Global Digital Forensics · Guide edition 2026-11-03 · evestigate.com/resources/audit-discovery-preparation/02-ny-private-information/

AUDIT AND DISCOVERY PREPARATION

New York private information gathering package

Organize New York private information records, data maps, safeguards and breach facts for a privacy or cybersecurity specialist.

Find where New York residents information is held and assemble existing safeguards and incident records for a privacy or cybersecurity specialist.

Owners, lawyers, privacy and risk managers, office administrators and client IT

General Business Law 899-aa and 899-bb preparation, with a separate branch for state entities and sector specific obligations. It prepares records for a specialist's review under those specific laws.

Before you gather

PII is a useful broad working label for the first pass. New York statutory private information under 899-aa has a particular definition, while DFS nonpublic information and HIPAA protected health information have different scopes, and a specialist will classify against each definition separately. Inventory the actual fields and the combinations in which they are stored before anyone makes the legal classification, because the classification turns on combinations rather than on field names.

The current 899-aa text reviewed includes medical and health insurance information as well as the specified identifiers, financial access information, biometrics and online credentials. A strong first inventory covers each of those categories and reaches well beyond Social Security and credit card numbers. For owners and licensees, 899-aa(2) uses prompt notice with a 30 day outer limit after discovery, subject to its terms. The maintainers branch in 899-aa(3) calls for immediate notice to the owner or licensee, again with a 30 day limit. These clocks are distinct from the DFS incident and payment clocks, so obtain the dates and the decisions, and counsel makes the notice determination from them.

899-bb has a safeguard compliance route for a person subject to and in compliance with specified regulatory regimes, so the file pairs the regulated status with the evidence of compliance with the named regime, which the specialist will ask to see. Its small business provision tailors safeguards to the business, so a small business gathers the records of the safeguards it keeps. State Technology Law 208 is a separate branch with its own state entity definition and local government provisions, so that branch is built from its own text, with its own definitions, deadlines and recipients. General hospitals, schools, employers, financial firms and government bodies may need additional specialist modules.

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

Give each request to the suggested owner. Record each answer, including the items awaiting confirmation, in the editable CSV checklist. Keep the records themselves in a secure evidence location agreed with the recipient and use the checklist as the index that points to them; passwords stay with their owners, and real patient data and controlled technical information stay in the secure location.

Records to find

CSV files hold plain records, and your spreadsheet sets the layout. Import as UTF-8, keep IDs as text, wrap text and widen columns before use. Blank client fields are intentional.

NY-R01 Organization and legal context

Ask
Legal or business owner

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

Where to ask
Corporate files and business sponsor

Why it may be needed
Routes the facts to the right law and sector.

If missing or uncertain
Ask counsel which regime applies, and mark the branch pending until the answer comes back.

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

NY01 NY02 NY03

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 may be needed
Supports classification while the checklist holds only field names and masked samples.

If missing or uncertain
Name the owner who can supply a schema or masked example, and record counts as the owner reports them.

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

NY01 NY02 DFS01

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

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 may be needed
Looks for extra copies and processors beyond the device list.

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

Reference: NY02 2(b)

NY02

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 may be needed
Organizes administrative safeguard records for the recipient.

If missing or uncertain
Name the person who may have records; the specialist makes any control finding after that person has been asked.

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

NY02

NY-R05 Personnel and supplier safeguards

Ask
HR and procurement

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

Where to ask
HR, procurement, provider agreements

Why it may be needed
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.

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

NY02

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

NY-R06 Technical protection records

Ask
IT and service providers

Gather
Access/MFA scope, secure configurations, patch/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 may be needed
Lets the consultant assess existing technical safeguards.

If missing or uncertain
Request a scoped explanation of records held elsewhere or by providers; any new testing starts with written authorization.

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

NY02

NY-R07 Physical records and disposal

Ask
Facilities and records manager

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

Where to ask
Facilities, offsite storage and media vendor

Why it may be needed
Covers paper, portable media and disposal alongside cloud security.

If missing or uncertain
List the storage sites and providers to contact next.

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

NY02

NY-R08 Incident facts and chronology

Ask
Legal and incident owner

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

Where to ask
Restricted incident file

Why it may be needed
Supports legal notice analysis with open facts clearly marked.

If missing or uncertain
Escalate live matters, and label suspected facts and dates as awaiting confirmation.

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

NY01 NY03

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

NY-R09 Notification and decision file

Ask
Legal and compliance

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

Where to ask
Counsel and incident correspondence

Why it may be needed
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.

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

NY01

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 may be needed
Supports the specific 899-bb route with the compliance records that sit behind the regulated status.

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

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

NY02

NY-R11 Government and sector routing

Ask
Legal or privacy lead

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

Where to ask
Legal records and sector owner

Why it may be needed
Identifies which specialist should add a tailored module.

If missing or uncertain
Build any hospital requirement list from the current 10 NYCRR 405.46 text.

Reference: NY03; NY04; HE01; DFS01

NY03 NY04 HE01 DFS01

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

NY-R12 Gaps and transmittal

Ask
Coordinator

Gather
Completed source inventory, request responses, periods to cover next, access restrictions and named follow up owners.

Where to ask
This package and receiving specialist

Why it may be needed
Creates an honest, navigable handoff.

If missing or uncertain
Keep the Unknown and Partially received statuses visible, and ask the recipient which open item comes first.

Reference: Preparation method; NY02

NY02

Questions for client IT and owners

A useful answer names the actual system, period, supporting record and its coverage. Where the answer sits with someone else, name the person or provider who can give it.

1. What exact information fields and combinations do you hold about New York residents?

Suggested responder
Client IT or system owner

Useful supporting record
Schema and masked examples, including credentials, medical and health insurance fields.

2. Which outside parties hold the same information or additional copies?

Suggested responder
Client IT or system owner

Useful supporting record
Provider list, contracts, tenants, exports and return/deletion terms.

3. What can you say about encryption and who could obtain the decryption keys?

Suggested responder
Client IT or system owner

Useful supporting record
Configuration description and responsible owner.

4. Which safeguards were in operation during the period, rather than added later?

Suggested responder
Client IT or system owner

Useful supporting record
Dated settings, reports, tickets and change history.

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

5. Are accounts, archives, paper stores or backups outside the main system inventory?

Suggested responder
Client IT or system owner

Useful supporting record
One inventory row for each actual location and owner.

6. If an incident is relevant, what happened, when was each fact learned and which questions are open?

Suggested responder
Client IT or system owner

Useful supporting record
Counsel approved chronology with evidence pointers.

7. What records were already supplied to a regulator, insurer or prior assessor?

Suggested responder
Client IT or system owner

Useful supporting record
Copies, scope and receipts subject to authorized disclosure.

8. Which people can explain a record being traced or a technical constraint?

Suggested responder
Client IT or system owner

Useful supporting record
Contact roster and next action per open item.

Facts to confirm and specialist decisions

These are explicit handoff questions, and each one closes with the specialist's written answer, drawing on the records marked Received. Add client specific questions and a responsible person.

NY-Q01 Which statutory definition and organizational branch apply?

Ask
Counsel and privacy specialist

Gather
Entity status, fields, residents, sector licenses and contracts

Resolution needed
Written scope and definitions for the actual recipient.

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

NY-Q02 Which additional sector or other state modules are necessary?

Ask
Legal team and specialist

Gather
Business locations, customers, patients, students, contracts and regulator orders

Resolution needed
A named list of additional work for each further state or sector in scope.

Preparing the handoff

The handoff is ready when the data map uses actual fields and repository owners rather than a generic PII label; when the government, DFS and healthcare branches are kept separate; when any active incident has been escalated outside the ordinary preparation schedule; and when the specialist receives a record index, masked examples and explicit scope notes, with the records themselves held in the agreed secure location.

Sources for this package

Official laws/rules establish duties within their scope. Guidance explains programs; NIST supplies methods; vendor documentation describes possible product behavior. The package works alongside the actual contracts, facts, configuration and case orders.

- DFS final adopted second amendment to Part 500 (DFS01)
- New York General Business Law 899-aa (NY01)
- New York General Business Law 899-bb (NY02)
- New York State Technology Law 208 (NY03)
- New York hospital cybersecurity rule (NY04)
- HIPAA Security Rule (HE01)
- FTC Safeguards Rule business guidance (FT01)

Bring the completed pack to a free scoping call and a senior examiner sets the scope from it. Call (800) 868-8189.

Source review date: October 18 2026.

Reviewed by Joseph Caruso, Founder, CEO and CTO, CISSP. Last reviewed November 3, 2026.

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

Start With a Free Consultation

The initial consultation is free, and requests are handled in confidence. On the first call a senior member of our team listens to the question you need answered, identifies the records and systems involved, and recommends the next step.

Call (800) 868-8189, answered 24/7, request a consultation at evestigate.com/contact, or email info@evestigate.com.

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