

How to Talk to Legal About Data Retention

Guide for IT Leaders



Preparation: Retention Audit

Data Inventory

- Where does data live? (Email, Teams/Slack, SharePoint, file shares, legacy archives, backups)
- Who owns each platform or data source?
- Roughly how much data is in each location, and how fast is it growing?

Current State of Retention

- What retention settings (if any) already exist across your systems?
- Are there platforms with no retention rules at all?
- Are there known instances of "keep everything" defaults still in place?

Possible Constraints

- Storage cost trends and budget
- Systems nearing end-of-life or planned migrations
- Any existing legal holds and how they're currently tracked
- Active retentions on WORM devices

Information: Questions to Ask Legal

- What regulatory or industry requirements apply to us?
- Are there different retention periods for different record types?
- What triggers a legal hold, and who's responsible for issuing one?
- How should legal holds interact with automatic deletion?
- What counts as acceptable documentation if a deletion is ever questioned?
- How often should the policy be revisited? How will changes in regulations trigger a policy review?
- Who has final sign-off when IT and Legal disagree on a retention period?

Follow-Up: Technical Logistics

- Whether your systems can enforce different retention periods by data type, department, or platform
- What it takes to place and lift a legal hold across your current tools
- Where automated deletion is (and isn't) currently possible
- The cost and effort difference between "retain everything" and a tiered schedule

Flag any requirement Legal proposes that isn't technically enforceable with your current system. Offer solutions: adjustments to their proposal, implementing new software or tools, or a timeline for adjusting your current environment.

Resources

Defensible Retention Checklist

- ☐ Retention periods are documented by record type, not applied as one blanket rule
- ☐ The policy specifies which regulations or standards drove each retention period
- ☐ Legal hold process is documented, including who can issue and lift a hold
- ☐ Legal holds are confirmed to override automatic deletion across every platform
- ☐ Retention rules are mapped to every platform where data lives
- ☐ Responsibilities are assigned: who enforces the policy day to day, and who updates it
- ☐ A review cadence is set (annually, at minimum, or whenever relevant regulations change)
- ☐ Enforcement is consistent
- ☐ The policy itself is stored and version-controlled

Templates

[Download Template \(.xlsx\)](#)

Data Inventory

Location	Volume	Ownership	Current Retention

Data Retention Regulations

Regulation	Data Type	Retention Period	Source(s)	Applies To
HIPAA	Compliant and Resolution Documentation	6 years	Email, Teams, EHR, OneDrive	All
Texas Medical Board	Patient Medical Records	- Adults: 7 Years after last treatment - Minors: 7 years after last treatment or until patient is 21 (whichever is longer)	EHR	Physicians
Texas Health and Safety Code	Patient Medical Records	- Adults: 10 years after last treatment - Minors: 10 years after last treatment, or until patient is 20 (whichever is longer) - Records related to any known unresolved litigations: Never - Records related to sexual assault forensic medical examination: 20 years	EHR	Hospitals