COMMUNITY HEALTH CARE ASSOCIATION of New York State

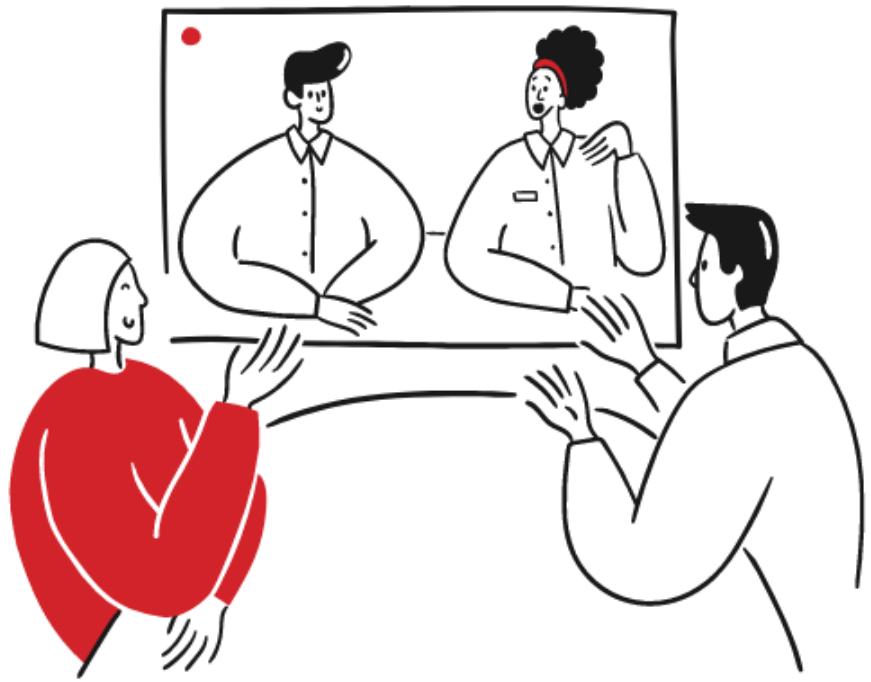
A CHCANYS NYS-HCCN funded webinar with Truvantis, Inc.

Business Associate Agreements: Controlling Your Risk Before the Breach

June 16, 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.

Every vendor that touches patient data is a risk you own

The BAA exists to manage that risk

HIPAA built the Business Associate Agreement as a tool for Covered Entities.

Most centers leave the tool unused

Sign a generic template and most power goes to waste.

See it differently today

Leave knowing the BAA is a risk instrument, and which terms you control.

The BAA is a Covered Entity's tool to manage vendor risk.

The law already gives you control over these terms

1. **Permitted uses & disclosures of PHI**
2. **Appropriate safeguards**
3. **Reporting & breach notification**
4. **Subcontractor flow-down**
5. **Return or destruction of PHI**
6. **Termination rights**

Source: 45 CFR 164.504(e) (Privacy Rule contract elements) · 45 CFR 164.314(a) (Security Rule contract elements)

The template most centers sign just restates the law

WHAT THE LAW REQUIRES

45 CFR 164.504(e)(2)(ii)(B)

"Use appropriate safeguards and comply, where applicable, with subpart C of this part with respect to electronic protected health information …"

WHAT THE HHS TEMPLATE SAYS

HHS Sample BAA, provision (b)

"Use appropriate safeguards, and comply with Subpart C of 45 CFR Part 164 with respect to electronic protected health information …"

Source: 45 CFR 164.504(e)(2)(ii)(B) (eCFR) · HHS Sample Business Associate Agreement Provisions (Jan. 25, 2013)

And the rule it points to lets the vendor decide

REQUIRED

Must implement. No discretion.

"… must implement the implementation specifications." (164.306(d)(2))

ADDRESSABLE

Assess, then implement OR document why not and use an alternative.

Encryption is addressable, not required — at rest 164.312(a)(2)(iv), in transit 164.312(e)(2)(ii). In practice, treated as optional.

Source: 45 CFR 164.306(d), 164.312(a)(2)(iv), 164.312(e)(2)(ii) (eCFR, Security Rule / Subpart C)

The reframe: you can be more specific than the law requires

WHAT THE RULE REQUIRES

“appropriate safeguards”
and
“satisfactory assurances”

The rule does not dictate how specific you can be.

WHAT THAT MEANS FOR YOU

You can mandate concrete security controls in a BAA today.

This latitude is the leverage most health centers leave on the table.

Source: 45 CFR 164.502(e)(1) (satisfactory assurances) · 45 CFR 164.504(e)(2)(ii)(B) (appropriate safeguards)

60 days is the maximum, not the target.

60

calendar days

The default outer limit for a Business Associate to notify a Covered Entity of a breach: “without unreasonable delay and in no case later than 60 calendar days after discovery of a breach.”

You can contract for tighter. Nothing stops a Covered Entity from requiring faster notice than the regulatory maximum.

Source: 45 CFR 164.410 (Business Associate breach notification)

Risk drives controls. The BAA passes them through.

Risk analysis

Required by the Security Rule. Identifies the controls you need.

→

Your controls

The standard you set to protect your own ePHI.

→

The BAA

The pass-through that carries your standard outward.

→

Vendors & subcontractors

Held to your standard, the full length of the chain.

This is our standard, and we expect you to hold to it.

A weak pass-through is a weak link

STRONG CE PROGRAM

- Mature internal controls
- Documented risk program
- Strong safeguards in place

WEAK BA, WEAK BAA

- Generic template terms
- No control requirements
- Operates below your standard

Your protection only reaches your data at the vendor if the BAA carries it there. The chain is only as strong as its weakest pass-through.

The breach that shows the chain

TriZetto / Cognizant

Clearinghouse subcontractor. Breached.

Business Associate

A health information network where TriZetto sat as a subcontractor.

Community Health Center

Affected downstream, even though its own systems were never touched.

The health center's own security posture was beside the point once the risk lived several links down the chain.

Source: TriZetto Provider Solutions / OCHIN subcontractor breach, 2024-2025; reported to HHS OCR. Calif. AG and affected health-center notices.

Two questions worth considering

Could a stronger BAA have helped the affected Covered Entities get notified sooner?

Could mandating better security controls have reduced the risk of a breach in the first place?

What could have, and should have, been passed down

COULD HAVE

- Faster, specified notification timing
- Clear cooperation duties during an incident
- Explicit subcontractor flow-down obligations

SHOULD HAVE

The specific controls a prudent Covered Entity would mandate, the controls its own risk analysis would have surfaced.

Without that analysis, the Covered Entity is guessing at its standard, or inheriting the vendor's.

The proposed Security Rule points in this direction

PROPOSED, NOT IN FORCE. NPRM 90 FR 898 (Jan 6, 2025). Comment period closed Mar 7, 2025.

1

Annual verification

Written verification, with expert analysis and certification, that a BA has deployed required controls (§164.308(b)).

2

24-hour notice

Notice up the chain within 24 hours when a contingency plan is activated.

3

No more “addressable”

Removal of the “addressable vs. required” distinction for implementation specifications.

Supports what a strong BAA can already do voluntarily today.

From contract terms to incident response

The BAA

Notification & cooperation terms

Incident response readiness

Session 2

A stronger BAA reduces risk and improves notification. It does not prevent breaches.
Incidence response readiness is covered next time.

Five moves you can make this quarter

1. Start from your risk analysis to define your standard.
2. Pull your existing BAAs, and find out whose template you're on.
3. Identify your highest-risk vendors and their subcontractors.
4. Check your real notification window against the 60-day default.
5. Decide which security controls you should be mandating.

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/YmWx7PXuU7