Recovery evidence map: hospitals and health systems

What an assessor would ask to see, under the HIPAA Security Rule

Saying you have backups is not the same as showing a dated record of them. This map takes each recovery item in the HIPAA Security Rule's contingency plan standard, says in plain words what an auditor or assessor would ask to see, and leaves room for whether your own process produces it and where it is kept.

Before you start

Required and addressable.
Required items must be in place. Addressable does not mean optional: you assess whether the item is reasonable and appropriate for you, and if it is not, you write down why and put an equal alternative in place where that is reasonable.

A working map.
This is a working map for your own records, not a compliance opinion or legal advice. Your compliance and legal teams decide what meets the rule.

The rule as it stands today.
The January 2025 proposed changes are on the back. They are not in force, and nothing on this side comes from them.

The rule's recovery items

1 Data backup plan (Required)

Exact copies of patient data that can be retrieved. Asked to see: the written backup procedure, which systems holding patient data it covers, and job records showing copies were made.

Does your process produce it? Yes, partly or no	Where it is kept, and its date

2 Disaster recovery plan (Required)

Procedures to restore lost data. Asked to see: the written restore procedure, and records of restores actually done, with dates and how long they took.

Does your process produce it? Yes, partly or no	Where it is kept, and its date

3 Emergency mode operation plan (Required)

Keeping critical work going, with patient data protected, while systems are down. Asked to see: downtime procedures and who decides to switch to them.

Does your process produce it? Yes, partly or no	Where it is kept, and its date

4 Testing and revision (Addressable)

Testing the plans from time to time and updating them. Asked to see: dated test records and results, the changes made after, or the written reason and the alternative.

Does your process produce it? Yes, partly or no	Where it is kept, and its date

5 Applications and data criticality (Addressable)

Ranking which systems and data matter most. Asked to see: the ranked list, and how it set the order systems come back in.

Does your process produce it? Yes, partly or no	Where it is kept, and its date

6 Documentation, kept 6 years (Required)

The written policies and records, kept 6 years from when made or last in effect, available to the people who use them, reviewed. Asked to see: where they live and their dates.

Does your process produce it? Yes, partly or no	Where it is kept, and its date

> If an assessor asked for your last restore test today, how long would it take to find the record?

The proposed changes, and what this map does not prove

In January 2025 HHS published proposed changes to the HIPAA Security Rule in the Federal Register. As of October 27, 2026 they are still only proposed: no final rule or withdrawal has been published, and the current text has not changed. Among other things, the proposal would make every implementation specification required, with limited exceptions, and would ask for written procedures to restore critical systems and data within 72 hours. None of that applies today. If it is finalized, this map changes with it.

> Who on your team owns each row, and do they know it?

What this does not prove

That you comply. It is a working map, not a compliance opinion or legal advice.

That the evidence is enough. A record shows the process ran. Whether it meets the rule is for your compliance and legal teams.

That recovery works. A written plan and a job report are not a restore. Only a timed restore shows that.

Anything past recovery. The rule has other standards. This map covers the contingency plan and its documentation only.

Words used here

Patient data
electronic protected health information (ePHI), the records the rule protects.

Implementation specification
the rule's name for each item under a standard, marked required or addressable.

Assessor
anyone checking your controls against the rule: an auditor, a regulator or an outside reviewer.

Emergency mode
running the organization while key systems are down.

Sources

- eCFR, 45 CFR 164.308(a)(7), text as amended January 2013, current as of October 23, 2026.
- eCFR, 45 CFR 164.306(d) and 164.316(b), as amended January 2013.
- Federal Register, proposed rule 2024-30983 (January 6, 2025); status checked October 27, 2026.

Made by StepKnock, a small team in San Diego, paid through our partners when a customer buys. This page sells nothing.

Nothing to sign up for. No cookies, no analytics, and nothing you type here leaves this page.

stepknock.com/toolkit/checks/evidence-map-hospitals/