COMMUNITY HEALTH CARE ASSOCIATION of New York State

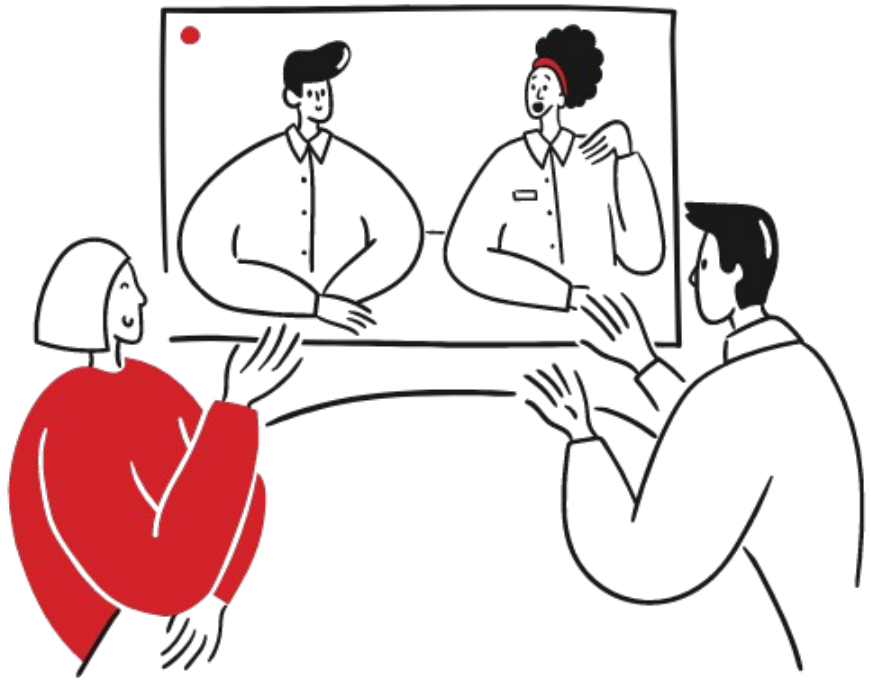
A CHCANYS NYS-HCCN funded webinar with Truvantis, Inc.

Disaster Recovery and Operational Resilience: Planning to Keep Running and Recover Faster

July 29, 2026

Zoom Guidelines

- Please share your questions in the chat. CHCANYS staff will raise your questions to our speakers and follow up as needed if there are unanswered questions.
- The session is being recorded and materials will be shared after the session.



COMMUNITY HEALTH CARE ASSOCIATION of New York State

Jerrod Montoya, JD, CIPP/US

Principal Security Consultant & General Counsel

Truvantis, Inc

COMMUNITY HEALTH CARE ASSOCIATION of New York State chcanys.org

Disclaimer

General education, not legal advice

- This presentation is for general education and is not legal advice.
- Consult your own counsel and compliance staff on how it applies to your organization.
- This is not a HIPAA compliance course. HIPAA is a supporting reference and the compliance floor, not the subject.

THE BIG PICTURE

Overview

Every practice sharpens your view of risk. Start with the Business Impact Analysis (BIA).

PILLAR 1: BIA

Why the BIA Comes First

You can plan without a BIA. In a live event, the cost of having guessed compounds fast.

A good BIA targets everything downstream

- What to keep running, and what can wait.
- What to back up, and in what order to restore it.
- Which backups and which scenarios are worth testing.

Better data in the BIA means higher quality in every plan, test, and risk decision.

Source: *Applications and data criticality analysis, 45 CFR 164.308(a)(7)(ii)(E), Addressable.*

PILLAR 1: BIA

What a Business Impact Analysis Produces

Inventory

- List the systems and applications that touch patient care and ePHI.

Rank by impact

- How badly does losing each one hurt care, not just administration?

Set downtime tolerance

- How long can you run without each one? That becomes your recovery target.

Answer these for your own center. The result is your ranking, and it drives everything downstream.

PILLAR 2: PLAN

Keep Operating When Systems Go Down

Plan to deliver care while systems are down, with ePHI still protected.

Downtime procedures

- How the center runs on manual and paper workflows.

Paper is still PHI

- The same protection, storage, and later reconciliation.

Alternate communication

- How the team coordinates when the usual tools are down.

Source: *Emergency mode operation plan, 45 CFR 164.308(a)(7)(ii)(C), Required.*

PILLAR 2: PLAN

Who Has Authority: Define the Role, Not a Name

1

Define the role

- Decide in advance what the role can authorize, not who fills it.

2

Whoever is present

- Whoever is present and capable takes the role when a disruption starts.

3

Hand off cleanly

- When someone better positioned arrives, transfer with a short briefing.

Source: *Best practice, drawn from federal emergency-management practice (FEMA and NIMS incident command).*

PILLAR 2: PLAN

Back Up, Then Restore in Priority Order

Back up

- Retrievable, exact copies of ePHI.
- Three copies, two media types, one off-site.

Then restore

- Restore is the act, not the copy.
- Bring care systems back first, by the BIA ranking.

Back up what the BIA ranked, and restore it in that order.

Source: *Data backup plan (A) and disaster recovery plan (B), 45 CFR 164.308(a)(7)(ii), both Required.*

PILLAR 2: PLAN

Ransomware: Immutable and Offline Copies

Ransomware targets connected backups first. If the only backup is reachable, ransomware takes it too.

Immutable copies

- Cannot be altered or deleted for a set period.

Offline or air-gapped

- Unreachable from the network, so an attack cannot reach it.

Source: *Best practice. These methods make retrievable backups real under a destructive attack.*

PILLAR 3: TEST

Test the Plans and the Restores

A plan or a backup you have never tested is an assumption.

Tabletop the plan

- A facilitated discussion, not a technical drill. A room, a scenario, a couple of hours.

Test the restore

- Recover a real record sample and time it against your target.

Near zero cost

- No systems touched, no budget required, and it finds the gaps first.

Source: *Testing and revision procedures, 45 CFR 164.308(a)(7)(ii)(D), Addressable.*

PILLAR 3: TEST

Find the Gaps, Then Fix the Plan

What a test reveals

- Unclear authority
- Stale contact lists
- Undocumented steps
- Over-optimistic recovery times

What to do about it

- Revise the plan while it is fresh
- Re-test the parts that failed
- Update the BIA if priorities shifted

Testing and revision are one loop. What you learn goes straight back into the plan.

ON THE HORIZON

Where This Is Heading: Proposed HIPAA Changes

Proposed, not final. The timeline is uncertain and has recently been delayed.

72-hour restoration

- Restore certain critical systems and data within 72 hours.

Two items become required

- Criticality analysis and testing would move from addressable to required.

Faster vendor notice

- Business Associates would give 24-hour notice on activation.

Source: *2025 HIPAA Security Rule NPRM, 90 FR 898 (proposed, not final).*

TAKEAWAYS

Key Takeaways

1

Start with the BIA, the foundation

- Know what is critical first. A better BIA means stronger plans, tests, and risk decisions.

2

Plan to keep running, and to recover

- Keep operating through the disruption, then restore in priority order.

3

Test the plans and the restores

- Tabletop both and fix what the test surfaces.

Workshop Evaluation Survey

SCAN QR CODE

Please share your feedback on this session. This should take less than 3 minutes to complete.

Survey Link: https://forms.office.com/r/tj5XRbheRZ