COMMUNITY HEALTH CARE ASSOCIATION of New York State

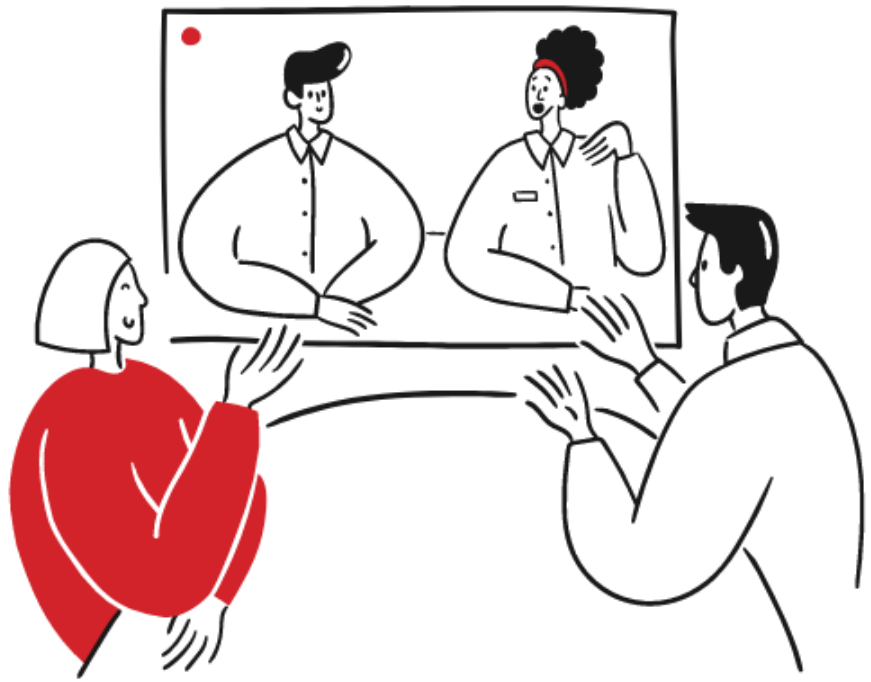
A CHCANYS NYS-HCCN funded webinar with Truvantis, Inc.

Incident Response Planning: Preparing for the Breach You Didn't See Coming

July 8, 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:

The following presentation is for informational purposes only and not intended as legal advice.

Please consult your lawyer for legal questions on how this information relates to your specific situation.

HIPAA requires a written plan so you can respond to an incident

An incident response plan is not a script for the incident you predicted.

It is preparation for the one you didn’t.

One incident, three regulatory questions

Security incident

The broadest category. Attempted or successful unauthorized access to systems or PHI. Most incidents stop here. 45 CFR 164.308(a)(6).

Breach

A subset: unsecured PHI acquired, accessed, used, or disclosed. You decide with a documented risk assessment. 45 CFR 164.402.

Notification

Only when it is a breach. Clocks run to individuals, to HHS, and sometimes to the media. 45 CFR 164.404 to 164.410.

Most incidents are never breaches. The plan is the architecture that sorts them, so the call is reliable instead of improvised.

Source: 45 CFR 164.304, 164.308(a)(6), 164.402, 164.404-410 (eCFR, HIPAA Security and Breach Notification Rules)

What is a security incident?

WHAT THE LAW SAYS

45 CFR 164.304 (definition)

“The attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.”

Source: 45 CFR 164.304 (security incident, definition) · 45 CFR 164.308(a)(6) (security incident procedures) (eCFR)

The rule requires procedures, and defines their job

WHAT THE LAW SAYS

45 CFR 164.308(a)(6)(i)

Implement policies and procedures to address security incidents. This is a required standard, not a best practice you may skip.

WHAT THE PROCEDURES MUST DO

Response and Reporting, 164.308(a)(6)(ii)

Identify and respond to suspected or known incidents. Mitigate their harmful effects, to the extent practicable. Document each incident and its outcome.

Source: 45 CFR 164.308(a)(6) (security incident procedures) (eCFR)

Get the incident reported

Set the threshold low

Workforce reports on suspicion, not proof. A missed report is a missed clock.

Name the path and the owner

One place to report, one role that owns the next step. Written down, not assumed.

Your carrier has a clock too

Prompt notice is often a condition of coverage. Confirm the terms with your broker or counsel.

Before you know whether it is a breach, the plan is already moving.

Determining a breach: the risk assessment

1. **Nature and extent of the PHI**
2. **Who received or used it**
3. **Whether it was actually acquired or viewed**
4. **How far the risk was mitigated**

The floor, not the whole test. An impermissible use or disclosure of unsecured PHI is presumed a breach unless a documented risk assessment shows a low probability of compromise. The rule requires at least these factors, not only these. The burden of proof is on the covered entity, and the assessment is kept for six years.

Source: 45 CFR 164.402(2) (risk assessment) · 164.414(b) (burden) · 164.530(j) (six-year retention) (eCFR)

The notification clock starts at discovery

60

calendar days to notify individuals

Notify affected individuals “without unreasonable delay and in no case later than 60 calendar days after discovery of a breach.” Discovery is when you knew, or by reasonable diligence should have known.

Discovery, not confirmation. The clock can start before your investigation is finished. A slow start burns days you cannot get back.

Source: 45 CFR 164.404 (notification to individuals); 45 CFR 164.404(a)(2) (discovery) (eCFR)

The clocks you answer to, side by side

ONE CLOCK BELOW IS PROPOSED. NPRM 90 FR 898, not in force. The other two are current law.

1

Individuals, and HHS at 500+

60 days from discovery. HHS notice is contemporaneous at 500 or more, an annual log below that. Current law. 45 CFR 164.404, 164.408.

2

Your BA reports to you

Without unreasonable delay, and no later than 60 days. Current law. 45 CFR 164.410.

3

Contingency activation (PROPOSED)

Report up the chain within 24 hours of activating a contingency plan. Proposed only, not in force. 45 CFR 164.314(a)(2)(i)(D).

Calling your cyber insurer is not on this list. Carrier notice protects coverage; it does not satisfy any HIPAA clock.

What a missed notification actually costs

$475K

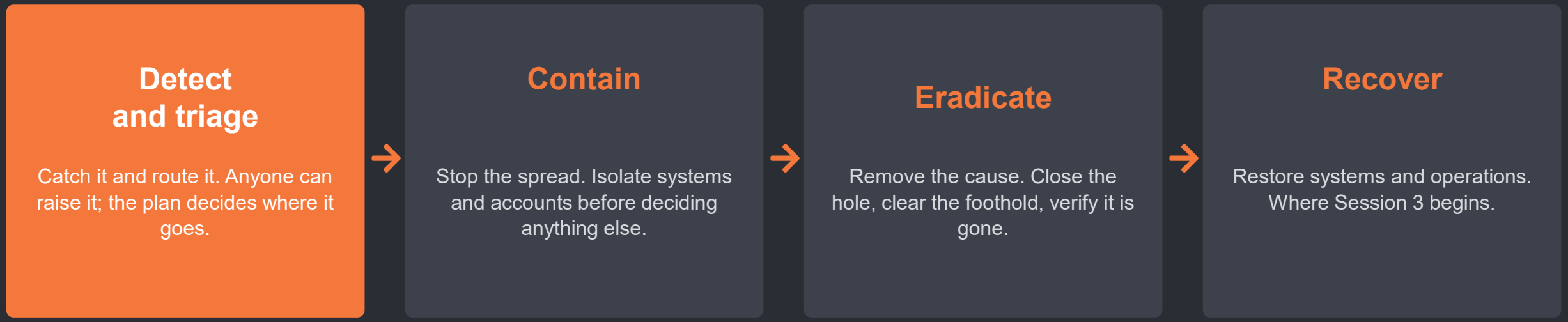
for notifying 836 people too late

Presence Health, 2017. The first OCR settlement for delayed breach notification. A breach affecting 836 individuals, where individuals, the media, and OCR were not notified within the 60-day window.

The lesson: the penalty turned on the delay, not the size of the breach. A plan that stalls between discovery and notification is where the cost lands.

Source: HHS OCR Resolution Agreement, Presence Health Network, 2017 (hhs.gov)

A usable plan sorts, then acts



The compliance track, assess whether it is a breach and notify on the clocks, runs in parallel, coordinated by the Incident Manager. Containment does not wait for the breach call. (NIST SP 800-61; CISA.)

What a minimum viable plan contains

1. Roles and contacts: who leads, who to call, kept current and printed offline.
2. A reporting threshold: what staff report, and to whom, on suspicion.
3. A breach-decision step: the risk assessment, and who runs it.
4. Notification triggers and clocks: individuals, HHS, media, and your carrier.
5. Documentation: the timeline, the decisions, and the after-action as your evidence.
6. Response steps: how you contain, eradicate, and recover.

Someone has to run the incident

INCIDENT MANAGER

Leads the response. No hands-on tech.

Runs the response and watches the clock. Under stress, people lose track of how long things are taking.

TECH AND COMMS

Two more roles the plan names in advance.

The Technical Manager runs containment, eradication, and recovery. The Communications Manager runs notification. The Incident Manager keeps both tracks moving. A small center can combine roles, but name them before the incident.

Source: CISA, Incident Response Plan (IRP) Basics (cisa.gov)

A runbook helps. A script for the whole incident does not.

TASK-LEVEL RUNBOOK

- Isolate a host
- Reset credentials
- Pull the right logs

EVENT-LEVEL SCRIPT

- Assumes the incident you pictured
- Breaks on the one you get
- Trains no judgment

Automate the tasks you can name. Do not script the incident you cannot predict. That difference is the whole point of the plan.

The plan is never finished

START HERE

CISA IRP Basics

Roles, a reporting path, and a tested habit. Enough to be useful now.

GROWS TOWARD

NIST SP 800-61 is the maturity reference.

Where a developed program lands, not where a small center starts. A proposed rule (NPRM 90 FR 898, not in force) would add testing at least every 12 months.

Source: CISA, Incident Response Plan (IRP) Basics (cisa.gov) · NIST SP 800-61, Computer Security Incident Handling Guide

A plan you have not tested is a hypothesis

A TABLETOP COSTS NOTHING

- A conference room, no tools or vendors
- Walk a real scenario out loud
- Find the gaps before an incident does

THE METHOD

Build a test plan. Run the team against its own plan. Watch where it stalls.

The gaps become the next version. The review is blameless: a system failed, not a person.

From incident response to disaster recovery

Incident response

Detect, contain, eradicate, notify

Disaster recovery

Session 3

Response contains and eradicates the threat, and improves how you notify. It does not, on its own, get you back up. Recovery, getting systems and the business back on their feet, is where Session 3 begins.

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/gDgEUXdDga

Thank you!