In addition, HR might consider integrating preservation-related steps into exit processes, such as obtaining a certification from the departing employee acknowledging any continuing preservation obligations.

IT: technical enforcement of preservation

When notified that a departing employee is subject to a hold, IT may take steps to ensure that automated deprovisioning processes do not compromise preservation efforts.

Depending on the circumstances, this could include:

- Placing mailboxes on hold.
- Preserving OneDrive, Google Drive or similar personal cloud storage.
- Securing data from collaboration platforms.
- Suspending applicable auto-deletion policies, where appropriate.
- Imaging devices, where appropriate.
- Preserving mobile device data consistent with company policy and applicable law.

Managers: early visibility and practical insight

Managers often have advance awareness of employee departures. Organizations may benefit from training managers to promptly escalate notice of departures and to avoid informal data transfers or deletions.

Managers can also provide useful insight into where key business data resides — particularly within shared drives or applications that may not be apparent from centralized systems.

Taking a 360° view of departing employee data

While email data is often critical, a common preservation misstep is concentrating exclusively on email. Today's custodians create and retain information across a broad array of platforms, many of which house unique, non-duplicative, and potentially relevant data that may also require preservation.

Email

Email remains central, and preservation should encompass, if applicable:

- Active mailbox content.
- Archived mailboxes.
- Exported PST files (a format used by Microsoft to store email data locally).
- Journaling systems.

Holds must be applied before licenses are reassigned or accounts disabled.

Cloud storage and collaboration platforms

Modern work environments rely on cloud-based platforms.

These may include:

- OneDrive, Google Drive or other individual cloud storage accounts.
- Shared drives (e.g., SharePoint).
- Microsoft Teams, GChat, Slack, or similar collaboration platforms.
- Project management tools.

Data stored in shared environments can present unique challenges, particularly when ownership or permissions change upon departure.

Local devices and network storage

Employees may store relevant information on:

- Laptops and desktops.
- Network file shares.
- External storage devices.

Reimaging or redeployment of devices without preservation of unique, non-duplicative potentially relevant data presents risk. In certain matters, forensic imaging may be appropriate.

Mobile devices and messaging

Business communications increasingly occur via mobile devices and messaging platforms.

Organizations should evaluate:

- Company-issued phones and tablets.
- BYOD devices, consistent with company policy and applicable law.
- Text messages.
- Third-party messaging applications used for business (e.g., WhatsApp, Telegram, Signal).

Mobile preservation requires careful coordination, technical capability, and sensitivity to privacy considerations.

Structured systems

Employees may generate or store relevant information within structured systems such as:

- CRM platforms.
- ERP systems.
- Financial applications.
- Industry-specific databases.

Preservation may involve securing user-generated content, logs, or reports.

Paper records

Physical documents should not be overlooked. Paper files, notebooks, and offsite storage may contain relevant materials. Offboarding procedures should include collection and secure storage where required.

A step-by-step departure preservation workflow

To ensure consistency and defensibility, organizations should implement a standardized process. Recommended steps include:

Advance notice and automated notification: When a manager becomes aware of a departure, HR should be notified promptly. HR then can notify Legal and IT.

Legal hold verification: Legal confirms whether the employee is subject to active holds and this is communicated to the other stakeholders.

Pre-departure communication: Where feasible and appropriate, a pre-departure meeting should remind the employee of ongoing preservation obligations and instruct the employee not to delete information as well as gather information regarding their data storage habits for any data that is subject to a legal hold.

Technical preservation before deactivation: IT applies holds, suspends deletion policies, and secures devices before access changes occur.

Device and record collection: Company devices are collected and preserved as appropriate. Physical documents are secured.

Policies, controls, and best practices

A well-designed process depends on strong governance.

Organizations should consider implementing:

- Written legal hold and offboarding policies.
- HR–Legal–IT notification workflows when feasible.
- Standardized preservation checklists.
- Manager and HR training programs.
- Periodic audits of offboarding procedures.

Pre-exit certifications acknowledging preservation obligations can further strengthen defensibility. Organizations may also conduct periodic testing of their departure workflows to identify gaps.

Tara Lawler is a regular contributing columnist on e-discovery for Reuters Legal News and Westlaw Today.

About the authors

Tara Lawler (L), a partner at **Morgan Lewis**, with experience in strategic discovery portfolio management and data governance, focuses on discovery, information governance (IG), data privacy, security, and artificial intelligence (AI). She partners with in-house legal and technology teams to assess, develop and implement best practices for discovery and data management. She is based in the Philadelphia office and can be reached at tara.lawler@morganlewis.com. Matthew Hamilton (C), of counsel at the firm, is a civil litigator and e-discovery counsel who represents clients in complex pharmaceutical and medical products liability, data breach, antitrust, and commercial litigation. He is based in the Philadelphia office and can be reached at matthew.hamilton@morganlewis.com. Lindsey Bonafede (R), an associate at the firm, focuses her practice on e-discovery, information governance, and data privacy. She partners with in-house legal departments, information technology, and records management teams to provide litigation management across the pharmaceutical, healthcare, and technology industries in all phases of e-discovery. She is based in the firm's Princeton office and can be reached at lindsey.bonafede@morganlewis.com.

This article was first published on Reuters Legal News and Westlaw Today on March 23, 2026.