COMPLIANCE DATASHEET

HIPAA and Your ServiceNow Data

How Rezilient Restore helps covered entities and business associates back up, restore and test the ePHI in ServiceNow under the HIPAA Security Rule.

45 CFR PART 164, SUBPART C | SECTIONS 164.308, 164.312 AND 164.316 | MAPPED TO REZILIENT RESTORE

WHY SERVICENOW IS IN SCOPE

Backup is a required implementation specification

The Security Rule applies to covered entities and their business associates. Its contingency plan standard, §164.308(a)(7), requires a data backup plan, a disaster recovery plan and an emergency mode operation plan for electronic protected health information.

HR cases, member interactions and clinical workflow data put ePHI inside ServiceNow. ServiceNow protects the platform, and its native backup is built for infrastructure disaster recovery, with a 14-day window and full-instance restore. The ePHI inside it is your responsibility.

> "Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information."
>
> 45 CFR §164.308(A)(7)(II)(A) · REQUIRED

6 years
Retention of Security Rule documentation.
§164.316(b)(2)(i)

3 of 5
Contingency plan specifications marked Required.
§164.308(a)(7)

14 days
ServiceNow's native backup window, built for platform disaster recovery.
ServiceNow platform documentation

REQUIREMENT TO CAPABILITY

Contingency plan standard · continued on page 2

SECTION	HIPAA REQUIREMENT	REZILIENT RESTORE CAPABILITY
§164.308(a)(7)(ii)(A)	**Data backup plan** Procedures to create and maintain retrievable exact copies of ePHI. Required.	**Continuous, full-fidelity capture.** Every change to protected tables is captured with its relationships, attachments and history, and stored immutably off the platform.
§164.308(a)(7)(ii)(B)	**Disaster recovery plan** Establish (and implement as needed) "procedures to restore any loss of data". Required.	**Restore exactly what was lost.** Record, field or table restore, without rolling back the instance and every other team's work.
§164.308(a)(7)(ii)(C)	**Emergency mode operation plan** Continue critical business processes and protect ePHI while operating in emergency mode. Required.	**A copy outside the blast radius.** If the instance is compromised, the copy and the restore path stay outside the attacker's reach.
§164.308(a)(7)(ii)(D)	**Test the plans** Periodic testing and revision of contingency plans. Addressable.	**Restore tests you can actually run.** A surgical restore in a non-production instance, with the result exported as evidence.
§164.308(a)(7)(ii)(E)	**Rank applications and data** Assess the relative criticality of specific applications and data. Addressable.	**Coverage you can see.** The Coverage Gaps dashboard shows which tables, attachments and applications are in or out of the backup set.

REQUIREMENT TO CAPABILITY, CONTINUED

Sections 164.312 and 164.316

SECTION	HIPAA REQUIREMENT	REZILIENT RESTORE CAPABILITY
§164.312(c)(1)	**Protect integrity** Policies and procedures to protect ePHI from improper alteration or destruction.	**Pre-state and post-state for every record.** Point-in-time history shows what changed and when, and any record can be put back.
§164.312(a)(2)(iv)	**Encrypt ePHI** A mechanism to encrypt and decrypt ePHI. Addressable.	**Keys stay with you or ServiceNow.** AES-256 (NIST FIPS 197) in transit and at rest, with keys held only by you or ServiceNow. Rezilient can never read your data.
§164.316(b)(2)(i)	**Keep documentation six years** Retain required documentation for six years from creation or the date last in effect, whichever is later.	**Retention set to the rule.** Per-table retention keeps contingency records and test evidence for the period HIPAA names.

Four questions OCR could ask

Q1
Exact copies
Where is the retrievable exact copy of the ePHI in ServiceNow, and who controls it?

Q2
Restore
When did you last restore ePHI from that copy, and how long did it take?

Q3
Emergency mode
If the instance is unavailable or compromised, can you still reach a protected copy?

Q4
Documentation
Can you produce six years of contingency plan documentation and test records on request?

How it works

01
Connect
Install in ServiceNow and link off-platform storage. Live in under one business day.

02
Capture
Continuous, schema-aware change capture across ITSM, CMDB, HRSD, CSM, GRC, SecOps and custom tables.

03
Restore
Record, field, table or workflow level, inside the native ServiceNow experience.

04
Prove
Chain-of-custody exports and audit-ready evidence on demand.

Enforcement screen. Regulators have announced 58 public actions and settlements that cite HIPAA against 39 organizations we have confirmed as ServiceNow customers, about $264 million in total (2008 to 2026). These are evidence of regulatory exposure, not a claim that ServiceNow data was involved. Source: Rezilient review of public regulator records, 31 Oct 2026.

What this datasheet does not claim. No product makes an organization HIPAA compliant on its own. The Security Rule covers administrative, physical and technical safeguards, from risk analysis and workforce training to access controls and audit logs. Rezilient Restore supports the contingency plan standard, integrity and documentation retention for the ePHI in ServiceNow.

Run a real restore test in 30 days

The 30-day Rezilient Restore trial runs in your non-production instance, live in under one business day, with no commitment. You keep the evidence.

Back Up Now →

rezilient.co/contact-us

Requirement text is summarized from the HIPAA Security Rule, 45 CFR Part 164, Subpart C; quoted text is verbatim. This datasheet is for information only and is not legal advice. ServiceNow and Now Assist are trademarks of ServiceNow, Inc.
© 2026 Rezilient Corp. · Naples, FL · info@rezilient.co · rezilient.co/compliance/hipaa · v1.4 · 2 / 2

Back Up Now. Restore Anytime. Always Rezilient.