GLOBAL DIGITAL FORENSICS

INFORMATION GATHERING LIBRARY

Information Gathering Reference

Preparation packages for NYDFS Part 500, New York private information, defense contracting, export controls, departed employees, commercial disputes and medical matters

Edition 2026-11-03 | November 3, 2026

> Use this reference to organize the facts, records and contacts a specialist needs before an audit, a forensic collection or a legal review begins. Each package lists the records to find, who usually holds them, the questions for IT and business owners, and the decisions that belong to counsel or the receiving specialist.
>
> The editable CSV worksheets in the library carry the same requests, so a coordinator can assign owners, track responses and hand over an index of what was found and what is missing.

Questions about this document: call (800) 868-8189 or write to info@evestigate.com.

© 2026 Global Digital Forensics, Inc. All rights reserved.

Contents

1. How to use this library
2. Walkthrough from request to handoff
3. Who helps with the gathering
4. Suggested handoff folders
5. Choosing the right package
6. Common terms
7. Receiving the package and timing
8. Where relevant data can live: the data source atlas
9. Package 01: NYDFS Part 500
10. NYDFS Part 500: records to find
11. NYDFS Part 500: questions for IT and system owners
12. NYDFS Part 500: decisions and handoff
13. Package 02: New York private information
14. New York private information: records to find
15. New York private information: questions for IT and system owners
16. New York private information: decisions and handoff
17. Package 03: Defense contractor cybersecurity
18. Defense contractor cybersecurity: records to find
19. Defense contractor cybersecurity: questions for IT and system owners
20. Defense contractor cybersecurity: decisions and handoff
21. Package 04: Export controls
22. Export controls: records to find
23. Export controls: questions for IT and system owners
24. Export controls: decisions and handoff
25. Package 05: Departed employee
26. Departed employee: records to find
27. Departed employee: questions for IT and system owners
28. Departed employee: sample questions for counsel
29. Departed employee: decisions and handoff
30. Package 06: Commercial and contract disputes
31. Commercial and contract disputes: records to find
32. Commercial and contract disputes: questions for IT and system owners
33. Commercial and contract disputes: sample questions for counsel
34. Commercial and contract disputes: decisions and handoff
35. Package 07: Medical matters

© 2026 Global Digital Forensics, Inc. All rights reserved.

36. Medical matters: records to find
37. Medical matters: questions for IT and system owners
38. Medical matters: sample questions for counsel
39. Medical matters: decisions and handoff
40. Source register

© 2026 Global Digital Forensics, Inc. All rights reserved.

How to use this library

Begin with the records you already have.

Each package follows the same pattern. It opens with the facts to settle before you gather, lists the records to find with a suggested owner for each, gives a short question set for client IT and system owners, and closes with the decisions that belong to counsel or the receiving specialist. An unanswered question is a request for help, not evidence of a problem.

Work from the CSV worksheets. Import them as UTF-8, keep the ID columns as text, and widen and wrap the columns before you start. The blank response columns are for your entries. Each worksheet is an index: point to records held in your approved evidence location rather than pasting passwords, patient data or controlled technical information into it.

The first conversation

Open Intake-template.csv and settle seven topics with the business sponsor and counsel: the matter and organization, the purpose and who asked for the work, the period and locations, the people involved, the systems and data, any immediate concerns, and how records will be shared. Immediate concerns come first. An active incident, imminent deletion, expiring logs, a court order or a contractual deadline goes to counsel or the responsible specialist at once, ahead of the worksheet.

Walkthrough from request to handoff

Eight steps take a matter from the first request to a controlled handoff.

1. Name the matter and the recipient

Record the legal entity, business unit or case, the intended recipient, the purpose, the relevant period, the sites, the systems and the client contact. Ask the recipient which criteria, versions and deliverable format they expect. Keep an audit preparation request separate from an incident response or litigation deadline.

2. Identify people and places

Ask the business owner what work occurred and ask IT where the resulting information lives. Include providers, acquired businesses, former accounts, paper files and legacy systems. Start with the data source atlas and create one inventory row per actual tenant, repository or device, not one row per vendor name.

3. Check authority and preserve when necessary

Before anyone changes accounts, retention settings or content, ask counsel and the authorized system owner what must be preserved and who can act. Escalate short lived logs and pending deletions promptly. Check that each hold covers the intended scope and was applied successfully, and record the date it took effect.

4. Gather existing records safely

Request existing exports and documentation through approved channels. Ask for a scoped collection plan if forensic acquisition, production testing, restoration or third party access is needed. Use IDs and redacted examples until the receiving specialist confirms a secure route, and keep passwords, recovery secrets, private

© 2026 Global Digital Forensics, Inc. All rights reserved.

keys, patient records and controlled technical data out of ordinary email and web forms.

5. Describe what was supplied

Give every request an ID and every record an identifier. Record the source system, account or tenant, owner, period, collection time with time zone, method, filters, permissions, file format and known omissions. Where appropriate, the collector creates and verifies a cryptographic hash. A matching hash shows two copies are identical, so the specialist reviews exactly the record that was collected.

6. Show gaps and limits

Use the statuses Not started, Requested, Received awaiting specialist review, Partially received, Not available after inquiry, and Proposed not applicable awaiting confirmation. Explain a missing period, an excluded field, a failed export or an uncertainty. Keep Unknown as Unknown, and mark a request complete when every record it asks for has arrived.

7. Prepare a controlled handoff

Reconcile the request checklist with the file inventory. Separate ordinary records from restricted evidence and potentially privileged material. Agree access, permitted recipients, transmission encryption and retention, then obtain a receipt and list the follow up questions. The recipient decides whether the information supports the proposed engagement.

8. Keep the package current

Keep the edition and the date the sources were last checked with the handoff. Recheck the rules and vendor documentation before the next engagement and whenever the facts change. Version new submissions, keep the earlier index and explain the changes. Release a preservation hold or destroy records only on the decision of the owner and counsel.

Who helps with the gathering

Small organizations combine roles; the decisions stay with the person who holds the authority.

Role	What they contribute
Business contact	Explains the business, the relevant events, services and people, and can point to records without answering technical control questions.
Project coordinator	Tracks requests, owners, dates, follow up and the handoff, and keeps receipt separate from specialist acceptance.
IT and provider contacts	Describe actual systems, permissions, retention, logging and export limits, and arrange authorized technical work.
Counsel and privacy lead	Decide case scope, preservation, legal authority, privilege, protected information and applicable duties.
Receiving specialist	Agrees criteria and scope, specifies further evidence and evaluates it. Export classifications and audit conclusions stay with qualified decision makers.

© 2026 Global Digital Forensics, Inc. All rights reserved.

Suggested handoff folders

Use Record-index-template.csv for one row per file or defined record set: the request it answers, the original source, date range, collector and method, approved location and limits. Handoff-checklist.csv tracks the ten handoff steps.

Folder	Contents
00 Scope and contacts	Engagement purpose, entity or matter facts, period, owner roster and exclusions.
01 Requests and responses	Completed request list, IT questionnaire, follow up records and open questions.
02 Record index	Pointers to approved evidence locations with source, date, method, limits and receipt; no sensitive data in the index itself.
03 Source records	Existing policies, diagrams, contracts and exports; restricted material stays in its approved repository.
04 Specialist decisions	Applicability, legal or process decisions, export classifications or the technical collection plan once supplied.
05 Handoff and updates	Transmittal, recipient receipt, known gaps, version history and supplemental requests.

Choosing the right package

Seven packages cover the most common requests. For other programs, the table shows what to collect first.

Program	Starting facts	Records to locate	Where to start
NYDFS Part 500	Entity operating, or required to operate, under a DFS authorization.	Legal entity and license, examination request, exemption and Class A support, period and program records.	Package 01.
New York private information	New York resident data, owner or maintainer status and sector.	Data fields and combinations, data flows, safeguards, entity facts and any incident chronology.	Package 02.
CMMC and defense safeguarding	Actual solicitation, contract, flowdowns, data types and current modifications.	Signed clauses, SSP and boundary, FCI and CUI facts, providers and assessment records.	Package 03.

© 2026 Global Digital Forensics, Inc. All rights reserved.

Program	Starting facts	Records to locate	Where to start
EAR and ITAR	Items, software, technology and services, parties, locations and planned activity.	Specifications, prior classifications, licenses and agreements, access map and data handling.	Package 04.
Departed employee, commercial or medical matters	The legal matter, its issues, custodians and period.	The sources listed in the package for that matter type.	Packages 05, 06 and 07.
Other federal contracting or cloud review	Agency, contract, data and cloud service context.	Agency clauses, security attachment, required framework and revision, boundary and authorization.	Collect these records, then ask the specialist which framework applies.
HIPAA security review	Covered entity or business associate facts.	Role and agreements, ePHI flows, risk analysis and program records.	Package 07 covers a legal matter; scope a HIPAA security review with the specialist.
FTC Safeguards Rule	Business activities and which regulator has jurisdiction.	Business model, customer information, provider arrangements, existing program and regulator correspondence.	Collect these records with the current 16 CFR Part 314 text.
Utilities and operational technology	Facilities, sector, state and permits.	Applicability register, operating permissions and facility evidence.	Use the OT assessment planning library at evestigate.com/resources/ot-assessment-planning-library/.

Common terms

Term	Meaning
Custodian	A person who may hold or manage relevant information. The system owner may be someone else.
Tenant	An organization specific cloud environment. One company can have several tenants and acquired or dormant domains.
Native file	A file in its original working format. A PDF printout can omit formulas, comments, versions, metadata or embedded material.
Metadata	Information describing a record, such as dates, owner, IDs or revision details. Its meaning depends on the application and the collection method.
Log	A record of selected system activity. A log covers an event when logging was enabled, captured that event and kept it for the period in question.
Archive	A retained repository that may preserve selected content. Coverage depends on capture, indexing, policy and configuration.

© 2026 Global Digital Forensics, Inc. All rights reserved.

Term	Meaning
Backup	A recovery copy. Confirm its contents, restore capability and point in time; searching it and holding it are separate steps.
Legal hold	A preservation measure directed by counsel or an authorized process. The instruction, the technical implementation and the confirmation are separate records.
CUI and FCI	Controlled Unclassified Information and Federal Contract Information. The contracting or data owner confirms the category and its contractual basis.
ECCN and USML	An Export Control Classification Number under the EAR and the United States Munitions List under the ITAR. A specialist determines classification and jurisdiction from the facts.

Receiving the package and timing

Receiving the package

Ask the recipient to acknowledge what arrived, name any unreadable or missing files and confirm the next request. Keep their substantive review separate from the delivery receipt. A complete collection is the starting point the specialist works from for the audit, export review or test planning.

Timing and urgent matters

Agree gathering dates with the recipient based on records, access and provider availability. Those dates are project targets. Active incidents, imminent deletion, filing deadlines, litigation orders and pending transactions go to counsel or the responsible specialist immediately, outside the ordinary package schedule.

Where relevant data can live: the data source atlas

Use the atlas as an interview menu. A category is a possibility until an owner confirms the actual system, account, period and available records. Record the business content and the separate metadata and logs. Counsel and the receiving specialist set relevance, preservation, lawful authority and scope, and choose the sources each matter needs. The same entries are in Data-source-inventory.csv with columns for the owner response.

D01 Laptops and desktops

What it may hold: Local files, downloads, synced copies, browser records and user or application artifacts if retained.

Ask the owner: Which device IDs, user profiles, encryption or recovery arrangements and relevant dates exist? Is a scoped forensic collection needed?

Likely contact: IT asset owner and custodian.

Limits to confirm: A local synced folder may contain placeholders rather than all cloud content. Leave the device as it is; the inventory records its identifiers and custodian.

Sources: NI04; MS01

© 2026 Global Digital Forensics, Inc. All rights reserved.

D02 Mobile phones and tablets

What it may hold: Messages, work apps, photographs, attachments and account links subject to device or app state.

Ask the owner: Company owned or personal? Which apps and accounts were used, who can authorize collection, and what is still available?

Likely contact: Custodian, MDM owner and counsel.

Limits to confirm: Confirm which app data the MDM can reach and who can authorize collection of personal information. Deletion and encryption can limit recovery.

Sources: NI04; LG01

D03 External media and paper

What it may hold: USB or external disks, removable media, notebooks, printouts and offsite files.

Ask the owner: Which media or physical locations were used and who has custody?

Likely contact: Custodian, facilities and records manager.

Limits to confirm: A record may have left the managed network without a surviving access log. Preserve physical identifiers and custody.

Sources: NI04; NY02

D04 Email and calendars

What it may hold: Messages, attachments, drafts, calendars, tasks, shared or delegated mailboxes and groups where supported.

Ask the owner: Identify all primary, alias, legacy or shared addresses and relevant mail systems; what export includes attachments and metadata?

Likely contact: Messaging administrator and business owner.

Limits to confirm: An individual mailbox search can omit shared mailboxes, external mail, deleted or inactive users and cloud linked documents.

Sources: MS01; GO01

D05 OneDrive and personal work storage

What it may hold: User owned work files, supported versions, sharing links and retained content.

Ask the owner: Which exact user or site URLs exist, including deleted or unlicensed accounts? What holds, licenses and deletion schedules apply?

Likely contact: SharePoint or OneDrive administrator.

Limits to confirm: Request recycle bin contents directly, alongside the normal eDiscovery search. Check the current archive terms for unlicensed accounts and the date each account will be removed.

Sources: MS03; MS05

© 2026 Global Digital Forensics, Inc. All rights reserved.

D06 SharePoint and Teams files

What it may hold: Team sites, libraries, lists and separate channel sites where used.

Ask the owner: Which site or library and private or shared channel locations are relevant? Where do linked files actually live?

Likely contact: Site and collaboration administrators.

Limits to confirm: Collect channel files, lists, versions and linked targets alongside the mailbox messages.

Sources: MS01; MS02; MS05

D07 Teams messages and meetings

What it may hold: Searchable compliance records, chats or posts, recordings or transcripts and meeting artifacts where supported.

Ask the owner: Which chat, channel or meeting types, policies, organizers and storage locations apply? What known content exclusions exist?

Likely contact: Teams, messaging and site administrators.

Limits to confirm: eDiscovery uses compliance records rather than the live Teams database. Files and recordings may require different locations. Features and channel behavior change.

Sources: MS02

D08 Google Gmail and calendars

What it may hold: Messages, attachments and calendar content supported by the actual Workspace or Vault setup.

Ask the owner: Which accounts or domains, delegated or group mail, licenses and retention or holds existed for the relevant period?

Likely contact: Workspace or Vault administrator.

Limits to confirm: Vault holds what its licenses and configured policies cover, so confirm both. Deleting users or required licenses can destroy availability.

Sources: GO01

D09 Google Drive and shared drives

What it may hold: Owned or shared files, shared drive material and versions or exports as supported.

Ask the owner: Who owns each file or shared drive, including external owners? Which search and export settings were used?

Likely contact: Drive or Vault administrator and document owners.

Limits to confirm: Request the external target and the historical versions behind any shortcut or user search. Confirm the export scope with the provider.

Sources: GO01

© 2026 Global Digital Forensics, Inc. All rights reserved.

D10 Google Chat Meet and Voice

What it may hold: Supported messages, meeting artifacts, recordings and Voice records if used and retained.

Ask the owner: Which services, history settings, organizers and licenses were in use?

Likely contact: Workspace or Vault and communications administrators.

Limits to confirm: Confirm coverage service by service, including which calls were recorded.

Sources: GO01; GO02

D11 Slack and shared workspaces

What it may hold: Channels, direct messages, files and preserved edits or deletions where the plan and tools support them.

Ask the owner: Which workspaces, plan, export authority, apps, retention and Slack Connect parties apply?

Likely contact: Workspace or org owner and counsel.

Limits to confirm: Exports or API access are plan or permission dependent. External organizations can control relevant content and retention.

Sources: SL01; SL02

D12 Other messaging and meeting systems

What it may hold: Business use of texts, WhatsApp, Signal, Zoom, chat, voice or other collaboration tools.

Ask the owner: Ask each custodian which actual accounts or apps were used, whether history or recording existed and who controls it.

Likely contact: Custodian, communications owner and counsel.

Limits to confirm: Encryption, device state, disappearing settings, contracts and legal authority differ.

Sources: NI04; LG01

D13 Identity and access platforms

What it may hold: Account, sign in, role, group, authentication and administrator records if logged.

Ask the owner: Which tenant or account IDs, role assignments, event sources and dates can be exported?

Likely contact: Identity administrator.

Limits to confirm: Pair sign in records with device and session records, which are where the examiner looks to attribute later actions. Log availability depends on actual coverage and retention.

Sources: NI04; MS04; GO02

D14 Security monitoring and endpoints

What it may hold: SIEM, EDR, DLP, alerts, case records and file or device activity if collected.

Ask the owner: Which endpoint agents, policies, sensors, fields, exclusions and retained periods cover the relevant event?

Likely contact: SOC, endpoint owner and providers.

© 2026 Global Digital Forensics, Inc. All rights reserved.

Limits to confirm: An alert is a lead requiring interpretation. Record where agents had visibility and for which periods.

Sources: NI04; MS04

D15 Network and remote access

What it may hold: VPN, firewall, proxy, DNS, wireless and remote support records if enabled.

Ask the owner: Which identity, device or IP mappings and times are available; what NAT, clock or shared account issues exist?

Likely contact: Network team and remote access provider.

Limits to confirm: Pair network records with endpoint and identity records, which are where the examiner looks for file content and the person acting.

Sources: NI04

D16 Microsoft audit and export reports

What it may hold: Activity logs, query or export job records, processing errors and source counts.

Ask the owner: What exact licenses, policies, event types, role filters, earliest dates and error reports apply?

Likely contact: Purview administrator.

Limits to confirm: Content retention is separate from audit log retention. A zero result can arise from scope, indexing, permissions or filters.

Sources: MS04; MS06

D17 Google audit and export reports

What it may hold: Admin, login, Drive and other service events, job histories and errors as available.

Ask the owner: Which log type, time period, query, export mechanism and event delay apply?

Likely contact: Workspace security or Vault administrator.

Limits to confirm: Retention and delay vary by log. Preserve each activity log under its own retention setting alongside the Vault hold.

Sources: GO01; GO02

D18 Cloud infrastructure and storage

What it may hold: Virtual machines, object stores, snapshots, databases, cloud keys and management or data access logs where configured.

Ask the owner: List accounts, subscriptions, regions, services, logging settings, bucket or container IDs, lifecycle rules and providers.

Likely contact: Cloud administrator and application owners.

Limits to confirm: AWS default Event history is regional 90 day management history; it excludes data events. Enable or request data event logging for storage downloads.

© 2026 Global Digital Forensics, Inc. All rights reserved.

Sources: AW01; NI04

D19 Email journals and compliance archives

What it may hold: Journaled or ingested mail, attachments, other captured feeds and archive search histories.

Ask the owner: Which feeds, users or date ranges were captured, what failed, and does export preserve original fields and attachments?

Likely contact: Archive owner and provider.

Limits to confirm: Verify capture, deduplication and migration gaps so the archive can be compared with its source.

Sources: NI04; LG01

D20 Backups snapshots and recovery replicas

What it may hold: Point in time data, application or database copies, endpoint backups and old recovery media.

Ask the owner: Which systems or dates, catalogs, keys, overwrite dates, restore methods, cost and licensing are involved?

Likely contact: Backup administrator and provider.

Limits to confirm: Restore to an isolated environment. Ask the specialist whether an isolated restoration is justified, and confirm restorability with a test restore.

Sources: NI04; LG01

D21 Legacy systems and migrations

What it may hold: Decommissioned servers, previous tenants or domains, migration staging, historical exports and transfer logs.

Ask the owner: What moved, when, from or to which system, with what reconciliation and known exclusions?

Likely contact: Former owners, integration or migration team and provider.

Limits to confirm: A current system report can omit earlier data; old schemas, software or keys may be needed.

Sources: NI04; LG01

D22 CRM and sales systems

What it may hold: Customer or contact records, opportunities, activities, attachments, quotes and field histories where supported.

Ask the owner: Which objects, IDs, fields, audit or history features, attachments and integrations cover the dispute?

Likely contact: Sales operations and CRM administrator.

Limits to confirm: Standard reports may omit history, deleted records, relationships or linked files. Confirm vendor/version.

Sources: NI04; LG01

© 2026 Global Digital Forensics, Inc. All rights reserved.

D23 ERP accounting and procurement

What it may hold: Orders, invoices, payments, approvals, vendor or customer changes and journals where retained.

Ask the owner: Which transaction IDs, attachments, effective or posting dates, approval records and audit histories are needed?

Likely contact: Finance, procurement and application owner.

Limits to confirm: Collect the approval, delivery, adjustment and bank detail change records with each invoice.

Sources: NI04; LG01

D24 Contracts and electronic signatures

What it may hold: Negotiation files, clause versions, signature envelopes, completion certificates and recipient events where available.

Ask the owner: Which CLM or electronic signature service, envelope or agreement IDs, history or certificates and linked exhibits exist?

Likely contact: Legal operations, contracting and signing service administrator.

Limits to confirm: A signature certificate is one part of the record; collect the identity checks and negotiation history with it.

Sources: DS01; LG01

D25 Document management and deal rooms

What it may hold: Matter or project files, version chains, comments, permissions, workspace activity and external shares where supported.

Ask the owner: Which workspaces, version policies, exports and external party copies should the specialist consider?

Likely contact: Records or legal operations and workspace owner.

Limits to confirm: Current document download can omit earlier drafts, annotations or workspace audit history.

Sources: NI04; LG01

D26 Tickets project and engineering tools

What it may hold: Requests, task comments, approvals, attachments, release or change records, code and designs.

Ask the owner: Which project or repository IDs, branches, issue types, revisions and external integrations contain relevant work?

Likely contact: Engineering, service desk and project owners.

Limits to confirm: Export relationships and linked artifacts may require separate requests.

Sources: NI04; EA01; IT01

© 2026 Global Digital Forensics, Inc. All rights reserved.

D27 HR payroll and offboarding

What it may hold: Employment dates, role or device assignments, access change requests, separation and reimbursement records.

Ask the owner: Which relevant dates, devices, accounts and policy acknowledgments can be supplied lawfully?

Likely contact: HR, payroll, IT and counsel.

Limits to confirm: Restrict personnel and unrelated personal data. Offboarding can trigger deletion, token changes or wiping; coordinate preservation with counsel and security.

Sources: LG01; NI04

D28 Legal practice management

What it may hold: Matter metadata, documents, notes, billing, trust or accounting entries, communications, tasks and portals where used.

Ask the owner: Which modules, linked storage, client portal and separate exports are relevant?

Likely contact: Firm administrator, legal operations and provider.

Limits to confirm: Clio matter list export contains matter form data; other subtabs may be needed. Export each subtab the matter needs and keep privileged material segregated.

Sources: CL01; CL02

D29 EHR or EMR clinical record

What it may hold: Visits, notes, orders, results, medication records, amendments, addenda and signed or unsigned status as stored.

Ask the owner: Which systems, patient or encounter IDs, modules, authors, date types and export formats hold the relevant episodes?

Likely contact: Health information management and clinical application owner.

Limits to confirm: Confirm the vendor and site. A printed chart may omit audit data, versions, attachments or separate departmental systems.

Sources: HE01; HE03; HE06

D30 Clinical audit and provenance

What it may hold: Audit events, accesses, amendments, signatures, proxy activity and emergency overrides if recorded.

Ask the owner: Which events or fields, identifiers, clock settings, retention and reports exist? Ask for a legend and known gaps.

Likely contact: Clinical security or application owner and vendor.

Limits to confirm: Certification guidance describes capabilities; confirm the fields, events and retention in this deployment.

Sources: HE01 164.312(b); HE06

© 2026 Global Digital Forensics, Inc. All rights reserved.

D31 Imaging laboratory and pharmacy

What it may hold: PACS or RIS images or reports, laboratory or pathology systems, medication and administration records if used.

Ask the owner: Which separate systems, identifiers, original files, result revisions and interfaces relate to the episode?

Likely contact: Radiology, laboratory, pharmacy and department IT.

Limits to confirm: Confirm with each department which events and files exist and what the EHR export includes.

Sources: HE01; NI04

D32 Patient portals exchanges and telehealth

What it may hold: Portal messages, upload or download records, referrals, health information exchange traffic and telehealth artifacts where retained.

Ask the owner: Which platform, patient or account IDs, sending or receiving organizations and interface messages are relevant?

Likely contact: Portal, HIE or telehealth owner and privacy lead.

Limits to confirm: Read account activity with the proxy and import records, which are where the examiner looks for who acted.

Sources: HE01; HE03; HE06

D33 Practice management billing and claims

What it may hold: Scheduling, check in, referrals, coding, authorizations, claims or remittances and adjustments if used.

Ask the owner: Which clinical or financial IDs join the records and what does the billing export omit?

Likely contact: Practice administrator, billing and payer or clearinghouse contact.

Limits to confirm: Billing, clinical and legal records can differ. Pair charge codes with the clinical records, which are where the examiner looks for the care delivered.

Sources: HE01; HE03; NI04

D34 Facilities and physical systems

What it may hold: Badge or visitor events, CCTV, building controls and vehicle or location records if operated and retained.

Ask the owner: Which camera, door or location IDs, overwrite times, clocks and system owners relate to the matter?

Likely contact: Facilities, security, fleet and counsel.

Limits to confirm: Confirm privacy and authority, preserve the time context, and pair badge events with video or visitor records, which are where the examiner looks for who entered.

Sources: NI04; LG01

© 2026 Global Digital Forensics, Inc. All rights reserved.

D35 Third parties insurers and outside professionals

What it may hold: Vendors, brokers, advisers, counterparties, outsourced IT and external archives may hold distinct records.

Ask the owner: Who owns or controls each copy and what request, consent or order or contract right is needed?

Likely contact: Counsel, business owner and provider.

Limits to confirm: Obtain third party data through a lawful request agreed with counsel. Coordinate lawful requests and restrictions.

Sources: LG01 Rules 34 and 45; HE03

D36 Automations AI tools and integration copies

What it may hold: Prompts or outputs, connected data, workflow histories, generated summaries and intermediate files where actually retained.

Ask the owner: Which tools were actually used, with which organization or personal accounts, connectors and retention settings?

Likely contact: Application owner, users and provider.

Limits to confirm: Preserve the original record and its provenance alongside any generated text, and verify the feature and export coverage.

Sources: MS01; GO01; NI04

Package 01: NYDFS Part 500

Assemble the entity facts and existing cybersecurity records that a Part 500 auditor, examiner or consultant will ask for first. Who uses it: Compliance teams, CISOs, project coordinators, business contacts and internal IT. Scope: 23 NYCRR Part 500 for an entity operating, or required to operate, under a license, registration or similar authorization from the New York Department of Financial Services. Other DFS examination areas, such as financial condition or anti money laundering, need their own preparation.

Before you gather

Start with the DFS license or other authorization and the legal entity. Ask counsel to record the basis for coverage under 500.1(e) and any exemption, starting from the license itself. A limited exemption under 500.19(a) removes specified duties, not the whole regulation. Gather the employee and independent contractor counts, revenue, year end assets and affiliate information so the specialist can apply the definitions, including the Class A tests in 500.1(d).

Know the clocks before you need them. A covered entity must notify the superintendent as promptly as possible and no later than 72 hours after determining that a cybersecurity incident has occurred (500.17(a)(1)). An extortion payment requires notice within 24 hours of the payment and a written explanation within 30 days (500.17(c)). Each year by April 15 the entity files a certification of material compliance or an acknowledgment of noncompliance, signed by its highest ranking executive and its CISO (500.17(b)). Since November 1, 2025, multifactor authentication must be used for any individual accessing any information system of a covered entity, with a narrower list for entities that qualify for a limited exemption under 500.19(a) (500.12(a)).

© 2026 Global Digital Forensics, Inc. All rights reserved.

Keep the activities distinct. A Class A independent audit under 500.2(c), the annual filing, a DFS examination and a readiness review each have a different scope and different evidence. Read the adopted amendment for the rule text and the DFS reading copy for navigation; the September 10, 2026 DFS letter on risk assessments is guidance. Ask the receiving professional to reconcile the current rule with the examination request before the final evidence list is fixed.

Using the worksheets

Give each request to its suggested owner and record each response, including any gap, in Gathering-checklist.csv. Point to records held in the approved evidence location, where passwords, real patient data and controlled technical information stay.

NYDFS Part 500: records to find

Each request below matches a row in Gathering-checklist.csv. Record the response, status and record IDs there.

DFS-R01 Entity and authorization file

Ask: Legal or compliance.

Gather: Legal name, DFS license or registration numbers, authorizations, affiliate chart, covered activities and a copy of any examination letter.

Where to ask: Corporate records, licensing team, DFS correspondence.

Why it matters: The recipient must identify the actual entity and engagement scope.

If missing or uncertain: Record who holds each authorization or request.

Sources: DFS01 500.1(e); DFS04

DFS-R02 Exemption and Class A support

Ask: Finance, HR and compliance.

Gather: Prior determinations and notices; employee or contractor counts and methods; relevant multiyear revenue and year end assets; affiliates and shared systems or programs; changes to eligibility.

Where to ask: Finance reports, HR roster, corporate chart, submission receipts.

Why it matters: Supports professional decisions under 500.1(d) and 500.19 without asking the coordinator to classify the entity.

If missing or uncertain: Use Pending determination; obtain missing affiliate figures or dated receipt. Confirm that any past exemption still applies for the current period.

Sources: DFS01 500.1(d), 500.19; DFS03

DFS-R03 Prior filings and regulator requests

Ask: Compliance.

© 2026 Global Digital Forensics, Inc. All rights reserved.

Gather: Prior calendar year certification or acknowledgment, supporting file, signatory authority, exemption notices, regulator correspondence and unresolved examination items.

Where to ask: Compliance repository and DFS portal receipts.

Why it matters: The April 15 certification or acknowledgment is signed by the highest ranking executive and the CISO (500.17(b)); these records connect the period to actual filings.

If missing or uncertain: List absent years, filing confirmations and signatory gaps. No one should sign a certification from checklist completion.

Sources: DFS01 500.17(b), 500.19; DFS03

DFS-R04 Program policies and approvals

Ask: CISO or security lead.

Gather: Current and period relevant cybersecurity policies, operating procedures, approval records, policy revision history and any affiliate program adoption agreement.

Where to ask: Policy library, board portal, service agreements.

Why it matters: Shows what the organization adopted and when; procedures and implementation records are separate from policy statements.

If missing or uncertain: Supply draft or superseded documents with their status stated. Ask who holds the actual approval record.

Sources: DFS01 500.2, 500.3, 500.4; DFS04

DFS-R05 Governance and staffing records

Ask: Executive sponsor and HR.

Gather: CISO appointment or service arrangement, responsible management, governing body reports, relevant minutes, budget or resource decisions and qualifications or training of security staff.

Where to ask: Board records, HR, vendor agreements.

Why it matters: Helps the auditor plan interviews and understand responsibility and oversight.

If missing or uncertain: Provide names and dates, and mark each report as located, being located or not prepared.

Sources: DFS01 500.4, 500.10

DFS-R06 Risk assessment history

Ask: Risk lead.

Gather: Current and prior assessments, methodology, scoped systems or data, business inputs, threats, vulnerabilities, control evidence, accepted risks and resulting action plans.

Where to ask: Risk register and assessment repository.

Why it matters: Shows why risks and controls were selected and whether changes were considered. The 2026 letter emphasizes traceable, business specific work.

© 2026 Global Digital Forensics, Inc. All rights reserved.

If missing or uncertain: Identify omitted systems, missing rationale or updates awaiting approval as questions for the specialist.

Sources: DFS01 500.9; DFS05

DFS-R07 System and data inventory

Ask: IT and business system owners.

Gather: Hardware, software, cloud or OT inventory where relevant, owners, locations, sensitivity, support dates, recovery objectives, network or data flow diagrams and inventory reconciliation records.

Where to ask: Asset register, network team, procurement and provider portals.

Why it matters: Supports the scope of the review, including specialized systems and third party dependencies.

If missing or uncertain: Use the source atlas and owner interviews to identify unconfirmed repositories.

Sources: DFS01 500.1(i), 500.13

DFS-R08 Access and authentication records

Ask: Identity administrator.

Gather: Account and privileged account lists, review or approval records, joiner or leaver examples, MFA configurations and coverage or exclusions, remote access settings and written compensating control approvals.

Where to ask: Identity, HR, application administrators and provider.

Why it matters: Since November 1, 2025, 500.12(a) requires multifactor authentication for any individual accessing any information system; these records let the specialist compare approved access with actual coverage.

If missing or uncertain: Describe unsupported systems and missing review periods, and record an MFA exception as approved when its written approval is attached.

Sources: DFS01 500.7, 500.12

DFS-R09 Existing vulnerability and penetration test records

Ask: Security lead and service provider.

Gather: Scope, qualifications, dated internal or external penetration test reports, scan or manual review coverage, risk based schedule, significant change records, remediation tickets and existing retest results.

Where to ask: Security provider and ticket system.

Why it matters: Prepares the 500.5 review. Obtain existing work first; scanners, penetration testing and an audit are different activities.

If missing or uncertain: Record absent scope or results and request professional planning. Written authorization, safe scope and third party permissions precede any new test.

Sources: DFS01 500.5; NI05

DFS-R10 Logs and reconstruction examples

Ask: Security operations and finance systems.

© 2026 Global Digital Forensics, Inc. All rights reserved.

Gather: Logging policy, inventory, actual earliest or latest retained dates, protected storage, alert review records, and examples of reconstructing a material financial transaction and a relevant cyber event.

Where to ask: SIEM, financial application owner, archive and provider.

Why it matters: 500.6 distinguishes transaction records from cyber audit trails. Show actual coverage with the earliest and latest retained records.

If missing or uncertain: Identify missing systems or time periods and whether the source ever logged the activity. Supply records as they exist today.

Sources: DFS02 500.6; DFS01 500.14

DFS-R11 Application and supplier records

Ask: Application owners and procurement.

Gather: Application security procedures or reviews, change records, third party inventory, risk based due diligence, security clauses, incident notice terms and reassessments.

Where to ask: Development, procurement, vendor management and contracts.

Why it matters: Connects internal and external services to the entity scope and evidence responsibilities.

If missing or uncertain: Request the actual contract and shared responsibility records; a vendor certificate alone is incomplete.

Sources: DFS01 500.8, 500.11

DFS-R12 Encryption and disposal records

Ask: IT and records management.

Gather: Data inventory, encryption coverage or key management descriptions, exceptions and approvals, disposal policy, retention schedule and disposal records with preservation overrides.

Where to ask: Storage, application owners, records team.

Why it matters: Lets the specialist trace protection and lifecycle decisions to the relevant information.

If missing or uncertain: Describe uncertainty about keys, backups or disposal without supplying secrets. Ask counsel about retention conflicts.

Sources: DFS01 500.13, 500.15

DFS-R13 Monitoring and training records

Ask: Security operations and HR.

Gather: Risk based monitoring coverage, detection and filtering descriptions, training content or attendance and social engineering exercises if conducted; Class A EDR or centralized logging records if potentially relevant.

Where to ask: SOC, learning platform and providers.

Why it matters: Supplies actual operational records for monitoring or training and conditional Class A review.

If missing or uncertain: List the dates, personnel and systems each record covers so the specialist can judge relevance.

© 2026 Global Digital Forensics, Inc. All rights reserved.

Sources: DFS01 500.14

DFS-R14 Response and recovery records

Ask: Continuity lead and IT.

Gather: Incident response and business continuity or disaster recovery plans; staff roles or training; offsite backup scope or protection; existing annual exercises and critical data or system restoration results; after action updates.

Where to ask: Continuity system, backup team, providers.

Why it matters: Supports review of prepared plans, staff participation and actual restoration evidence.

If missing or uncertain: Document an untested dependency as a question. Supply any restore exercise records alongside backup job reports.

Sources: DFS01 500.16

DFS-R15 Incident and notice chronology

Ask: Counsel and incident lead.

Gather: Incident inventory, determination times, decision records, third party notices, DFS submissions or updates and extortion payment records if any, kept in a restricted workspace.

Where to ask: Incident case files, counsel and compliance.

Why it matters: DFS notice is due no later than 72 hours after determining a cybersecurity incident occurred and within 24 hours of an extortion payment (500.17(a)(1) and (c)); these facts set those clocks.

If missing or uncertain: Escalate an active incident immediately. Record unknown times, escalate now, and set each clock from its own triggering event.

Sources: DFS01 500.1(g), 500.17; DFS03

DFS-R16 Prior assurance and open actions

Ask: Internal audit and project lead.

Gather: Prior independent audit reports if applicable, scope and independence records, management responses, open actions, assigned owners, target dates and existing verification records.

Where to ask: Audit or risk repository.

Why it matters: Lets the recipient see earlier work, limitations and unresolved matters without implying closure.

If missing or uncertain: Track missing evidence separately from a proposed corrective action and from accepted verification.

Sources: DFS01 500.2(c), 500.17(b)

NYDFS Part 500: questions for IT and system owners

A useful answer names the actual system, period, supporting record and limits. Where someone else holds the answer, record who can give it. The same questions are in IT-and-owner-questions.csv.

© 2026 Global Digital Forensics, Inc. All rights reserved.

No.	Question	Suggested responder	Supporting record
1	Which legal entity and DFS authorization does the request concern?	Legal or compliance	Attach authorization and examination request or record who has them.
2	Which period, systems and affiliates does the receiving professional expect to review?	Engagement sponsor and auditor	Return a marked diagram and entity list.
3	Which MFA routes, privileged accounts and older applications are outside the normal configuration?	Identity and application owners	Provide dated coverage and exception records, with no credentials.
4	What did the last internal and external penetration tests actually cover?	Security lead	Return scope, dates, reports and exclusions.
5	How did the risk assessment affect decisions about each critical service and common provider?	Risk and service owners	Link risk entries, decisions, control records and action owners.
6	Which logs can you still retrieve for the review period?	Security operations	List each source, earliest or latest dates, gaps and relevant retention policy.
7	What evidence shows a critical system was restored and used successfully?	Recovery owner	Supply actual exercise records with limitations.
8	Who can securely supply missing records and approve disclosure to the recipient?	Project sponsor	Provide a responsibility list and approved transfer route.

NYDFS Part 500: decisions and handoff

These decisions belong to counsel or the receiving specialist. Each stays open until its owner records a decision. Add questions specific to the client and a responsible person in Open-questions.csv.

Preparing the handoff

The handoff is ready when the engagement sponsor has confirmed the entity and period, with any exemption or Class A question marked as pending; every request has a response or a named gap with a period and a next owner; incident and testing material is indexed without travelling as an ordinary email attachment; and the specialist has the actual examination request from which to set the final criteria.

Use Record-index.csv for one row per file or defined record set, and follow the walkthrough in the library for custody, restricted records and receipt.

ID	Decision	Decision owner	Information needed	Closed by
DFS-Q01	Does this legal entity qualify as covered, exempt or Class A for the period?	Counsel and receiving Part 500 specialist	Authorizations, affiliate facts, figures and prior notices	Written scope determination for the period.

© 2026 Global Digital Forensics, Inc. All rights reserved.

ID	Decision	Decision owner	Information needed	Closed by
DFS-Q02	Is the planned engagement a DFS examination, Class A independent audit, internal review or readiness consultation?	Sponsor and receiving auditor	Examination letter, charter and intended deliverables	Agreed scope, independence, criteria and recipient responsibilities.

Sources: DFS01, DFS04, DFS03, DFS05, NI05, DFS02, DFS07

Package 02: New York private information

Find where New York residents' private information is held and assemble the safeguard and incident records a privacy or cybersecurity specialist will review. Who uses it: Owners, counsel, privacy and risk managers, office administrators and client IT. Scope: New York General Business Law 899-aa (breach notice) and 899-bb (safeguards), with a separate branch for state entities under State Technology Law 208 and for sector rules such as the DFS and hospital regulations.

Before you gather

Inventory actual fields, not labels. PII is a useful working term, but private information under GBL 899-aa has its own definition, and DFS nonpublic information and HIPAA protected health information have different scopes. The current 899-aa definition reaches beyond Social Security and card numbers to biometric information, online account credentials, medical information and health insurance information, so a checklist built only on identification numbers will miss records.

Record the times that start the notice clocks. Notice to affected New York residents must be made in the most expedient time possible and without unreasonable delay, and within 30 days after the breach has been discovered, subject to the law enforcement provision (GBL 899-aa(2), as revised March 28, 2025). A business that maintains data on behalf of its owner must notify the owner or licensee immediately, and within 30 days following discovery (899-aa(3)). When the business is a DFS covered entity, notice also goes to the Department of Financial Services under 23 NYCRR 500.17, without delaying notice to residents (899-aa(8)). These clocks are separate from the DFS incident and payment clocks in package 01.

Gather the safeguard records, not only the policies. GBL 899-bb requires reasonable administrative, technical and physical safeguards. A business that is subject to, and in compliance with, Gramm Leach Bliley regulations, HIPAA and HITECH, 23 NYCRR Part 500 or similar data security rules is treated as compliant, so collect the records that show that compliance. A small business meets the duty with safeguards appropriate for its size and complexity (899-bb(2)(c)).

Keep the state entity branch separate. State entities follow State Technology Law 208, with its own definitions, deadlines and recipients. Hospitals, schools, employers, financial firms and government bodies may need an added module.

Using the worksheets

Give each request to its suggested owner and record each response, including any gap, in Gathering-checklist.csv. Point to records held in the approved evidence location, where passwords, real patient data and controlled technical information stay.

© 2026 Global Digital Forensics, Inc. All rights reserved.

New York private information: records to find

Each request below matches a row in Gathering-checklist.csv. Record the response, status and record IDs there.

NY-R01 Organization and legal context

Ask: Legal or business owner.

Gather: Legal entity, ownership or government status, business activities, resident populations and contracts or regulator requests.

Where to ask: Corporate files and business sponsor.

Why it matters: Routes the facts to the right law and sector.

If missing or uncertain: Ask counsel which regime applies; keep the branch unresolved.

Sources: NY01 2; NY02 2; NY03 1(c), 10

NY-R02 Data field and combination inventory

Ask: Business process owners.

Gather: Field names and masked samples; people concerned; purpose; volumes; residence facts; data combinations; encryption and key exposure facts.

Where to ask: HR, payroll, customer, financial and medical systems.

Why it matters: Supports classification without collecting real identifiers in the checklist.

If missing or uncertain: Name the owner who can supply a schema or masked example; no guessed counts.

Sources: NY01 1; NY02 1; DFS01 500.1(k)

NY-R03 Information journey

Ask: IT and business owners.

Gather: Where information is collected, used, shared, exported, archived, backed up and disposed; devices, tenants, integrations, paper copies and recipient organizations.

Where to ask: Data source atlas, purchasing and application diagrams.

Why it matters: Reveals extra copies and processors that a device list misses.

If missing or uncertain: Mark each unconfirmed location as a candidate until its owner confirms it.

Sources: NY02 2(b)

NY-R04 Responsibility and risk records

Ask: Management and security lead.

Gather: Program coordinator, risk assessments, decisions, policy set and business changes since last review.

Where to ask: Policy and risk systems.

Why it matters: Organizes administrative safeguard records for the recipient.

© 2026 Global Digital Forensics, Inc. All rights reserved.

If missing or uncertain: Name the person who may have records so the specialist can follow up.

Sources: NY02 2(b)(ii)(A)

NY-R05 Personnel and supplier safeguards

Ask: HR and procurement.

Gather: Training records, confidentiality or access procedures, provider list, selection reviews, contracts requiring safeguards and change or reassessment records.

Where to ask: HR, procurement, provider agreements.

Why it matters: Supplies the actual administrative and provider arrangements.

If missing or uncertain: Request actual signed terms and records for the period rather than a sales brochure.

Sources: NY02 2(b)(ii)(A)

NY-R06 Technical protection records

Ask: IT and service providers.

Gather: Access or MFA scope, secure configurations, patch or change history, monitoring coverage, existing test reports and response procedures for the relevant data flows.

Where to ask: Identity, endpoint, application and provider records.

Why it matters: Lets the consultant assess existing technical safeguards.

If missing or uncertain: Request a scoped explanation of missing or outsourced records; any new testing runs under written authorization.

Sources: NY02 2(b)(ii)(B)

NY-R07 Physical records and disposal

Ask: Facilities and records manager.

Gather: Storage, transport and visitor procedures; cabinet or media controls; retention schedules; destruction certificates and holds that prevent disposal.

Where to ask: Facilities, offsite storage and media vendor.

Why it matters: Includes paper, portable media and disposal, not only cloud security.

If missing or uncertain: Identify storage sites and providers not yet contacted.

Sources: NY02 2(b)(ii)(C)

NY-R08 Incident facts and chronology

Ask: Counsel and incident owner.

Gather: Discovery, detection or determination timestamps, system events, affected fields, persons or residences, access versus acquisition evidence, encryption or key facts and provider notice.

Where to ask: Restricted incident file.

© 2026 Global Digital Forensics, Inc. All rights reserved.

Why it matters: GBL 899-aa(2) requires notice to affected residents within 30 days after discovery; accurate times let counsel apply that clock.

If missing or uncertain: Escalate live matters; label suspected facts and dates as unconfirmed.

Sources: NY01 1(c), 2, 3; NY03

NY-R09 Notification and decision file

Ask: Counsel and compliance.

Gather: Notice decisions and basis, templates, dates or recipients, agency receipts, any law enforcement delay determination and updates.

Where to ask: Counsel and incident correspondence.

Why it matters: Allows review of actual actions and applicable branches.

If missing or uncertain: Keep legal advice segregated; provide counsel approved factual chronology and privilege handling instructions.

Sources: NY01 2, 4, 7, 8, 9

NY-R10 Regulated entity or size support

Ask: Finance and legal.

Gather: Other applicable security regimes, actual compliance records relied on, small business facts and the prior determination.

Where to ask: Legal, finance and other assessment files.

Why it matters: Supports the 899-bb provision for regulated entities with the records the specialist reviews for compliance.

If missing or uncertain: Send the available facts and the proposed basis to the specialist.

Sources: NY02 1 and 2(b)-(c)

NY-R11 Government and sector routing

Ask: Legal or privacy lead.

Gather: State or local status, governmental policy, actual healthcare, school or financial licenses, contractual requirements and regulator orders.

Where to ask: Legal records and sector owner.

Why it matters: Identifies which specialist should add a tailored module. Read the hospital regulation itself, not only the guidance.

If missing or uncertain: Obtain the current text of 10 NYCRR 405.46 before building a hospital requirement list.

Sources: NY03; NY04; HE01; DFS01

NY-R12 Gaps and transmittal

Ask: Coordinator.

© 2026 Global Digital Forensics, Inc. All rights reserved.

Gather: Completed source inventory, request responses, periods not covered, access restrictions and named follow up owners.

Where to ask: Coordinator and receiving specialist.

Why it matters: Gives the specialist a clear handoff.

If missing or uncertain: Keep Unknown or Partially received visible; ask recipient which gap is first priority.

Sources: NY02

New York private information: questions for IT and system owners

A useful answer names the actual system, period, supporting record and limits. Where someone else holds the answer, record who can give it. The same questions are in IT-and-owner-questions.csv.

No.	Question	Suggested responder	Supporting record
1	What exact information fields and combinations do you hold about New York residents?	Client IT or system owner	Schema and masked examples, including credentials, medical and health insurance fields.
2	Which outside parties hold the same information or additional copies?	Client IT or system owner	Provider list, contracts, tenants, exports and return or deletion terms.
3	What can you say about encryption and who could obtain the decryption keys?	Client IT or system owner	Configuration description and responsible owner, with keys kept in their secure store.
4	Which safeguards were in operation during the period, rather than added later?	Client IT or system owner	Dated settings, reports, tickets and change history.
5	Are accounts, archives, paper stores or backups outside the main system inventory?	Client IT or system owner	One inventory row for each actual location and owner.
6	If an incident is relevant, what happened, when was each fact learned and what is still uncertain?	Client IT or system owner	Counsel approved chronology with evidence pointers.
7	What records were already supplied to a regulator, insurer or prior assessor?	Client IT or system owner	Copies, scope and receipts subject to authorized disclosure.
8	Which people can explain a missing record or technical limitation?	Client IT or system owner	Contact roster and next action per gap.

New York private information: decisions and handoff

These decisions belong to counsel or the receiving specialist. Each stays open until its owner records a decision. Add questions specific to the client and a responsible person in Open-questions.csv.

© 2026 Global Digital Forensics, Inc. All rights reserved.

Preparing the handoff

The handoff is ready when the data map uses actual fields and repository owners rather than a generic PII label; the government, DFS and healthcare branches stay separate; an active incident has gone to counsel outside the ordinary schedule; and the specialist has a record index, masked examples and a list of what is still missing.

Use Record-index.csv for one row per file or defined record set, and follow the walkthrough in the library for custody, restricted records and receipt.

ID	Decision	Decision owner	Information needed	Closed by
NY-Q01	Which statutory definition and organizational branch apply?	Counsel and privacy specialist	Entity status, fields, residents, sector licenses and contracts	Written scope and definitions; state entities follow State Technology Law 208 separately.
NY-Q02	Which additional sector or other state modules are necessary?	Counsel and specialist	Business locations, customers, patients, students, contracts and regulator orders	A named list of the additional state or sector modules needed.

Sources: NY01, NY02, NY03, DFS01, NY04, HE01, DFS07

Package 03: Defense contractor cybersecurity

Gather the contract, information flow and security records a CMMC or NIST SP 800-171 specialist needs to scope the work. Who uses it: Contract managers, small business owners, CISOs, project coordinators and IT providers. Scope: Safeguarding of Federal Contract Information and Controlled Unclassified Information under FAR 52.204-21 and DFARS 252.204-7012, and preparation for CMMC. Scoring, assessment and certification stay with the specialist and the authorized assessor.

Before you gather

Read the contract first. The Department of War CIO memorandum of July 13, 2026 suspended the November 2026 CMMC Phase 2 transition. Class Deviation 2026-O0025 Revision 3 directs contracting officers to amend solicitations and contracts to match, permits Level 1 and Level 2 self assessments, keeps baseline compliance with NIST SP 800-171 Revision 2 under DFARS 252.204-7012, and prescribes the clause at DFARS 252.240-7997, NIST SP 800-171 DoD Assessment Requirements (FEB 2026). The client's own solicitation amendments and contract modifications decide what applies, so collect them.

Use the right revision. NIST has published SP 800-171 Revision 3, but the CMMC rule incorporates Revision 2 (32 CFR 170.2), and Revision 2 is the baseline the deviation keeps. Map evidence to the Revision 2 requirements and the matching SP 800-171A assessment procedures unless the contract says otherwise.

Separate the information types. FCI, CUI, export controlled information and classified information each rest on a different basis. Ask the government or prime contractor owner for the CUI categories, markings and handling instructions, which set the level and the boundary.

Plan where artifacts will live. For a Level 2 certification assessment or a Level 3 assessment, the organization hashes its artifact files with a NIST approved hashing algorithm and keeps them for six years from the CMMC Status Date (32 CFR 170.17 and 170.18). Keep sensitive records in the agreed controlled environment and let

© 2026 Global Digital Forensics, Inc. All rights reserved.

the preparation index point to them.

Using the worksheets

Give each request to its suggested owner and record each response, including any gap, in Gathering-checklist.csv. Point to records held in the approved evidence location, where passwords, real patient data and controlled technical information stay.

Defense contractor cybersecurity: records to find

Each request below matches a row in Gathering-checklist.csv. Record the response, status and record IDs there.

CM-R01 Actual contract package

Ask: Contract administrator.

Gather: Solicitation, statement of work, contract, orders, incorporated clause versions, flowdowns, amendments, modifications, options and correspondence about CMMC.

Where to ask: Contract repository and prime customer.

Why it matters: Establishes the basis for specialist scoping.

If missing or uncertain: Ask prime or contract officer through authorized client channels; record unresolved interpretations.

Sources: CM04; CM05; CM06; CM07

CM-R02 Current implementation instructions

Ask: Contracts and counsel.

Gather: Current applicable deviations, written direction and modification history addressing the July 2026 suspension and any subsequent changes.

Where to ask: Contract file and official deviation index.

Why it matters: Prevents reliance on a superseded generic rollout date.

If missing or uncertain: The specialist reconciles the deviation with the actual contract before an assessment path or date is set.

Sources: CM02; CM03; CM07; CM10

CM-R03 Information types and authority

Ask: Program or data owner.

Gather: Customer provided CUI categories or markings, handling instructions, FCI description, contract data lists and export or security restrictions; masked examples where permitted.

Where to ask: Program office, contract data repository.

Why it matters: Supports the data classification and boundary discussion.

© 2026 Global Digital Forensics, Inc. All rights reserved.

If missing or uncertain: Record who can confirm the designation; the government or prime owner sets CUI designations and markings.

Sources: CM01; CM04; CM06

CM-R04 Boundary and data flow

Ask: IT architect and process owners.

Gather: Systems that create, receive, process, store, transmit or protect relevant information; tenant, site or network diagrams, users, interfaces and external transfers.

Where to ask: Architecture, process walkthrough and providers.

Why it matters: Lets the specialist define candidate in scope assets and dependencies.

If missing or uncertain: List unconfirmed paths, personal accounts and legacy systems for follow up.

Sources: CM08; CM01

CM-R05 System security plan and asset facts

Ask: Security lead.

Gather: Existing SSP and revision history; asset inventory; proposed asset categories; facilities, endpoints, identity, remote access, backups and security services.

Where to ask: Security repository and asset manager.

Why it matters: Helps the specialist evaluate actual scope and existing descriptions.

If missing or uncertain: Supply drafts as drafts. Label each control as operating, planned or unverified.

Sources: NI01; CM08

CM-R06 Providers and cloud responsibilities

Ask: Provider manager.

Gather: MSP, MSSP or CSP contracts, service boundaries, customer responsibility matrices, subcontractor access and existing authorization or equivalency evidence requested by the specialist.

Where to ask: Procurement, cloud providers and contract files.

Why it matters: Clarifies inherited versus client performed work and evidence access.

If missing or uncertain: Request the client's configured service boundary alongside any sales claim or FedRAMP listing. Ask for exact service or scope and responsibility records.

Sources: CM05; CM08

CM-R07 Access and identity records

Ask: IT administrator.

Gather: Authorized user or device lists, role approvals, remote, privileged or MFA settings, employee lifecycle records and prior reviews.

Where to ask: Identity, HR, endpoint and application records.

© 2026 Global Digital Forensics, Inc. All rights reserved.

Why it matters: Enables evidence planning for access and identification or authentication topics.

If missing or uncertain: Provide scoped records through the approved route, with credentials kept in their secure store.

Sources: NI01 access control and identification/authentication

CM-R08 Configuration and change records

Ask: Infrastructure and development owners.

Gather: Baselines, inventory, authorized software, change approvals, configuration reviews and existing patch, vulnerability or remediation records.

Where to ask: Configuration, software and ticket systems.

Why it matters: Supports configuration, integrity and risk topics.

If missing or uncertain: Identify unsupported assets and missing historical settings as gaps.

Sources: NI01 configuration management, risk assessment and system integrity

CM-R09 Logging and incident records

Ask: Security operations.

Gather: Logging policy and actual coverage or retention, alert reviews, time synchronization, incident plans, existing exercises and reporting records when releasable.

Where to ask: SIEM, providers and incident repository.

Why it matters: Prepares audit or accountability and incident response discussions.

If missing or uncertain: Document inaccessible logs or periods; incident reports follow the incident response plan.

Sources: NI01 audit and accountability, incident response; CM05

CM-R10 Physical and personnel records

Ask: Facilities and HR.

Gather: Authorized areas, visitor or access records, personnel screening or separation processes, relevant training and responsibility records.

Where to ask: Facilities, HR and providers.

Why it matters: Includes nontechnical evidence often outside IT's custody.

If missing or uncertain: Use restricted handling for personnel data and route missing policies to their owner.

Sources: NI01 awareness, personnel security and physical protection

CM-R11 Media maintenance and transfer records

Ask: IT and operations.

Gather: Removable media rules, transfer paths, storage or disposal records, maintenance approvals and remote support restrictions.

© 2026 Global Digital Forensics, Inc. All rights reserved.

Where to ask: IT, operations, service partners.

Why it matters: Supports discussions of portable copies and service provider work.

If missing or uncertain: Identify any untracked path; specialist chooses follow up rather than assuming a control failure.

Sources: NI01 media protection and maintenance

CM-R12 Network and data protection records

Ask: Network and application owners.

Gather: Existing diagrams, boundary rules, segmented environments, communications protection, encryption or module descriptions and applicable exception decisions.

Where to ask: Network, application and cryptographic owners.

Why it matters: Lets the specialist request evidence appropriate to the actual environment.

If missing or uncertain: Supply the module and validation certificate details, with secrets kept in their secure store.

Sources: NI01 system and communications protection

CM-R13 Prior assessments and status records

Ask: Security lead and affirming official.

Gather: Existing assessment reports, scope or CMMC UID if issued, dates, SPRS records, affirmations, scoring basis and previous government findings.

Where to ask: Authorized SPRS user and assessment repository.

Why it matters: Distinguishes actual status from a readiness worksheet or marketing claim.

If missing or uncertain: State Not provided or No prior assessment reported, as appropriate. Record the status, assessment date and score exactly as issued.

Sources: CM01; CM04

CM-R14 Outstanding actions and artifacts

Ask: Project lead and security owner.

Gather: Existing POA&M, owners, dates, supporting evidence, documented constraints and prior closeout records.

Where to ask: Risk or project and assessment repository.

Why it matters: Helps plan remediation discussion; eligibility and permitted deferrals are specialist decisions.

If missing or uncertain: The specialist decides which gaps may be deferred; label proposed actions separately from implemented ones.

Sources: CM01 170.21; NI01

CM-R15 Evidence handling and collection access

Ask: Data owner and receiving specialist.

© 2026 Global Digital Forensics, Inc. All rights reserved.

Gather: Approved repository, authorized recipients, artifact retention instructions, provider cooperation, export limits, handling labels and secure review arrangements.

Where to ask: Security, legal and contract administration.

Why it matters: Keeps sensitive evidence in the controlled environment.

If missing or uncertain: Agree the route before providing CUI or detailed artifacts. If assessment hashes or retention records are required, obtain the applicable instructions.

Sources: CM01 170.17, 170.18; CM05

CM-R16 Specialized systems and field access

Ask: Operations and specialist.

Gather: OT, test equipment, restricted systems and shared services; owners, support or vendor rules, safe review options and exclusions.

Where to ask: Operations, engineering and providers.

Why it matters: Makes technical constraints visible before a proposed assessment.

If missing or uncertain: Scanning, penetration testing and physical entry each run under a written scope and permission.

Sources: CM08; NI05

Defense contractor cybersecurity: questions for IT and system owners

A useful answer names the actual system, period, supporting record and limits. Where someone else holds the answer, record who can give it. The same questions are in IT-and-owner-questions.csv.

No.	Question	Suggested responder	Supporting record
1	Which signed clauses and modifications tell us the required assessment type today?	Client IT or system owner	Contract extracts, effective dates and unresolved conflict log.
2	Where does the customer say the CUI comes from, and which category or handling instruction supports that?	Client IT or system owner	Written customer direction and a permitted masked example.
3	Can a relevant file leave the proposed enclave through email, sync, printing, support, backup or personal storage?	Client IT or system owner	A diagram and one actual workflow explanation.
4	Which security services protect the environment and who operates them?	Client IT or system owner	Provider scope and customer responsibility matrix.
5	What controls are planned rather than operating?	Client IT or system owner	Existing SSP or POA&M version and implementation dates.

© 2026 Global Digital Forensics, Inc. All rights reserved.

No.	Question	Suggested responder	Supporting record
6	What records are available for the period, and which are only current snapshots?	Client IT or system owner	An evidence period inventory with gaps.
7	Has an assessment or affirmation actually been entered into SPRS?	Client IT or system owner	Authorized export or receipt with the relevant identifier and scope.
8	What must the receiving specialist verify before scheduling work?	Client IT or system owner	Boundary, criteria or version, provider cooperation, access and secure evidence decisions.

Defense contractor cybersecurity: decisions and handoff

These decisions belong to counsel or the receiving specialist. Each stays open until its owner records a decision. Add questions specific to the client and a responsible person in Open-questions.csv.

Preparing the handoff

The handoff is ready when the actual contract package and its current amendments are indexed; the FCI and CUI questions and any boundary or provider gaps are visible; security records are grouped by subject and period with planned items labeled as planned; and the specialist has confirmed the assessment pathway, the requirement revision and the handling route before formal work starts.

Use Record-index.csv for one row per file or defined record set, and follow the walkthrough in the library for custody, restricted records and receipt.

ID	Decision	Decision owner	Information needed	Closed by
CM-Q01	What is the effect of the current suspension or deviation on this actual contract?	Contracts counsel and authorized contracting contact	Signed contract and modifications; current deviation including later changes	Written contract specific interpretation before committing to an assessment path or date.
CM-Q02	Which requirement and assessment revisions and asset boundary should the specialist use?	Receiving CMMC or NIST specialist	Contract data types, SSP, diagrams, provider services and official criteria	Agreed criterion, revision and scope.

Sources: CM04, CM05, CM06, CM07, CM02, CM03, CM10, CM01, CM08, NI01, NI05

Package 04: Export controls

Prepare the business, item, technology, transaction and access facts an export control specialist needs to determine jurisdiction, classification and the authorizations required. Who uses it: Business owners, contract teams, engineering, IT, attorneys and export coordinators. Scope: The Export Administration Regulations (EAR) and the International Traffic in Arms Regulations (ITAR), with cybersecurity and data handling questions. Sanctions, customs, nuclear exports and classified information need their own specialists.

© 2026 Global Digital Forensics, Inc. All rights reserved.

Before you gather

Start with what the business makes and does. EAR and ITAR are different regimes. List the items, software, technical information, services and transactions; the specialist determines jurisdiction and classification, including whether another agency or regime applies.

Map access as well as shipments. Electronic access, remote support, source code sharing and engineering collaboration can be exports or releases. Gather who may reach what, from where, with which permissions and under which authorization. Route questions about a person's citizenship or status to counsel through a restricted process that confirms status from the right records.

Treat earlier labels as inputs. DDTC registration, where required, sits alongside the licenses and agreements that authorize each export. A supplier's classification, an old ECCN, an ITAR clause or a cloud provider's statement is input for the specialist. Keep each classification, license, agreement and proviso with its change history.

Encryption and records follow their own rules. EAR 734.18 and ITAR 120.54 set different conditions for certain encrypted transmission and storage, so gather the encryption boundary, key custody, locations and provider access. Recordkeeping periods start from different events: EAR 762.6 keeps records five years from the latest of the listed events and bars destruction after an agency request, and ITAR 122.5 has its own rules. Collect the actual dates and holds so the specialist can set the schedule.

Using the worksheets

Give each request to its suggested owner and record each response, including any gap, in Gathering-checklist.csv. Point to records held in the approved evidence location, where passwords, real patient data and controlled technical information stay.

Export controls: records to find

Each request below matches a row in Gathering-checklist.csv. Record the response, status and record IDs there.

EX-R01 Entity activities and responsible people

Ask: Business owner.

Gather: Legal entities, sites or countries, products, manufacturing, software, research, services, brokering if relevant, customers and export responsibility contacts.

Where to ask: Corporate, engineering and sales records.

Why it matters: Defines the proposed consultation and possible regimes.

If missing or uncertain: Describe the activity and ask for jurisdiction review; no guessed classification.

Sources: EA01; IT04

EX-R02 Item and technology descriptions

Ask: Engineering or product owner.

Gather: Part, model or version list, function, performance specifications, materials, source or object code distinctions, drawings, manuals and technical data categories.

© 2026 Global Digital Forensics, Inc. All rights reserved.

Where to ask: Engineering, PLM, repositories and product documentation.

Why it matters: Provides the facts needed for a qualified jurisdiction or classification decision.

If missing or uncertain: Start with a sanitized description and arrange controlled specialist access before sharing technical data.

Sources: EA01; IT01

EX-R03 Existing jurisdiction and classifications

Ask: Export coordinator.

Gather: ECCNs, USML categories, EAR99 determinations, commodity jurisdiction or CCATS records if obtained, supplier classifications, rationale, dates and version history.

Where to ask: Export files, suppliers and counsel.

Why it matters: Shows what was actually determined and which item or version it covers.

If missing or uncertain: Record Not yet determined. Label supplier opinions separately from government determinations.

Sources: EA03; EA04; IT04

EX-R04 Transaction map

Ask: Sales and logistics.

Gather: Proposed or prior transactions, destinations, parties, intermediaries, end users, end uses, routing, reexports or retransfers and ultimate consignees.

Where to ask: CRM, ERP, shipping and project records.

Why it matters: Connects item facts to transaction specific review.

If missing or uncertain: Unknown end use or destination is a question for the specialist before release.

Sources: EA05; EA04; IT04

EX-R05 Authorizations and restrictions

Ask: Export coordinator and counsel.

Gather: Licenses, exceptions or exemptions basis, agreements, registrations where applicable, amendments, provisos, expiration dates and authorized parties/sites/data/services.

Where to ask: BIS or DDTC records and signed agreements.

Why it matters: Allows specialist comparison of actual activity with authorized scope.

If missing or uncertain: Identify the license or authorization for each activity, and record any activity still awaiting one.

Sources: IT03; IT05; EA04

EX-R06 Screening and escalation records

Ask: Compliance and sales.

© 2026 Global Digital Forensics, Inc. All rights reserved.

Gather: Screening procedure, dated results, party identifiers, red flags, end use statements, escalation and release approvals, plus screening tool scope.

Where to ask: Screening provider, compliance and sales.

Why it matters: Supports review of the actual decision at the time of transaction.

If missing or uncertain: Screen against the current restricted party lists and let the specialist confirm license needs for EAR99 items.

Sources: EA05; EA04

EX-R07 Technical information locations

Ask: Engineering and IT.

Gather: Where technical information lives: design or source repositories, email, Teams or Slack, cloud drives, PLM, ticket systems, backups, removable devices and outside partners.

Where to ask: Data source atlas, engineering and providers.

Why it matters: Exposes copies and transfers beyond the product shipment.

If missing or uncertain: Treat candidate locations as unconfirmed until an owner responds.

Sources: EA01; IT01; IT02

EX-R08 Access and support facts

Ask: IT, HR and counsel.

Gather: Actual access roles, contractor or provider organizations, work or support locations, foreign person review process, access approvals and permitted remote administration.

Where to ask: Identity, HR, vendor and access records.

Why it matters: Enables legal review of access or release risk without public disclosure of personal status.

If missing or uncertain: Keep passports and immigration records in the restricted counsel file. Counsel defines lawful, limited verification.

Sources: EA01; IT01; IT02

EX-R09 Cloud and cryptographic facts

Ask: IT architect and provider.

Gather: Services or regions, replication, backups, disaster recovery, subcontractors, admin or support access, encryption boundary, module or strength details, key custody and decryption permissions.

Where to ask: Architecture, service contracts and provider security documents.

Why it matters: Gives the specialist facts for the distinct EAR or ITAR encrypted data provisions.

If missing or uncertain: If keys, provider access or regions are unknown, obtain written technical facts from the provider.

Sources: EA01 734.18; IT02

© 2026 Global Digital Forensics, Inc. All rights reserved.

EX-R10 Technology access procedures

Ask: Export coordinator and IT.

Gather: Existing technology control plans, permission reviews, visitor or collaboration rules, travel or device processes and exception records.

Where to ask: Export, facilities, IT and engineering.

Why it matters: Supplies existing measures, with any implementation records, for specialist review.

If missing or uncertain: Label a draft or proposed measure clearly; specialist determines what the activity requires.

Sources: EA03; EA04; IT04

EX-R11 Shipment and electronic release records

Ask: Logistics and system owners.

Gather: Orders, invoices, shipment or export declarations where applicable, serial or item versions, authorizations referenced, transfer or access records and delivery acknowledgments.

Where to ask: ERP, freight forwarder, engineering and access logs.

Why it matters: Links activity, authority and recipient over time.

If missing or uncertain: Identify records controlled by another party and arrange an authorized request rather than implying possession.

Sources: EA02; IT03

EX-R12 Retention and reproducibility

Ask: Records manager and IT.

Gather: Schedules, license or transaction dates, record formats, change history, agency requests or holds, storage or access and ability to reproduce complete readable records.

Where to ask: Export archive, providers and legal holds.

Why it matters: Enables separate EAR or ITAR schedule and reproduction review.

If missing or uncertain: Keep records until the specialist sets each schedule from its own starting event.

Sources: EA02 762.6; IT03 122.5

EX-R13 Training and business change

Ask: HR and export coordinator.

Gather: Role specific training, attendance, policies, changes to product, ownership, country, personnel or providers and prior advice about those changes.

Where to ask: HR, export program and project history.

Why it matters: Helps the specialist assess whether old decisions still fit current facts.

© 2026 Global Digital Forensics, Inc. All rights reserved.

If missing or uncertain: Record the change and date so the specialist can confirm the determination for the new version or end use.

Sources: EA03; IT04

EX-R14 Prior review and incident records

Ask: Counsel and export lead.

Gather: Previous specialist reports, findings, corrective actions, suspected unauthorized access or shipments, regulator correspondence and disclosure records where authorized.

Where to ask: Restricted counsel or export files.

Why it matters: Avoids repeating unresolved issues or making inconsistent representations.

If missing or uncertain: Send potential violations to counsel and the specialist promptly; counsel decides reportability and any disclosure.

Sources: EA04; IT04

EX-R15 Secure specialist access

Ask: Business sponsor and counsel.

Gather: Identity or authorization of proposed recipients, secure repository, access restrictions, legal agreement and approved transfer method.

Where to ask: Engagement and information security records.

Why it matters: Sharing the preparation evidence can itself require export and privacy review.

If missing or uncertain: Supply a nonsensitive index until authority and secure delivery are agreed.

Sources: EA01; IT02; IT03

Export controls: questions for IT and system owners

A useful answer names the actual system, period, supporting record and limits. Where someone else holds the answer, record who can give it. The same questions are in IT-and-owner-questions.csv.

No.	Question	Suggested responder	Supporting record
1	What precisely are you asking the specialist to review: hardware, software, technical data, services or a transaction?	Client IT or system owner	Item or version list and a sanitized activity description.
2	Who made each existing classification and what version and facts did it cover?	Client IT or system owner	Dated rationale and government or supplier correspondence, clearly distinguished.
3	Where can people outside the approved project view, download or administer the information?	Client IT or system owner	Access map including support, backups, ticketing and collaboration.

© 2026 Global Digital Forensics, Inc. All rights reserved.

No.	Question	Suggested responder	Supporting record
4	Can any provider, administrator or subprocessor decrypt the information?	Client IT or system owner	Architecture and key custody statement; no secrets in the response.
5	Which countries, people and entities are involved in the planned activity?	Client IT or system owner	Restricted transaction or person review file approved by counsel.
6	Which license, agreement, exception or exemption is proposed as the authorization?	Client IT or system owner	Document, provisos, expiration, parties and specialist question.
7	What changed since the previous determination?	Client IT or system owner	Change list covering technology, parties, destinations and services.
8	Are there agency requests, existing holds or uncertain prior transfers?	Client IT or system owner	Counsel controlled chronology and records index.

Export controls: decisions and handoff

These decisions belong to counsel or the receiving specialist. Each stays open until its owner records a decision. Add questions specific to the client and a responsible person in Open-questions.csv.

Preparing the handoff

The handoff is ready when sanitized descriptions of the entity, activities, items and versions come first; settled classifications and authorizations are kept apart from proposed ones; the access, cloud, technical data and transaction maps name their unknowns and owners; and the specialist has confirmed authorization before receiving restricted technical information.

Use Record-index.csv for one row per file or defined record set, and follow the walkthrough in the library for custody, restricted records and receipt.

ID	Decision	Decision owner	Information needed	Closed by
EX-Q01	Which items, data or services are subject to EAR, ITAR, another regime or a documented exclusion?	Export control specialist and counsel	Specifications, jurisdiction or classification history, technical descriptions and activities	Written determination tied to the actual item and version.
EX-Q02	Is the proposed storage, access or transfer authorized, including provider support and key access?	Export control specialist with IT architect	Actual access paths, parties or locations, encryption facts and authorizations	Transaction and system specific instructions, including unresolved conditions before release.
EX-Q03	Which sanctions, nuclear, classified or contractual restrictions also apply?	Counsel and appropriate specialist	Parties, countries, products or services and contract	Explicit referral or documented exclusion for each other regime.

Sources: EA01, IT04, IT01, EA03, EA04, EA05, IT03, IT05, IT02, EA02

© 2026 Global Digital Forensics, Inc. All rights reserved.

Package 05: Departed employee

Help counsel and a forensic examiner identify the people, devices, accounts, repositories and short lived records that matter before collection begins. Who uses it: Attorneys, paralegals, HR, project coordinators and client IT. Scope: Employment, confidential information, trade secret and departure disputes under federal and state rules.

Before you gather

Begin with the events and dates. Ask counsel to name the issues, custodians, time ranges and preservation priorities, and include records that may support or contradict the allegation. A request for every record on every device slows the work and invites objections.

Preserve before offboarding erases it. Disabling an account, removing a license, transferring ownership, wiping a device or reissuing it can destroy evidence. Coordinate containment and preservation with counsel and authorized IT, and record what changed and when. Synced folders and emailed links often point to cloud copies, so request content, versions, sharing records and identity events from the cloud service as well.

Know the federal claim. The Defend Trade Secrets Act lets the owner of a misappropriated trade secret related to a product or service used in, or intended for use in, interstate or foreign commerce bring a civil action (18 U.S.C. 1836(b)(1)). Information is a trade secret only if the owner took reasonable measures to keep it secret and it derives independent economic value from not being generally known (18 U.S.C. 1839(3)), so gather the access controls, confidentiality agreements, training and marking records alongside the activity records. The action must be brought within three years after the misappropriation is discovered, or should have been discovered with reasonable diligence (1836(d)), and a court may order civil seizure only in extraordinary circumstances (1836(b)(2)). State trade secret, restrictive covenant and employee privacy law varies by state, so counsel confirms which state rules apply.

Match the procedure to the court. Counsel reviews preservation under Federal Rule of Civil Procedure 37(e), proportionality under Rule 26(b), possession, custody or control, privilege, local rules and case orders. Federal Rule 33 ordinarily limits interrogatories to 25, including discrete subparts. In New York state court, CPLR 3130 and the Uniform and Commercial Division rules add their own limits. The sample questions are a drafting bank for counsel to tailor.

Using the worksheets

Give each request to its suggested owner and record each response, including any gap, in Gathering-checklist.csv. Point to records held in the approved evidence location, where passwords, real patient data and controlled technical information stay.

Departed employee: records to find

Each request below matches a row in Gathering-checklist.csv. Record the response, status and record IDs there.

EMP-R01 Matter facts and timeline

Ask: Counsel and HR.

© 2026 Global Digital Forensics, Inc. All rights reserved.

Gather: Employment or role dates, departure timeline, relevant business files or events, parties, issues and permitted time range.

Where to ask: HR, manager and counsel.

Why it matters: Directs a proportionate information request without presuming wrongdoing.

If missing or uncertain: Separate known facts, allegations and questions.

Sources: LG01 26; NY05 11-c

EMP-R02 Preservation and offboarding status

Ask: Counsel and authorized IT.

Gather: Hold instructions or implementation, relevant retention settings, pending deletions, license changes, account disabling, wipes and replacement or reassignment records.

Where to ask: Counsel, messaging, identity and endpoint owner.

Why it matters: Identifies time sensitive risk of losing relevant information.

If missing or uncertain: Escalate imminent deletion or unknown hold coverage at once; an early hold preserves the most.

Sources: LG01 37(e); MS03; GO01

EMP-R03 Custodian and identifier list

Ask: HR and IT.

Gather: Names, roles, aliases, employee or user IDs, email addresses, tenant or domain IDs, device IDs and relevant shared or group accounts.

Where to ask: HR, identity and asset systems.

Why it matters: Allows the collector to resolve actual identities and sources.

If missing or uncertain: Record gaps for shared or renamed accounts and former or acquired domains.

Sources: NI04; MS01

EMP-R04 Devices and media

Ask: Asset owner and custodian.

Gather: D01 to D03 and any home or personal device used for work, with ownership, location, custody, status and authority unresolved where appropriate.

Where to ask: Asset records and interviews.

Why it matters: Surfaces devices and removable copies beyond the returned laptop.

If missing or uncertain: Ask counsel before seeking personal device data; a forensic examiner images it under that authority.

Sources: NI04; LG01

© 2026 Global Digital Forensics, Inc. All rights reserved.

EMP-R05 Mail calendars and archives

Ask: Messaging and archive owner.

Gather: D04/D08/D19, shared or delegated mail, aliases, mail journals, archive migrations and relevant holds.

Where to ask: Messaging and archive systems.

Why it matters: An individual active mailbox may omit the relevant communications.

If missing or uncertain: Identify archived, inactive or deleted sources and documented capture gaps.

Sources: MS01; GO01; NI04

EMP-R06 Work drives and shared files

Ask: Cloud or file administrators.

Gather: D05/D06/D09/D25, exact site or share paths, owners, external links, versions and relevant sharing records.

Where to ask: File servers, OneDrive, SharePoint, Drive and DMS.

Why it matters: Finds the cloud original and collaboration history beyond synced copies.

If missing or uncertain: List external owner links and recycle bin or hold limitations.

Sources: MS03; MS05; GO01

EMP-R07 Messages and meetings

Ask: Collaboration owners and custodians.

Gather: D07/D10/D11/D12, direct or group chats, external or shared channels, recordings or transcripts and linked attachments.

Where to ask: Collaboration systems and interview.

Why it matters: Identifies communications outside email.

If missing or uncertain: Ask about actual apps, subscriptions, history and limits so the examiner can assess what can be recovered.

Sources: MS02; GO01; SL01; SL02

EMP-R08 Access transfer and security traces

Ask: Security and network teams.

Gather: D13 to D18 and relevant D34; log coverage, earliest or latest dates, field legend, device or IP mappings and permissions.

Where to ask: Identity, SIEM, EDR or DLP, VPN, proxy and cloud admins.

Why it matters: Lets the forensic specialist evaluate leads and gaps.

If missing or uncertain: Describe each alert, download or USB event factually and leave interpretation to the examiner. Record unknown actor or content and missing coverage.

Sources: NI04; MS04; GO02; AW01

© 2026 Global Digital Forensics, Inc. All rights reserved.

EMP-R09 Business and project sources

Ask: Business and application owners.

Gather: D22 to D28, customer or project lists, code or design repositories, tickets and relevant documents/workflows.

Where to ask: CRM, engineering, projects and practice systems.

Why it matters: Can show legitimate work, chronology and alternate explanations as well as disputed activity.

If missing or uncertain: Identify actual modules and export omissions rather than assuming the current report is complete.

Sources: NI04; CL01

EMP-R10 Backups and historical environments

Ask: Backup or migration owner.

Gather: D20/D21, catalogs, retention or overwrite dates, restore dependencies, keys held by owner and earlier export copies.

Where to ask: Backup provider and migration project.

Why it matters: Determines whether potentially relevant earlier copies exist.

If missing or uncertain: Request a cost and scope estimate for an isolated restoration planned by the specialist.

Sources: NI04; LG01 26(b)(2)

EMP-R11 Personal external and third party sources

Ask: Counsel and custodian.

Gather: Known work related external accounts, recipient organizations and relevant third party systems, with the basis for knowledge and control.

Where to ask: Interview and business records.

Why it matters: Enables counsel to choose consent, party request or lawful third party process.

If missing or uncertain: No guessed passwords, bypassing access or blanket demands for private accounts.

Sources: LG01 34,45; NY05

EMP-R12 Collection and response index

Ask: Coordinator and collector.

Gather: What was actually preserved or collected, who performed it, exact scope or filters, date or time zone, hashes where used, errors and missing sources.

Where to ask: Collection report and file index.

Why it matters: Allows the receiving expert to assess coverage and request remaining work.

If missing or uncertain: Record the search terms, scope and errors with every download or zero result.

Sources: NI04; MS06

© 2026 Global Digital Forensics, Inc. All rights reserved.

Departed employee: questions for IT and system owners

A useful answer names the actual system, period, supporting record and limits. Where someone else holds the answer, record who can give it. The same questions are in IT-and-owner-questions.csv.

No.	Question	Suggested responder	Supporting record
1	Which accounts and devices did the person use for the relevant work, including shared and renamed accounts?	Client IT or system owner	Identifier crosswalk with dates and ownership.
2	Which offboarding actions have occurred and what remains scheduled?	Client IT or system owner	Dated action or change records and preservation confirmation.
3	Where do linked cloud files live, and who owns the external or shared copies?	Client IT or system owner	Exact tenant, site, share or workspace IDs and owner list.
4	Which tools other than email did the person and coworkers actually use?	Client IT or system owner	Custodian interview notes with apps or accounts and purpose.
5	What event types were logged at the time and how far back can each source be retrieved?	Client IT or system owner	Coverage or retention table, earliest or latest examples and field legend.
6	Could a device, account, IP or badge have been shared or used by an administrator?	Client IT or system owner	Assignment, delegation and remote support records.
7	What migrations, deletions, license changes or policy changes may have affected records?	Client IT or system owner	Change log with known gaps and decision owners.
8	What does a permitted export include, and which errors or unindexed items does it list?	Client IT or system owner	Export process report and documented limitations.

Departed employee: sample questions for counsel

These are drafting prompts for counsel to tailor: define the event, source, period and parties, and check relevance, proportionality, privilege, privacy, possession, custody or control, local rules and case orders. A document request, interview or deposition topic may be the better device. The prompts are also in Discovery-drafting-questions.csv.

No.	Prompt
1	Identify the custodians of records concerning [defined disputed event] during [period] and each custodian role.
2	Identify the devices assigned to [person] during [period], including their unique identifiers and current custodian.
3	Identify the business accounts used by [person] for [defined project], including aliases and shared accounts.
4	Identify the repositories holding [defined project records] during [period], their responsible administrators and relevant external owners.

© 2026 Global Digital Forensics, Inc. All rights reserved.

No.	Prompt
5	Describe the retention or deletion settings applicable to [defined source] during [period], including material changes and known data gaps.
6	Identify the log sources that record [defined activity] for [period] and the person able to explain their coverage and fields.
7	Identify the preservation and collection actions actually taken for [defined source], including dates and persons performing them, without requesting privileged advice.
8	Identify responsive sources not searched or produced and the factual basis for claimed inaccessibility or limitation, subject to the applicable rules and orders.

Departed employee: decisions and handoff

These decisions belong to counsel or the receiving specialist. Each stays open until its owner records a decision. Add questions specific to the client and a responsible person in Open-questions.csv.

Worked example

A returned laptop holds an online only shortcut to a project folder. The coordinator records the shortcut and asks IT for the site owner, the relevant versions and the sharing records. The examiner chooses the collection method; nobody assumes the laptop holds the full folder.

Preparing the handoff

The handoff is ready when counsel has agreed the issue, date and custodian scope and the authority to collect; imminent deletion and offboarding actions are recorded and escalated; cloud services, archives, backups and business systems are covered alongside the endpoints; and the source inventory distinguishes possible, confirmed, preserved and collected locations.

Use Record-index.csv for one row per file or defined record set, and follow the walkthrough in the library for custody, restricted records and receipt.

ID	Decision	Decision owner	Information needed	Closed by
EMP-Q01	What sources and time ranges are proportionate and within lawful possession, custody or control?	Counsel	Claims, issues, chronology, ownership and proposed source inventory	Counsel approved scope and authority before collection; preserve separately where required.
EMP-Q02	Can the relevant activity be attributed, and what alternatives remain?	Forensic specialist	Original records, timestamps, IDs, mappings and limitations	Expert analysis of the collected records.

Sources: LG01, NY05, MS03, GO01, NI04, MS01, MS05, MS02, SL01, SL02, MS04, GO02, AW01, CL01, MS06, NY06, NY07, NY08, LG03

© 2026 Global Digital Forensics, Inc. All rights reserved.

Package 06: Commercial and contract disputes

Help counsel and a technical consultant locate the records of negotiation, agreement, performance, payment and change across business systems. Who uses it: Attorneys, paralegals, business contacts, project coordinators and client IT. Scope: Contract and commercial disputes, including electronic agreements, performance records and damages workbooks.

Before you gather

Build a transaction chronology keyed to contract, project, order and customer IDs. Collect the executed agreement with its incorporated schedules, amendments and approvals, and the records of actual performance. The documents that explain a deal often sit in separate legal, sales, finance, engineering and provider systems.

Ask what an export really contains. A PDF of the signed contract may omit the negotiation history, a referenced cloud document, the signature envelope history and the completion certificate. A current CRM report may omit prior field values and attachments. The system owner can say what the actual export includes.

Keep source data, reports and calculations apart. Preserve the source transactions and the native spreadsheets, and record how any report or damages schedule was prepared, including filters, assumptions, underlying transaction IDs and cutoffs. Keep the native spreadsheet behind any PDF summary.

Tailor the sample questions. Counsel defines the terms, dates and scope and checks interrogatory limits, burden, privilege, third party control, local rules and case orders. Federal Rule 33 ordinarily limits interrogatories to 25, including discrete subparts; in New York state court, CPLR 3130 and the Uniform and Commercial Division rules add their own limits.

Using the worksheets

Give each request to its suggested owner and record each response, including any gap, in Gathering-checklist.csv. Point to records held in the approved evidence location, where passwords, real patient data and controlled technical information stay.

Commercial and contract disputes: records to find

Each request below matches a row in Gathering-checklist.csv. Record the response, status and record IDs there.

CON-R01 Matter and transaction crosswalk

Ask: Counsel and business owner.

Gather: Claims or issues, parties and roles, key dates, agreement, project, order or customer IDs, relevant entities, periods and disputed provisions.

Where to ask: Counsel, sales and contract team.

Why it matters: Links a legal question to actual business systems and identifiers.

If missing or uncertain: Separate disputed interpretation from agreed facts; record missing IDs.

Sources: LG01 26; NY05 11-c

© 2026 Global Digital Forensics, Inc. All rights reserved.

CON-R02 Agreement and incorporated material

Ask: Contract owner.

Gather: Executed agreements, exhibits, referenced documents, statements of work, amendments, side letters, notices and version or effective dates.

Where to ask: Legal files, CLM, DMS and deal room.

Why it matters: Defines which record family the specialist should organize.

If missing or uncertain: Identify missing incorporated documents and external links behind the visible PDF.

Sources: LG01 34; NI04

CON-R03 Drafts and negotiation

Ask: Counsel, sales and document owners.

Gather: Relevant drafts, redlines or comments, version history, approval chains, emails or chats and negotiation notes within counsel approved scope.

Where to ask: Mail, collaboration, DMS and CLM.

Why it matters: Shows development of the agreement and the actual custodians.

If missing or uncertain: Counsel handles privilege; collect or segregate factual metadata without demanding advice in general questionnaires.

Sources: LG01 26(b)(5); NY05 11-b; MS05

CON-R04 Signature and acceptance records

Ask: Signing service and contract owners.

Gather: Envelope or agreement IDs, signed originals, history, completion certificate, recipient roles, delivery and acceptance records.

Where to ask: Signing provider, email and contracting system.

Why it matters: Supplies supporting transaction records beyond the signature image.

If missing or uncertain: Availability is account, permission or retention dependent. Ask provider for the exact scope and field meanings.

Sources: DS01; LG02

CON-R05 Sales and commitments

Ask: Sales operations.

Gather: CRM opportunities or quotes, product representations, pricing versions, approvals, attachments and relevant activity/history.

Where to ask: CRM, quoting tool, mail and proposals.

Why it matters: Locates commercial representations and approval records.

If missing or uncertain: Determine the available object and field history and linked file capture for this CRM.

© 2026 Global Digital Forensics, Inc. All rights reserved.

Sources: NI04; LG01

CON-R06 Procurement delivery and performance

Ask: Operations and project manager.

Gather: Orders, shipment, delivery or receipt, work logs, milestones, acceptance or rejection, service tickets, quality records and change requests.

Where to ask: ERP, logistics, project, service and quality systems.

Why it matters: Enables a chronology of performance and disputes.

If missing or uncertain: Record separate date meanings and partial deliveries; identify third party records.

Sources: NI04; LG01

CON-R07 Engineering and service versions

Ask: Engineering and service owner.

Gather: Product, software or configuration versions, repository releases, change approvals, requirements and relevant existing technical logs.

Where to ask: Repositories, change systems and providers.

Why it matters: Can connect what was promised, delivered, changed and supported.

If missing or uncertain: Ask for historical records of the deployment in place at the time. Ask for historical records and limitations.

Sources: NI04

CON-R08 Invoices payments and adjustments

Ask: Finance.

Gather: Invoices, credits, payment or remittance records, accounts receivable or payable, journals, approval history and disputed bank detail changes.

Where to ask: ERP, banking records through owner, procurement.

Why it matters: Supports traceable transaction and chronology review.

If missing or uncertain: Identify system or report cutoffs, currency and adjustments; specialist evaluates financial meaning.

Sources: NI04; LG01

CON-R09 Communications and meeting material

Ask: Custodians and collaboration owner.

Gather: Relevant mail, chats, calls or recordings if made, minutes, internal or external channels and linked attachments.

Where to ask: D04 to D12 and D19.

Why it matters: Captures other than email discussions and external party collaboration.

© 2026 Global Digital Forensics, Inc. All rights reserved.

If missing or uncertain: Identify unsupported meeting content, external retention and which calls were recorded.

Sources: MS02; GO01; SL02

CON-R10 Damages inputs and workbooks

Ask: Finance and counsel.

Gather: Existing source transactions, calculation files with formulas, assumptions, revisions and relationship to the claimed categories.

Where to ask: Finance systems and working files.

Why it matters: Allows experts to test or explain calculations later.

If missing or uncertain: Keep native spreadsheets and source IDs. Keep the native spreadsheet behind any PDF summary.

Sources: LG01 26; NI04

CON-R11 Archives backups and former platforms

Ask: IT, archive and migration owners.

Gather: D19 to D21, older deal rooms or tenants, catalogs, relevant dates and restoration feasibility.

Where to ask: Historical systems and providers.

Why it matters: Identifies records that a present application search misses.

If missing or uncertain: Specialist evaluates proportionate isolated restoration; coordinator records known cost and access barriers.

Sources: LG01 26(b)(2); NI04

CON-R12 Third party and legal practice copies

Ask: Counsel and legal operations.

Gather: Counterparty, broker, logistics, advisers, insurer and practice management source inventory, including portals and separate module exports.

Where to ask: D28 and D35.

Why it matters: Reveals distinct copies and possible lawful request paths.

If missing or uncertain: Counsel confirms which adviser files the client controls. Privilege and control need counsel review.

Sources: LG01 34,45; CL01

CON-R13 Preservation and collection report

Ask: Counsel and collector.

Gather: Actual preservation or collection, source list, time zone, queries or filters, versions, exports, errors, chain of custody and known exclusions.

Where to ask: Preservation file and collection reports.

© 2026 Global Digital Forensics, Inc. All rights reserved.

Why it matters: Allows the receiving specialist to understand the record set limits.

If missing or uncertain: Record incomplete families, unresolved links and missing periods, and keep originals beside any corrected reconstruction.

Sources: NI04; MS06

Commercial and contract disputes: questions for IT and system owners

A useful answer names the actual system, period, supporting record and limits. Where someone else holds the answer, record who can give it. The same questions are in IT-and-owner-questions.csv.

No.	Question	Suggested responder	Supporting record
1	Which IDs join the agreement, quote, order, project, invoice and support case?	Client IT or system owner	Crosswalk with system owners and date definitions.
2	Where are versions, comments, approvals and side agreements kept?	Client IT or system owner	DMS, CLM or workspace paths and relevant custodians.
3	What does the executed contract export omit?	Client IT or system owner	List of incorporated documents, signature artifacts and linked files.
4	Which records show delivery, acceptance, rejection or a requested change?	Client IT or system owner	Existing operation records and their authors/dates.
5	How are sales or finance records corrected and can prior values be retrieved?	Client IT or system owner	Audit or history settings and reports for the period.
6	Which outside parties hold distinct performance or transaction records?	Client IT or system owner	Third party source list, ownership and proposed counsel request route.
7	How was each existing damages schedule generated?	Client IT or system owner	Native workbook, source IDs, filters, periods and assumptions.
8	What was migrated or deleted, and what remains available elsewhere?	Client IT or system owner	Migration or reconciliation and retention records.

Commercial and contract disputes: sample questions for counsel

These are drafting prompts for counsel to tailor: define the event, source, period and parties, and check relevance, proportionality, privilege, privacy, possession, custody or control, local rules and case orders. A document request, interview or deposition topic may be the better device. The prompts are also in Discovery-drafting-questions.csv.

No.	Prompt
1	Identify the custodians and repositories of the agreement identified as [agreement ID] and its incorporated schedules and amendments.

© 2026 Global Digital Forensics, Inc. All rights reserved.

No.	Prompt
2	Identify the systems used to store drafts, revisions and approvals for [defined agreement] during [period].
3	Identify the signing service envelope or agreement identifiers and the custodian of the available history and completion certificate.
4	Identify the order, project, invoice and support identifiers associated with [defined transaction].
5	Identify the sources of records concerning [specified delivery or acceptance event] and their responsible custodians.
6	Describe the report, fields, filters and source records used to prepare [identified factual transaction summary], excluding privileged advice.
7	Identify relevant third party repositories and the factual basis of the responding party's control over records within them.
8	Identify known retention, migration or export limitations affecting [defined record class] during [period].

Commercial and contract disputes: decisions and handoff

These decisions belong to counsel or the receiving specialist. Each stays open until its owner records a decision. Add questions specific to the client and a responsible person in Open-questions.csv.

Worked example

An invoice dispute turns on a change order signed through an electronic signature service. The team links the order ID, the signed document, the incorporated scope, the envelope history and the project acceptance records, and lists the sources still missing. Counsel decides whether the change was legally effective.

Preparing the handoff

The handoff is ready when agreement and transaction IDs connect the records across systems; source records, summaries and calculated schedules remain distinguishable; signature events and ordinary business records are indexed with their history; and counsel approved scope, privilege handling and known gaps travel with the file index.

Use Record-index.csv for one row per file or defined record set, and follow the walkthrough in the library for custody, restricted records and receipt.

ID	Decision	Decision owner	Information needed	Closed by
CON-Q01	Which agreement family, period and transaction issues define the request?	Counsel with business owner	Claim or case documents, agreement IDs, chronology and contract family	Written scope and proposed search or collection plan.
CON-Q02	Which reports omit history, attachments or relationships?	Application owner and receiving consultant	Export documentation, data dictionary, sample and error reports	Documented export plan with its limitations.

Sources: LG01, NY05, NI04, MS05, DS01, LG02, MS02, GO01, SL02, CL01, MS06, NY06, NY07, NY08

© 2026 Global Digital Forensics, Inc. All rights reserved.

Package 07: Medical matters

Help a legal and technical team identify the clinical, administrative and audit records that matter in a medical matter and hand them to a specialist lawfully and precisely. Who uses it: Attorneys, paralegals, health information management, privacy officers, project coordinators and client IT. Scope: Medical treatment, documentation and privacy disputes. Clinical opinions stay with qualified clinicians and experts.

Before you gather

Start with the episode. Use the clinical episode, issues, patient identifiers and date range selected by counsel. The EHR may be one of several systems, so ask about separate imaging, laboratory, pharmacy, practice management, claims, portal, interface, legacy and backup sources.

Separate the layers of the record. A chart rendering, the underlying clinical record, version and amendment information, audit events and billing records answer different questions. Ask what the actual export includes before treating a printed chart as the full electronic record.

Ask how logging was configured. The HIPAA Security Rule requires audit controls that record and examine activity in systems containing electronic protected health information (45 CFR 164.312(b)); each product and site sets which events it logs and how long it keeps them. Request the vendor and version, the enabled event types, field definitions, clock settings and the earliest and latest available dates.

Confirm the authority for each disclosure. 45 CFR 164.512(e) sets different conditions for a court order and for a subpoena. Substance use disorder records under 42 CFR Part 2, psychotherapy notes and other state protected categories carry added protections; HHS gives February 16, 2026 as the compliance date for the 2024 Part 2 final rule. Keep real patient records in the restricted workspace.

Find the actual retention rule. The HIPAA Privacy Rule sets no general retention period for medical records, and the six year period in 45 CFR 164.316(b)(2) applies to required HIPAA documentation, not to charts. State law, licensure, payer contracts and preservation duties set the period for each record type.

Using the worksheets

Give each request to its suggested owner and record each response, including any gap, in Gathering-checklist.csv. Point to records held in the approved evidence location, where passwords, real patient data and controlled technical information stay.

Medical matters: records to find

Each request below matches a row in Gathering-checklist.csv. Record the response, status and record IDs there.

MED-R01 Matter scope and legal authority

Ask: Counsel and privacy officer.

Gather: Issues, relevant care episodes or periods, providers, jurisdiction, proper patient or representative authority and applicable authorization, order or other approved process.

Where to ask: Counsel and privacy or HIM files.

© 2026 Global Digital Forensics, Inc. All rights reserved.

Why it matters: Defines the lawful, proportionate request and recipients.

If missing or uncertain: Collect and disclose through the route counsel approves.

Sources: HE02 164.512(e); HE03; LG01

MED-R02 Patient and encounter crosswalk

Ask: HIM and registration owner.

Gather: Approved patient identifiers, historical or merged IDs, encounter or account numbers, facilities, aliases as relevant and matching limitations.

Where to ask: Master patient index and registration.

Why it matters: Prevents wrong patient or missing encounter requests.

If missing or uncertain: Use masked IDs in general coordination; maintain the actual crosswalk in the restricted workspace.

Sources: HE01; NI04

MED-R03 System and vendor map

Ask: Clinical IT and department owners.

Gather: EHR vendor, version or modules, hosting, facilities, departmental systems, portal or HIE, practice management, billing, dictation, devices or interfaces, legacy and backup services.

Where to ask: Clinical architecture, application inventory and providers.

Why it matters: Identifies actual systems that may contain relevant records or logs.

If missing or uncertain: Confirm each candidate system with its owner.

Sources: HE01; HE06; NI04

MED-R04 Clinical record export description

Ask: HIM and application owner.

Gather: Available chart components, signed or unsigned status, notes, orders or results, attachments, flowsheets, medication or administration and export format or options for the selected episode.

Where to ask: Clinical record system and departmental records.

Why it matters: Allows the recipient to specify what is needed beyond a routine printout.

If missing or uncertain: Ask for a component list, data dictionary and exclusions rather than a claim of complete EMR.

Sources: HE01; HE06

MED-R05 Documentation history and amendments

Ask: Clinical application owner.

Gather: Existing addenda, corrections, amendment records, signature or cosignature history and available earlier versions relevant to the issue.

© 2026 Global Digital Forensics, Inc. All rights reserved.

Where to ask: EHR audit or version functions and provider.

Why it matters: Supports later professional interpretation of documentation chronology.

If missing or uncertain: Record the event definition and any workflow explanation for each timestamp difference.

Sources: HE06; NI04

MED-R06 Audit and access records

Ask: Clinical security and vendor.

Gather: Event types, actor, patient or encounter IDs, actions, source workstation, session or IP where available, emergency or proxy access, configuration changes, retention and report parameters.

Where to ask: Clinical audit system, vendor and security.

Why it matters: Helps the specialist understand what actions can actually be examined.

If missing or uncertain: Mark which fields are recorded, which periods each log covers and whether and when logging was enabled. Confirm actual log completeness with the vendor and site.

Sources: HE01 164.312(b); HE06

MED-R07 Timestamp and identity explanations

Ask: Clinical IT and HIM.

Gather: Meaning of entered, service, event, signed, imported or modified times; local, UTC, time zone or DST rules; clock sources; shared, delegated or service users and ID mappings.

Where to ask: Application data dictionary and administrators.

Why it matters: Prevents false sequences or attribution.

If missing or uncertain: Ask the vendor for a written explanation where needed and record any time conversion.

Sources: NI04; HE06

MED-R08 Imaging and diagnostic sources

Ask: Radiology laboratory and pathology owners.

Gather: Relevant source images or reports, diagnostic results, amendments, accession or order IDs and exchange or interface records from actual systems.

Where to ask: PACS or RIS, laboratory or pathology and interfaces if used.

Why it matters: Request the underlying diagnostic objects behind the chart report.

If missing or uncertain: The specialist defines the native objects and format needed, and the owner confirms whether and where each artifact is held.

Sources: HE01; NI04

MED-R09 Medication and treatment operations

Ask: Pharmacy and clinical operations.

© 2026 Global Digital Forensics, Inc. All rights reserved.

Gather: Relevant prescription, dispense or administration records, order changes, medication reconciliation and connected device records where actually kept.

Where to ask: Pharmacy, eMAR and relevant devices or providers.

Why it matters: Identifies distinct clinical record sources.

If missing or uncertain: Separate scheduled, ordered, dispensed, charted and administered meanings for a qualified clinician or expert to interpret.

Sources: HE01; NI04

MED-R10 Portal referral and exchange

Ask: Portal, HIE or telehealth owners.

Gather: Relevant messages, uploads, referrals, exchanged documents, telehealth material if recorded, proxy permissions and interface error or status records.

Where to ask: D32 and communications providers.

Why it matters: Surfaces patient facing and interorganization information.

If missing or uncertain: Confirm recording and retention; patient proxy activity and imports require interpretation.

Sources: HE01; HE03; HE06

MED-R11 Practice administration and claims

Ask: Practice manager and billing.

Gather: Scheduling or check in, calls if recorded, referrals, eligibility or authorizations, coding, claims or remittances and corrections for relevant episodes.

Where to ask: Practice management, clearinghouse, payer and phone systems.

Why it matters: Links clinical and administrative events without treating them as equivalent.

If missing or uncertain: Ask for unique IDs and export omissions, and pair claims and charges with clinical records.

Sources: HE01; HE03; NI04

MED-R12 Relevant communications and external copies

Ask: Counsel and custodians.

Gather: Permitted relevant internal or provider messages, secure texting, mail, incident communications, outside care records and legal or practice management files.

Where to ask: Clinical communication tools, D04 to D12, D28 and D35.

Why it matters: Finds sources outside the clinical chart.

If missing or uncertain: Counsel separates privilege, patient protections and third party authority. Request only patient and personnel material related to the matter.

Sources: LG01; HE02; CL01

© 2026 Global Digital Forensics, Inc. All rights reserved.

MED-R13 Preservation retention and historical data

Ask: Counsel, records and IT.

Gather: Actual retention schedules, holds, overwrite dates, former systems, migration reconciliation, backups or catalogs and access or restoration constraints.

Where to ask: HIM, records manager, migration and backup providers.

Why it matters: Supports a time sensitive, realistic collection plan.

If missing or uncertain: No generic HIPAA six year chart rule; identify actual state, provider, record or patient circumstances for specialist review.

Sources: HE04; HE01 164.316; LG01 37(e)

MED-R14 Sensitive record segmentation

Ask: Privacy officer and counsel.

Gather: Whether Part 2, psychotherapy or other specially protected records are involved; relevant consents or orders and release restrictions.

Where to ask: Privacy or HIM and counsel restricted file.

Why it matters: Allows lawful limited disclosure and separate handling.

If missing or uncertain: Pending authority stays visible. Counsel confirms the authority for any use in litigation against the patient.

Sources: HE05; HE07; HE02

MED-R15 Export quality and transfer

Ask: Collector and receiving specialist.

Gather: Export method, account or role, dates or time zone, parameters, counts by component, metadata or attachments, errors, field legend, hashes where used and transfer receipt.

Where to ask: Collection reports and approved evidence repository.

Why it matters: Makes completeness and limitations reviewable.

If missing or uncertain: The specialist chooses any additional export; keep originals and record every change.

Sources: NI04; HE06

Medical matters: questions for IT and system owners

A useful answer names the actual system, period, supporting record and limits. Where someone else holds the answer, record who can give it. The same questions are in IT-and-owner-questions.csv.

© 2026 Global Digital Forensics, Inc. All rights reserved.

No.	Question	Suggested responder	Supporting record
1	Which systems contain the selected patient episodes and which system owns each component?	HIM, privacy officer and clinical IT as appropriate	System, module or owner and identifier map.
2	What does your routine chart export include and omit?	HIM, privacy officer and clinical IT as appropriate	Written component or format description and a permitted masked sample.
3	Can earlier note versions, addenda, signatures and corrections be separately retrieved?	HIM, privacy officer and clinical IT as appropriate	Vendor or site specific capability and actual availability statement.
4	Which events does the audit export include?	HIM, privacy officer and clinical IT as appropriate	Event dictionary, enabled settings, query scope and retention dates.
5	What do the different timestamps and user identifiers mean?	HIM, privacy officer and clinical IT as appropriate	Data dictionary, time zone or DST rules and identity or proxy mappings.
6	What records remain in old systems, departmental platforms, exchanges or backups?	HIM, privacy officer and clinical IT as appropriate	Historical system and retention inventory with owners.
7	Which requested records require separate authority or segregation?	HIM, privacy officer and clinical IT as appropriate	Privacy or counsel approved release route and restrictions.
8	What errors, patient matching limits, missing intervals or excluded components affect the response?	HIM, privacy officer and clinical IT as appropriate	Exception report linked to the record request IDs.

Medical matters: sample questions for counsel

These are drafting prompts for counsel to tailor: define the event, source, period and parties, and check relevance, proportionality, privilege, privacy, possession, custody or control, local rules and case orders. A document request, interview or deposition topic may be the better device. The prompts are also in Discovery-drafting-questions.csv.

No.	Prompt
1	Identify the systems and responsible custodians maintaining records of [defined patient episode] during [period], subject to the authorized disclosure scope.
2	Identify the patient, encounter, accession and account identifiers used to link the responsive components, under the agreed privacy protections.
3	Describe the components included in and excluded from [identified chart export] and the export parameters used.
4	Identify available records of amendments, addenda and signature events for [defined documentation], without assuming those records establish improper alteration.

© 2026 Global Digital Forensics, Inc. All rights reserved.

No.	Prompt
5	Identify the recorded audit event types, retained periods and person able to explain the fields for [specified system and period].
6	Describe the meanings and time zone conventions of the date or time fields in [identified export].
7	Identify relevant predecessor or departmental systems or migration limitations affecting [defined record category].
8	Identify the factual preservation or collection steps and known omissions for [defined source], excluding privileged legal advice and respecting protected record restrictions.

Medical matters: decisions and handoff

These decisions belong to counsel or the receiving specialist. Each stays open until its owner records a decision. Add questions specific to the client and a responsible person in Open-questions.csv.

Worked example

The chart printout shows a note signed two days after the visit. The coordinator asks health information management for the definitions of service, entry and signature times and for any amendment or audit records. The specialist reviews the workflow and then interprets the sequence.

Preparing the handoff

The handoff is ready when counsel and the privacy officer have recorded the authority and any sensitive record restrictions; clinical, audit, diagnostic, portal and administrative records are requested as separate components; timestamps, identities, versions, formats and missing intervals have explanations or named questions; and restricted evidence moves only through the agreed route while the ordinary index uses masked identifiers.

Use Record-index.csv for one row per file or defined record set, and follow the walkthrough in the library for custody, restricted records and receipt.

ID	Decision	Decision owner	Information needed	Closed by
MED-Q01	What legal authority permits each disclosure and recipient, including specially protected material?	Counsel and privacy officer	Actual process, consent or order, case purpose and record categories	Written release instructions before any disclosure.
MED-Q02	Which record components, event types and versions exist in this deployment?	HIM, vendor and clinical forensic specialist	Vendor or version, configuration, dictionary, masked sample and actual retention	A scoped export plan with its coverage limits.
MED-Q03	Which retention and preservation requirements apply to these records?	Counsel and records specialist	Jurisdiction, provider or license, patient or record facts, schedules and case holds	Record specific schedule and preservation instructions; no blanket six year chart period.

Sources: HE02, HE03, LG01, HE01, NI04, HE06, CL01, HE04, HE05, HE07, NY05, NY06, NY07, NY08

© 2026 Global Digital Forensics, Inc. All rights reserved.

Source register

Laws and regulations set duties within their scope; agency guidance explains how they are applied; NIST supplies methods; vendor documentation describes how a product can behave, which depends on the version and settings in use. The eCFR is the current compilation of federal regulations; check its as of date. The same list, with the date each source was last checked, is in Source-register.csv.

DFS01 DFS final adopted second amendment to Part 500. Adopted regulatory text. 500.1 through 500.24 as amended November 1, 2023; read the amendment markup carefully. https://www.dfs.ny.gov/industry_guidance/regulations/final_adoptions_fs/rf_fs_2amend23nycrr500_text_20231101

DFS02 DFS Part 500 reading copy. Agency reading copy. Full Part 500 reading copy; compare it with the adopted text. https://www.dfs.ny.gov/cybersecurity/23-NYCRR-Part-500

DFS03 DFS cybersecurity submissions. Agency filing guidance. Annual compliance notification; incident and extortion notices. https://www.dfs.ny.gov/cybersecurity/submissions

DFS04 DFS cybersecurity FAQs. Agency interpretation. Exemptions, applicability and program guidance. https://www.dfs.ny.gov/cybersecurity/faqs

DFS05 DFS risk assessment guidance, September 10, 2026. Agency guidance. Risk identification, methodology and use of the risk assessment. https://www.dfs.ny.gov/industry_guidance/industry_letters/il20260910-cyber-risk-assessment

DFS06 DFS regulatory activity. Agency adoption index. Final adoption and notice dated November 1 2023. https://www.dfs.ny.gov/industry_guidance/regulatory_activity/financial_services

NY01 New York General Business Law 899-aa. State statutory text. 1 definitions; 2 and 3 notice; 8 agencies; 9 HIPAA notice. https://www.nysenate.gov/legislation/laws/GBS/899-AA

NY02 New York General Business Law 899-bb. State statutory text. 1 regulated entities and small business; 2 safeguards. https://www.nysenate.gov/legislation/laws/GBS/899-BB

NY03 New York State Technology Law 208. State statutory text. Breach notice regime for state entities. https://www.nysenate.gov/legislation/laws/STT/208

NY04 New York hospital cybersecurity rule. Agency regulatory text. 10 NYCRR 405.46; general hospitals only. https://regs.health.ny.gov/content/section-40546-hospital-cybersecurity-requirements

NY05 New York Commercial Division rules. Court rules. 11-a, 11-b, 11-c, 11-g and ESI Appendix A. https://www.nycourts.gov/rules/rule/section-20270-rules-commercial-division-supreme-court

NY06 New York Uniform Civil Rules Part 202. Court rules. 202.20 interrogatories; 202.20-j and Appendix A. https://www.nycourts.gov/rules/part-202-uniform-civil-rules-supreme-court-and-county-court

NY07 New York CPLR 3130. State procedural text. Use of interrogatories and restrictions. https://www.nysenate.gov/legislation/laws/CVP/3130

NY08 New York CPLR 3133. State procedural text. Answers and objections to interrogatories. https://www.nysenate.gov/legislation/laws/CVP/3133

© 2026 Global Digital Forensics, Inc. All rights reserved.

CM01 CMMC program rule. Federal regulatory compilation. 170.2 definitions and incorporation, 170.14 to 170.24 assessment requirements. https://www.ecfr.gov/current/title-32/subtitle-A/chapter-I/subchapter-G/part-170

CM02 Current CMMC program information. Agency program announcement. Phase 2 suspended July 13, 2026; Phase 1 continues. https://dodcio.defense.gov/cmmc/About/

CM03 CMMC Phase II suspension announcement. Agency announcement. Suspension of the Phase 2 transition, July 13, 2026. https://business.defense.gov/Engage/News/Newsfeed-Repository/Article/4542563/forging-the-arsenal-of-freedom-department-of-war-suspends-cmmc-phase-ii-require/

CM04 DFARS CMMC clause. Federal acquisition clause. 252.204-7021 as incorporated in the contract. https://www.acquisition.gov/dfars/252.204-7021-contractor-compliance-cybersecurity-maturity-model-certification-level-requirements.

CM05 DFARS safeguarding and cyber incident reporting. Federal acquisition clause. 252.204-7012; cloud and incident obligations where incorporated. https://www.acquisition.gov/dfars/252.204-7012-safeguarding-covered-defense-information-and-cyber-incident-reporting.

CM06 FAR basic safeguarding. Federal acquisition clause. 52.204-21; FCI and safeguards. https://www.acquisition.gov/far/52.204-21

CM07 Current defense acquisition class deviations. Agency implementation index. Class Deviation 2026-O0025 Revision 3 and any later revision. https://www.acq.osd.mil/dpap/dars/dfars_far_overhaul_class_deviations.html

CM08 CMMC Level 2 scoping guidance. Agency technical guidance. Asset categories, external and cloud service providers. https://dodcio.defense.gov/Portals/0/Documents/CMMC/ScopingGuideL2v2.pdf

CM09 CMMC resources and documentation. Agency resources index. Current assessment and scoping guides and implementation memoranda. https://dodcio.defense.gov/CMMC/Resources-Documentation/

CM10 Class Deviation 2026-O0025 Revision 3 (signed memorandum and attachments). Signed agency implementation memorandum and attachments. Suspension of the Phase 2 transition, NIST SP 800-171 Revision 2 baseline, clause 252.240-7997. https://www.acq.osd.mil/dpap/dars/classdev/DFARS_RFO/Part-240/2026-O0025_Rev3_TAB_A_Deviation_Memo.pdf

NI01 NIST SP 800-171 Revision 2. Technical standard publication page. 110 security requirements; the revision CMMC incorporates. https://csrc.nist.gov/pubs/sp/800/171/r2/upd1/final

NI02 NIST SP 800-171 Revision 3. Technical standard publication page. Published May 2024; CMMC and DFARS 252.204-7012 still use Revision 2. https://csrc.nist.gov/pubs/sp/800/171/r3/final

NI03 NIST SP 800-171A Revision 3. Technical assessment guidance. Examine, interview and test procedures; pair with the matching requirement revision. https://csrc.nist.gov/pubs/sp/800/171/A/r3/final

NI04 NIST SP 800-86. Technical forensic guidance. Sections 3 to 6; collection, data files, operating systems, network or application sources. https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-86.pdf

NI05 NIST SP 800-115. Technical testing guidance. Assessment planning, logistics, rules of engagement and reporting. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf

NI06 NIST Cybersecurity Framework 2.0. Voluntary risk framework. Govern, Identify, Protect, Detect, Respond, Recover. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

© 2026 Global Digital Forensics, Inc. All rights reserved.

EA01 EAR scope. Federal regulatory compilation. 734.3, 734.13 to 734.19; jurisdiction, releases and conditional encrypted transmission. https://www.ecfr.gov/current/title-15/subtitle-B/chapter-VII/subchapter-C/part-734

EA02 EAR recordkeeping. Federal regulatory compilation. 762.2, 762.6; records and retention trigger. https://www.ecfr.gov/current/title-15/subtitle-B/chapter-VII/subchapter-C/part-762

EA03 BIS export compliance programs. Agency program guidance. Eight elements of an export compliance program. https://www.bis.gov/learn-support/export-compliance-programs

EA04 BIS export compliance toolkit. Agency guidance index. Classification, screening, technology controls and self audit modules. https://www.bis.gov/learn-support/export-compliance-programs/export-compliance-toolkit

EA05 EAR end user and end use controls. Federal regulatory compilation. Transaction specific end user or end use controls. https://www.ecfr.gov/current/title-15/subtitle-B/chapter-VII/subchapter-C/part-744

IT01 ITAR definitions. Federal regulatory compilation. 120.31 to 120.33 and 120.50 to 120.63. https://www.ecfr.gov/current/title-22/chapter-I/subchapter-M/part-120

IT02 ITAR encrypted technical data provision. Federal regulatory compilation. 120.54(a)(5), (b) and (c). https://www.ecfr.gov/current/title-22/chapter-I/subchapter-M/part-120/subpart-C/section-120.54

IT03 ITAR registration and recordkeeping. Federal regulatory compilation. 122.1 registration and 122.5 recordkeeping. https://www.ecfr.gov/current/title-22/chapter-I/subchapter-M/part-122

IT04 DDTC understanding ITAR. Agency jurisdiction guidance. ITAR parts 120 to 130, USML, defense services and brokering. https://www.pmddtc.state.gov/ddtc_public/ddtc_landing?id=ddtc_public_portal_itar_landing

IT05 DDTC registration explanation. Agency registration guidance. Registration process; under 22 CFR 122.1(c) registration is generally a precondition to the issuance of a license or other approval. https://www.pmddtc.state.gov/registration/documents/DS2032v4.4.pdf

LG01 Federal Rules of Civil Procedure (December 1, 2025). Court procedural rules. Rules 26, 33, 34, 37(e) and 45. https://www.uscourts.gov/sites/default/files/document/federal-rules-of-civil-procedure.pdf

LG02 Federal Rules of Evidence. Court procedural rules index. Rules 502, 901 and 902. https://www.uscourts.gov/forms-rules/current-rules-practice-procedure/federal-rules-evidence

HE01 HIPAA Security Rule. Federal regulatory compilation. 164.308(a)(1), 164.312(b) and 164.316. https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C/part-164/subpart-C

HE02 HIPAA judicial proceedings provision. Federal regulatory compilation. 164.512(e) disclosures for judicial and administrative proceedings. https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C/part-164/subpart-E/section-164.512

HE03 HHS court orders and subpoenas. Agency interpretation. Court orders compared with other subpoenas. https://www.hhs.gov/hipaa/for-individuals/court-orders-subpoenas/index.html

HE04 HHS medical record retention FAQ. Agency interpretation. The Privacy Rule sets no general medical record retention period. https://www.hhs.gov/hipaa/for-professionals/faq/does-hipaa-require-covered-entities-to-keep-medical-records-for-any-period/index.html

HE05 HHS Part 2 confidentiality. Agency interpretation. 2024 final rule; compliance date February 16, 2026; proceedings against a patient. https://www.hhs.gov/hipaa/part-2/index.html

© 2026 Global Digital Forensics, Inc. All rights reserved.

HE06 ONC auditable events certification guidance. Agency certification guidance. 170.315(d)(2) auditable events and tamper resistance. https://healthit.gov/test-method/auditable-events-and-tamper-resistance/

HE07 Substance use disorder record regulation. Federal regulatory compilation. 42 CFR Part 2; consent and use in proceedings. https://www.ecfr.gov/current/title-42/chapter-I/subchapter-A/part-2

MS01 Microsoft eDiscovery data sources. Vendor documentation. Mailbox, OneDrive, SharePoint locations; source specific inclusion. https://learn.microsoft.com/en-us/purview/edisc-data-sources

MS02 Microsoft Teams content in eDiscovery. Vendor documentation. Compliance records, files, channels, recordings and known exclusions. https://learn.microsoft.com/en-us/purview/edisc-search-teams

MS03 OneDrive retention and deletion. Vendor documentation. Deleted users, unlicensed archives, retention or hold and recycle bin limitations. https://learn.microsoft.com/en-us/onedrive/retention-and-deletion

MS04 Microsoft audit retention. Vendor documentation. Audit retention policies by license; check the tenant configuration. https://learn.microsoft.com/en-us/purview/audit-log-retention-policies

MS05 SharePoint and OneDrive retention. Vendor documentation. Preservation Hold library, versions and recycle bin search limits. https://learn.microsoft.com/en-us/purview/retention-policies-sharepoint

MS06 Microsoft eDiscovery process reports. Vendor documentation. Search or export scope, location counts, errors and completeness limits. https://learn.microsoft.com/en-us/purview/edisc-process-report

GO01 Google Vault overview. Vendor documentation. Supported services, licenses, retention rules and holds. https://support.google.com/vault/answer/2462365?hl=en

GO02 Google audit lag and retention. Vendor documentation. Retention and reporting lag for each log type. https://support.google.com/a/answer/7061566?hl=en

SL01 Slack Discovery APIs. Vendor documentation. Enterprise, approved applications, preserved content and export scope. https://slack.com/help/articles/360002079527-a-guide-to-slacks-discovery-apis

SL02 Slack Connect data management. Vendor documentation. External organization ownership, export exclusions and retention. https://slack.com/help/articles/115004152843-How-data-management-features-apply-to-Slack-Connect

AW01 AWS CloudTrail event history. Vendor documentation. 90 day regional management event history; data events are excluded. https://docs.aws.amazon.com/awscloudtrail/latest/userguide/view-cloudtrail-events.html

DS01 Docusign history and completion certificate. Vendor documentation. Envelope history and certificate of completion. https://support.docusign.com/s/document-item?bundleId=oeq1643226594604&topicId=hha1578456343641.html&language=en_US

CL01 Clio matter export scope. Vendor documentation. What a matter export contains and the separate subtabs. https://help.clio.com/hc/en-150/articles/9286116462747-Filter-Export-and-Convert-Matters

CL02 Clio text message exports. Vendor documentation. Text message export to PDF. https://help.clio.com/hc/en-us/articles/9125220988827-Text-Messaging-in-Clio-Manage

FT01 FTC Safeguards Rule business guidance. Agency guidance. Covered financial institutions and limited exemptions. https://www.ftc.gov/business-guidance/resources/ftc-safeguards-rule-what-your-business-needs-know

© 2026 Global Digital Forensics, Inc. All rights reserved.

FP01 FedRAMP authorization explanation. Agency program index. Cloud service authorization. https://www.fedramp.gov/

DFS07 23 NYCRR 500.12 and 500.17 (Cornell LII text). Regulatory text. 500.12(a) multifactor authentication; 500.17(a)(1) 72 hour notice, 500.17(b) April 15 filing, 500.17(c) extortion payment notice. https://www.law.cornell.edu/regulations/new-york/23-NYCRR-500.17

LG03 Defend Trade Secrets Act, 18 U.S.C. 1836 and 1839. Federal statute. 1836(b) civil action and seizure, 1836(d) three year limitation, 1839(3) trade secret, 1839(5) misappropriation. https://www.govinfo.gov/content/pkg/USCODE-2023-title18/html/USCODE-2023-title18-partI-chap90-sec1839.htm

© 2026 Global Digital Forensics, Inc. All rights reserved.

Talk to a senior examiner

Global Digital Forensics has supported counsel, compliance teams and IT security teams since 1992 with forensic examinations, collections and expert analysis. If a package raises a question about preservation, collection or analysis, a senior examiner can help you scope the next step.

Get a free consultation. The initial consultation is free, and requests are handled in confidence.

Call (800) 868-8189 at any hour, or write to info@evestigate.com.

Request a consultation online at evestigate.com/contact.

© 2026 Global Digital Forensics, Inc. All rights reserved.