



COMMUNITY
HEALTH CARE
ASSOCIATION
of New York State

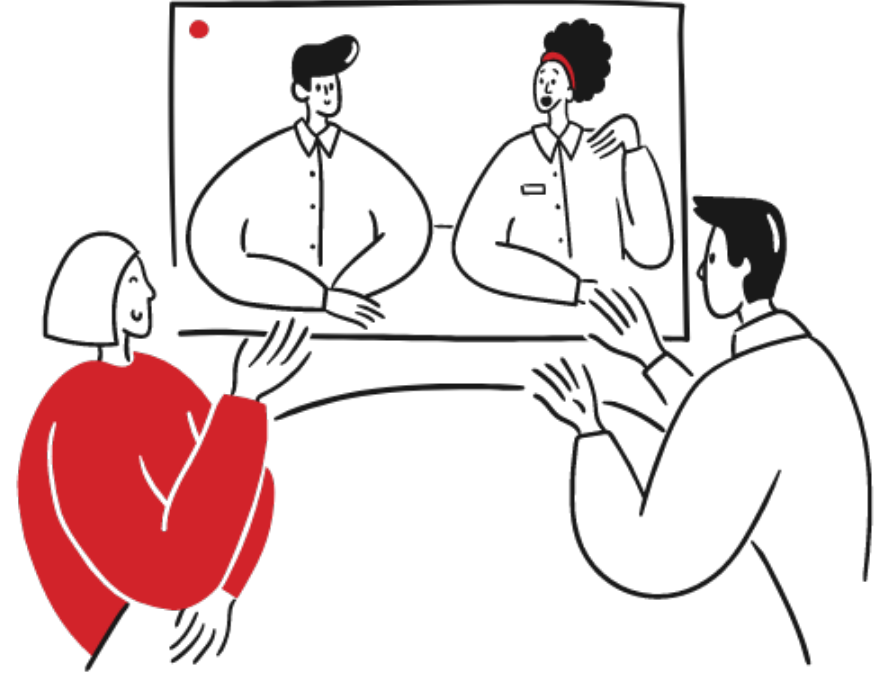
*CHCANYS NYS-HCCN presents a four-part
learning series with Online Business Systems*

Best Security Practices for Partnering with Third Party Vendors

**Session 3
February 15, 2023**

Zoom Guidelines

- You have been muted upon entry. Please respect our presenters and stay on mute if you are not speaking.
- 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 workshop is being recorded and slides will be shared after the session.



New York State HCCN Objectives



Project Period 2022–2025

1

Clinical Quality

2

Patient-Centered Care

3

Provider and Staff Wellbeing

2022-2025 Project Period

- ✓ Patient Engagement
- ✓ Patient Privacy & Cybersecurity
- ✓ Social Risk Factor Intervention
- ✓ Disaggregated Patient-level Data (UDS+)
- ✓ Interoperable Data Exchange & Integration
- ✓ Data Utilization
- ✓ Leveraging Digital Health Tools
- ✓ Health IT Usability & Adoption
- ✓ Health Equity and REaL Data Collection*
- ✓ Improving Digital Health Tools- Closed Loop Referrals*

* - Applicant Choice Objective
Bold- Objective Carried over into 2022-2025



Best Security Practices for Partnering with Third Party Vendors



Adam Kehler, CISSP
Director of RSP Healthcare Service
Online Business Systems



Jordan Wiseman, MLS, CISSP, QSA
Fellow; Risk, Security & Privacy Team
Online Business Systems





Session 3: Managing 3rd Party Risk

Best Practices, HIPAA Requirements, Special Considerations

Agenda

- ❖ Details: 3rd Parties and HIPAA

- ❖ Developments: *n*th Party Risk and Shadow HIT

- ❖ Best Practices: Managing 3rd Party Risks

- ❖ Additional Considerations

Security Goals

What are your goals?

1. Protect Patient Information
2. Comply with HIPAA (*et al*)
3. Avoid regulatory fines and corrective action plans
4. Meet requirements of cyber insurance
5. Reduce ~~financial~~ risk to the organization

Business Goals

What are your *specific* 3rd party security goals?

1. Provide patient care,
2. using third party services,
3. without them becoming a problem.

BAAs, DPAs, and due diligence

...but not in that order

“the *HIPAA Privacy Rule* [applied] only to **covered entities**... However, most ...do not carry out all...functions by themselves. Instead, they **often use the services** of a variety of **other persons or businesses.**”

- from <https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/business-associates/index.html>

The Security Rule and Third Parties

Administrative Safeguards 45 C.F.R. § 164.308

- (1) **Business associate contracts and other arrangements.** A covered entity may permit a business associate to create, receive, maintain, or transmit electronic protected health information on the covered entity's behalf only if the covered entity obtains satisfactory assurances, in accordance with § 164.314(a), that the business associate will appropriately safeguard the information. A covered entity is not required to obtain such satisfactory assurances from a business associate that is a subcontractor.
- (2) A business associate may permit a business associate that is a subcontractor to create, receive, maintain, or transmit electronic protected health information on its behalf only if the business associate obtains satisfactory assurances, in accordance with § 164.314(a), that the subcontractor will appropriately safeguard the information.
- (3) **Implementation specifications: Written contract or other arrangement (Required).** Document the satisfactory assurances required by paragraph (b)(1) or (b)(2) of this section through a written contract or other arrangement with the business associate that meets the applicable requirements of § 164.314(a).

Organizational Safeguards 45 C.F.R. § 164.314

- (a)
- (1) Standard: Business associate contracts or other arrangements. The contract or other arrangement required by § 164.308(b)(3) must meet the requirements of paragraph (a)(2)(i), (a)(2)(ii), or (a)(2)(iii) of this section, as applicable.
- (2) Implementation specifications (Required) -
- i. Business associate contracts. The contract must provide that the business associate will -
 - A. Comply with the applicable requirements of this subpart;
 - B. In accordance with § 164.308(b)(2), ensure that any subcontractors that create, receive, maintain, or transmit electronic protected health information on behalf of the business associate agree to comply with the applicable requirements of this subpart by entering into a contract or other arrangement that complies with this section; and
 - C. Report to the covered entity any security incident of which it becomes aware, including breaches of unsecured protected health information as required by § 164.410.
 - ii. Other arrangements. The covered entity is in compliance with paragraph (a)(1) of this section if it has another arrangement in place that meets the requirements of § 164.504(e)(3).
 - iii. Business associate contracts with subcontractors. The requirements of paragraphs (a)(2)(i) and (a)(2)(ii) of this section apply to the contract or other arrangement between a business associate and a subcontractor required by § 164.308(b)(4) in the same manner as such requirements apply to contracts or other arrangements between a covered entity and business associate.



Wait, didn't you say the ***Privacy*** Rule?!

Yes, but it's not comparing, you know...

- ▀ The Privacy Rule requires safeguarding ePHI
- ▀ The Security Rule is *how* that's done, more or less

Security Rule Safeguards

Basically, do what's **reasonable** and **appropriate** to protect ePHI

▀ General Rules

▀ Administrative Safeguards

▀ Physical Safeguards

▀ Technical Safeguards

▀ Organizational Requirements

▀ Documentation Requirements

The Security Rule and Third Parties

Administrative Controls

45 CFR §164.308(b)

Administrative Safeguards

45 C.F.R. § 164.308

Business Associates and contractors can handle a Covered Entity's ePHI:

- IF they promise to appropriately safeguard that ePHI,
- AND those assurances are in a *written* contract or other arrangement.

Organizational Controls

45 CFR §164.314(a)

Organizational Safeguards

45 C.F.R. § 164.314

Those contracts or other arrangements must contain agreements to:

- COMPLY with the Privacy Rule requirements,
- EMPLOY the Security Rule safeguards,
- HOLD subcontractors to the same,
- REPORT any security incidents and data breaches of unsecured ePHI.

Privacy Rule BAA Requirements

Define **WHAT** data may be used

Define **HOW** those data may be used

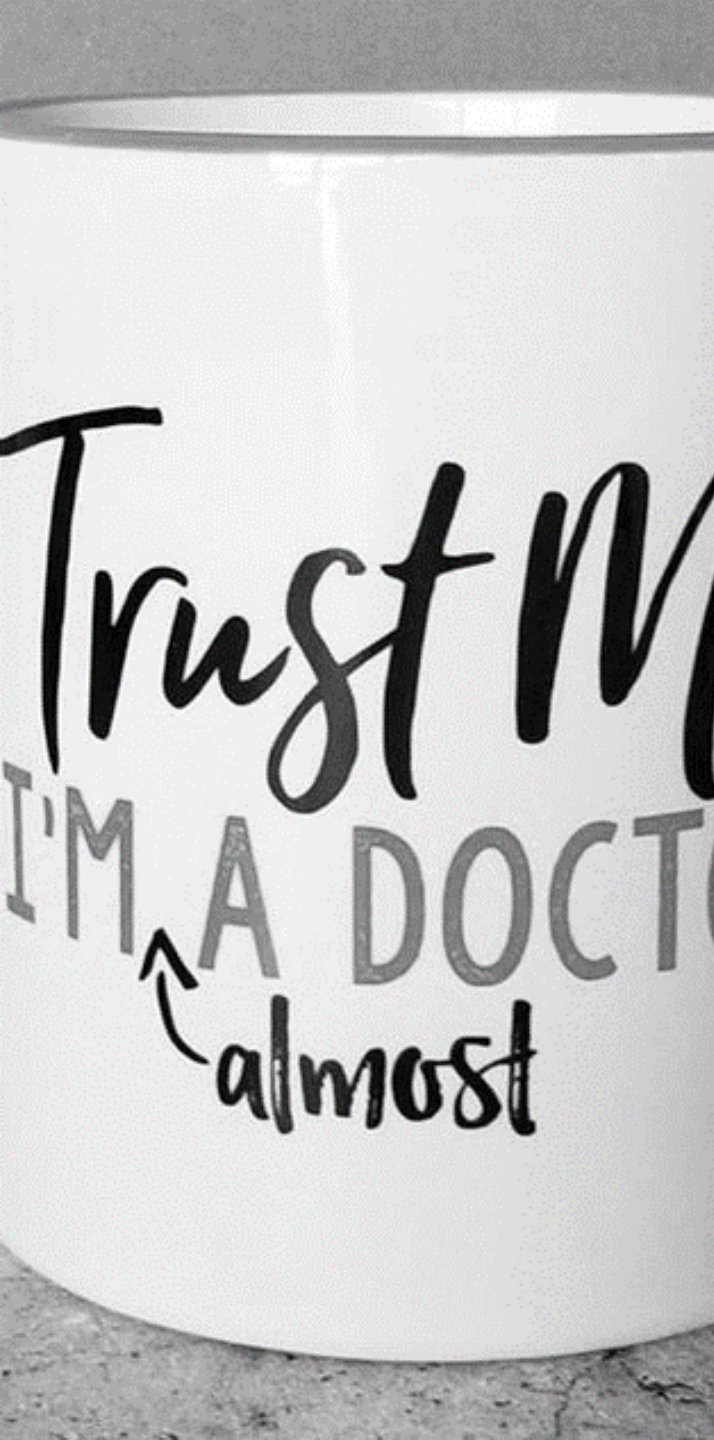
Require **TERMINATING** for non-compliance

And the Business Associate must also promise to:

- ONLY use the CE's ePHI as agreed
- PROTECT the CE's ePHI
- REPORT breaches of the CE's ePHI
- ENABLE access to and corrections to the ePHI
- SUPPORT the CE's HIPAA compliance
- RETURN or delete CE's data after contract






So, BAAs for all the third parties? ~~No~~, not quite.



Business Associates




Perform actions:

-  That involve using or disclosing ePHI, and
-  On behalf of a CE, or
-  To provide services to a CE

Business Associates are directly liable under HIPAA, but BAAs are still necessary.

Other Third Parties

Perform actions:

-  Only as conduit for ePHI, or
-  To provide software or support to a CE, etc., and
-  That don't normally involve using or disclosing ePHI

Other Third Parties do not need BAAs, but they may need DPAs.



So, what is a DPA?

Data Protection Agreement

- Kind of like a BAA, it details:
 - What data
 - What uses
 - What safeguards
- May include more specific provisions, e.g.:
 - Minimum encryption strength
 - Locale for storage and processing
 - Specific security controls
- Can complement a BAA



Due Diligence

Now that we've reviewed some of the relationships...

...we have some important questions before we enter one.

**Do they need
to access our
ePHI?**

**Will they
receive our
data?**

**Would they
affect our
security?**

Due Diligence (cont.)

If they need our
ePHI...

▀ They need to
sign a BAA

Remember:
BAAs are not
optional for BAs

If they receive
our data...

▀ If they're likely
to get ePHI,
they may need
to sign a BAA

▀ They should
sign a DPA

If they'll affect
our security...




▀ They should
sign a DPA

Business Associate Agreements

While BAs are directly liable under HIPAA...

...BAAs are still required by 45 C.F.R. § 164.504(e)

The CE who owns the ePHI must be known.

-  The CE decides the allowed uses
-  The CE decides what data is provided
-  The CE decides how long the BA can have the data

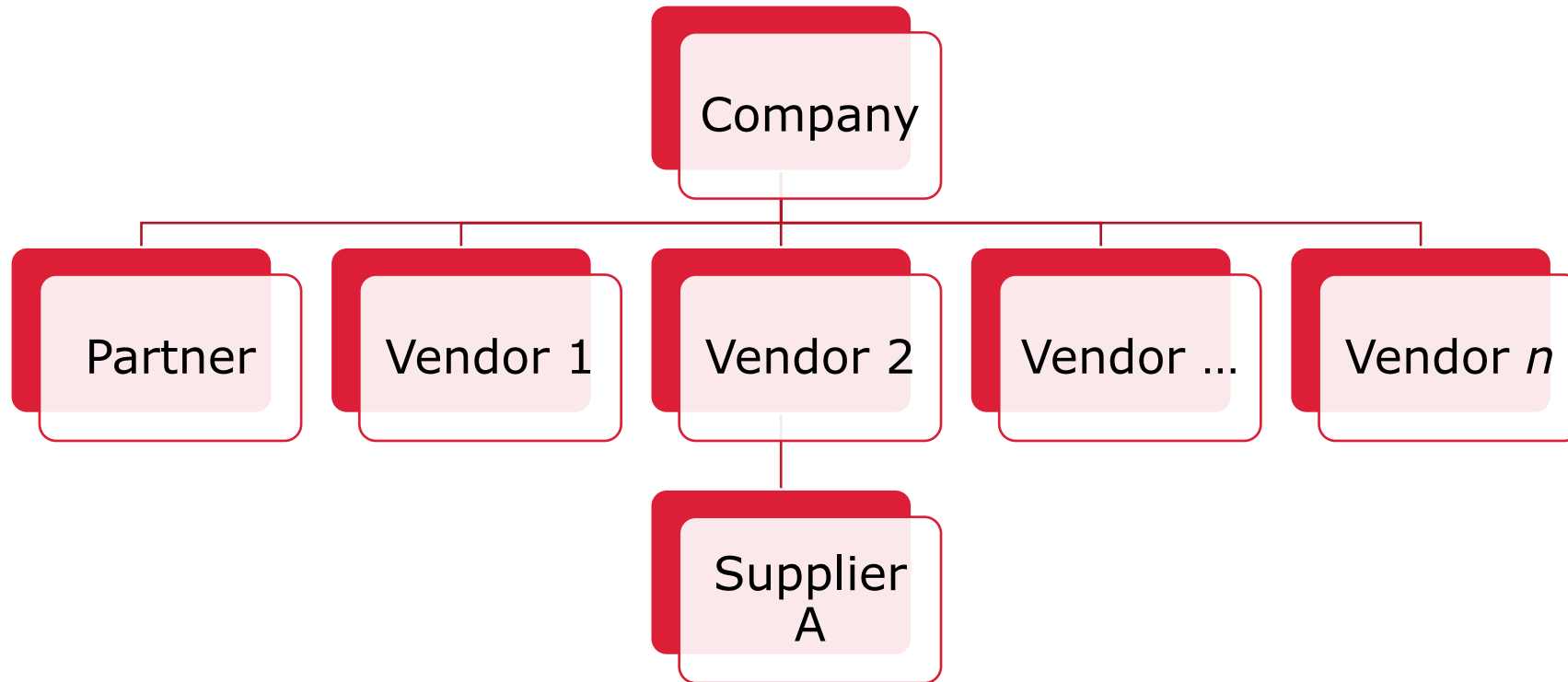
The evolution of 3rd party risk

Supply chains, partner chains, and managing the unknowns

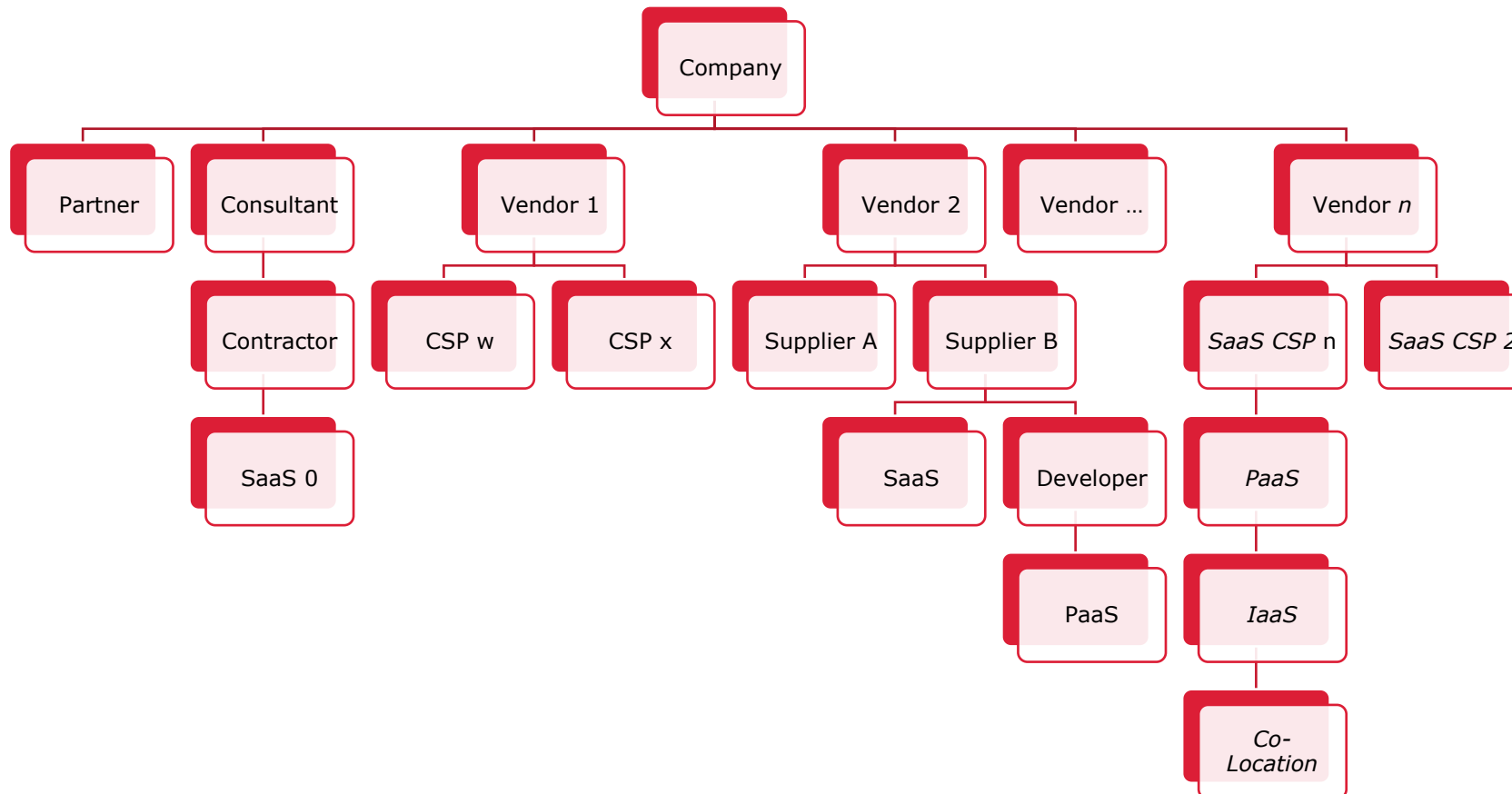
“Modern **products and services** depend on their supply chains, which connect a **worldwide network** of...**components and software** that...[might] contain malicious software or be susceptible to cyberattack”

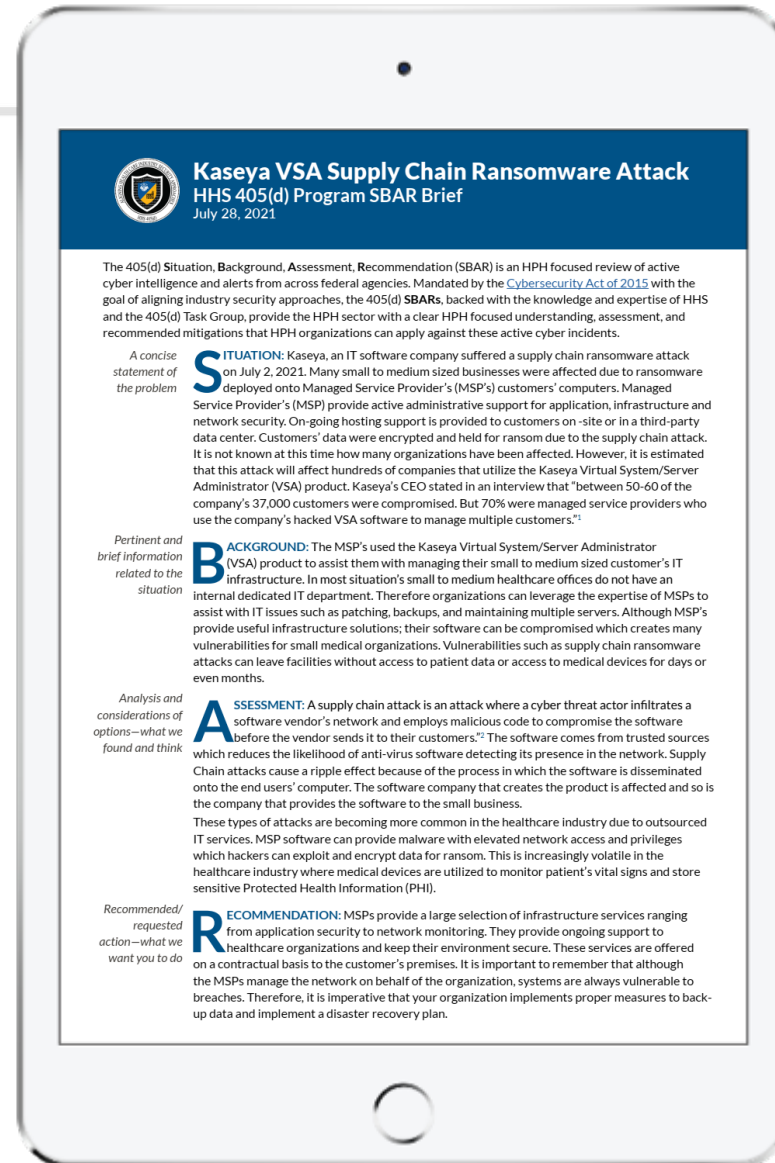
- NIST from <https://www.nist.gov/news-events/news/2022/05/nist-updates-cybersecurity-guidance-supply-chain-risk-management>

It used to be (mostly) just 3rd Party



But now...it's *complicated*.





Complexity
leads to
interesting
and scary
scenarios...



▀ Results. Guaranteed.

The Shadow knows...



...and does good works.

However, working outside the rules increases risks from:


- ▀ Shadow IT
- ▀ Shadow **H**IT
- ▀ Shadow BPO

Let's SWOT Shadow IT/HIT/BPO a bit


STRENGTHS

-  Enabling health operations
-  Supplements capabilities



WEAKNESNES

-  Lack of oversight
-  Reinforces silos

OPPORTUNITIES

-  Chance to optimize
-  Cost savings

THREATS

-  Failure to obtain a BAA
-  Inadequate safeguards

 Results. Guaranteed.

Managing 3rd party risks

Praxis, praxis, praxis your vendor risk management process.

Successful 3rd party risk management
takes consistent application
of vendor management
processes.

Vendor Mgmt. Notes



Policy



Sharing



Access



Risk



Monitor



Changes

Vendor Management Process

Establish a vendor security policy

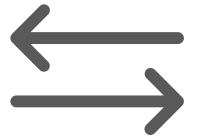


Recommended elements:

- Require appropriate agreements (e.g., BAAs, DPAs, etc.)
- Require initial and regular vendor risk assessments
- Include the right to audit in contracts; periodically execute
- Consider mandating industry accepted control frameworks

Vendor Management Process

Define minimum security for sharing



Recommended elements:





- Acceptable protocols for data transmission (SFTP, SCP, HTTPS, etc.)
- Encryption requirements, including algorithms and strengths
- Are faxes allowed?
- Is **secure** email an option?

Vendor Management Process

Define minimum access requirements



Recommended elements:

-  IAM and SSO requirements (SAMLv2, OIDC, UI-automation, *etc.*)
-  Multi-factor, attribute, and “frictionless” authentication
-  Machine-to-machine and non-interactive access
-  How long can access to the data be retained?

Vendor Management Process

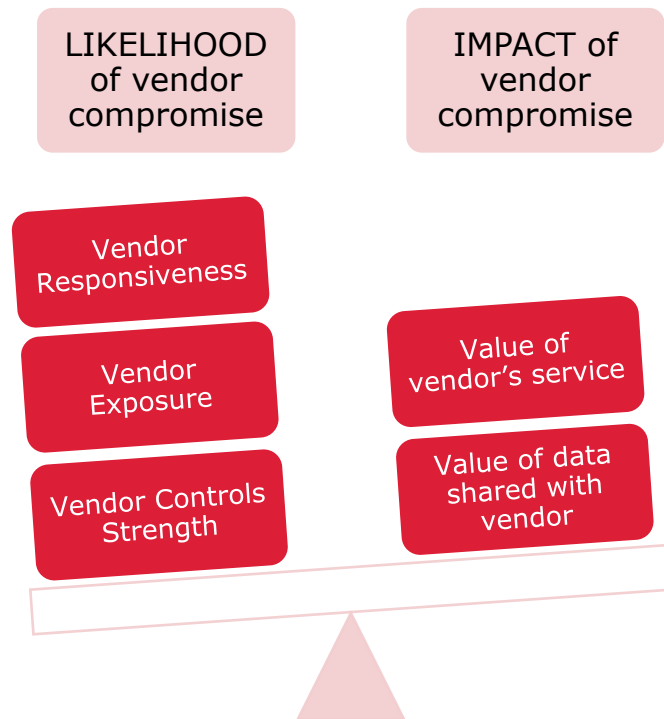
Assess vendor risks



Recommended elements:

- Assess the risk from a vendor *before* engaging them
- Document the results and keep an inventory
- Regularly re-assess, as often as appropriate (based on the risk)
- Implement compensating controls, if needed

An example vendor risk assessment



	IMPACT		
LIKELIHOOD	LOW	MODERATE	HIGH
LOW	LOW	LOW	MODERATE
MODERATE	LOW	MODERATE	HIGH
HIGH	MODERATE	HIGH	HIGH

Vendor Management Process

Monitor vendor compliance



Recommended elements:





- Periodically review any independent assessments, *e.g.*, SOC 2 Type II, ISO 27001, PCI AOCs, *etc.*
- Track and review reports of incidents, breaches, activity reports and AODs
- Consider other relevant metrics (even non-security)
- Regularly meet with your contact; make sure issues are corrected

Vendor Management Process

Manage relevant changes



Recommended elements:

-  Contract refreshes
-  Have our processes, technology, or patterns changed?
-  Does this vendor represent technical debt?
-  Are there new services or changes on the vendor side?

And another thing or two

Some additional and interesting considerations.

“If you really want to understand something, the best way is to try and explain it to someone else.”

- Douglas Adams

Other Security Standards

Address third party risk management too

HHS 405(d)

Tech Volume 1-10.S.A

Become familiar with which data, applications, systems, and devices your contractors and vendors are authorized to access.

ISO 27001:2022

Annex A.15.1

Information security in supplier relationships

Annex A.15.2

Supplier service delivery management

NIST CSF v1.1

Supply Chain Risk Management (ID.SC)

The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk.

A moment on 405(d)

The HIPAA Safe Harbor Bill was signed into law on January 5, 2021.

It calls for the HHS Secretary to consider whether an entity has

-  **adequately demonstrated recognized security practices**

-  that have been in place **for at least 12 months**, and

-  to **reduce the potential penalties**

which might have otherwise been implemented as a result of potential HIPAA Security Rule violations.

Insurance Requirements

You may be asked:

- If you have a vendor management program
- For example contracts or templates
- About supplier incidents and breaches

Breach Insurance is becoming expensive and even unavailable!

Insurance Savings

Vendor management may:

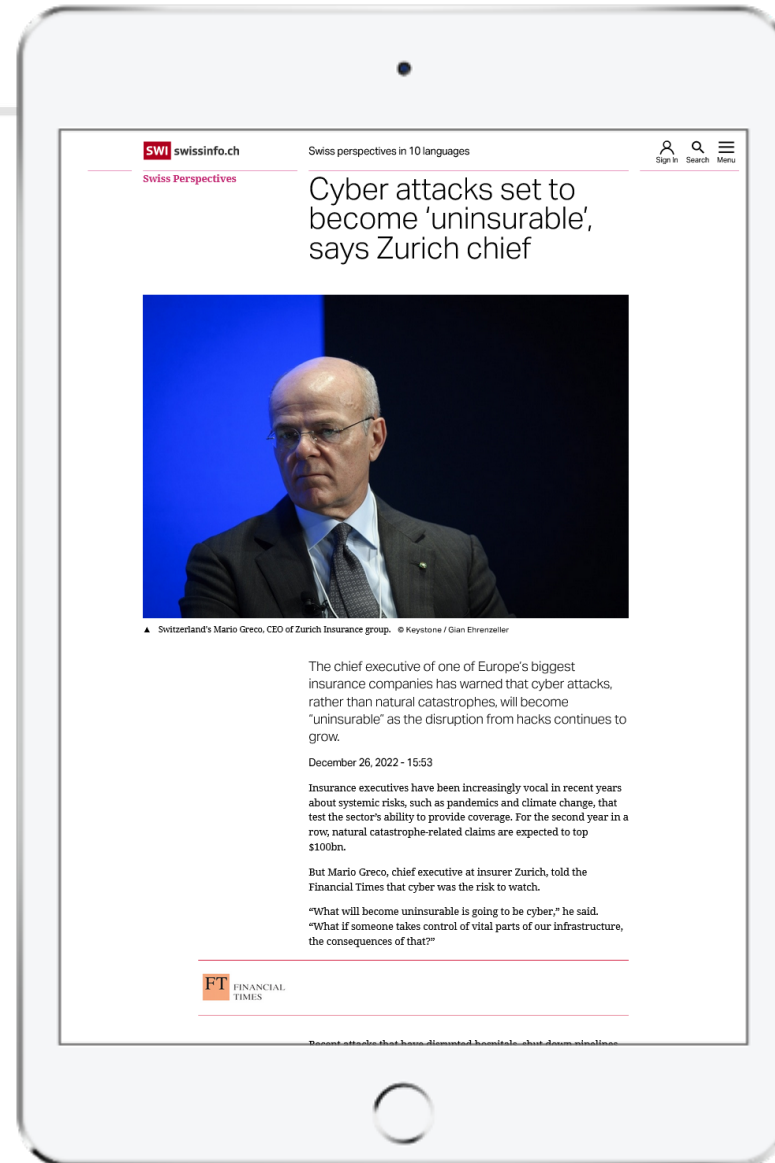
- Help reduce insurance premiums
- Help you obtain or retain coverage
- Cover third-party breaches, or part of your response

Don't forget to ask your vendors if *they* have breach insurance!



Wait, do you say *insurance may be unavailable?!*

Yep,
that
may
soon
be
true



"...there [is] **a limit** to **how much the private sector can absorb**...from cyber attacks."

"A report from the [GAO] highlighted the potential of **cyber incidents to 'spill over'** to other linked firms...**with catastrophic consequences.**"

And Back to Documentation

Some additional comments...

- Inventory all the vendors
 - Track last assessed dates
- Make adding new vendors easy
 - Else you'll make more shadows
- Accept Shadows into management
 - They'll happen
 - Have a process to include them



A blurred background image showing a person's arm and hand, possibly holding a device, in a dimly lit environment.

Thank You



Questions?



Next Cybersecurity Session:

Building an Incident Response Plan

Wednesday, March 1, 12-130PM

[Register for Session 4 Here](#)

Incident Response Workshop:

Tarrytown, NY In-Person Event

Tuesday, March 21, 10AM-4PM

[Register Here](#)

Limited availability!



Workshop Evaluation Survey

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

Survey Link:

https://forms.office.com/Pages/ResponsePage.aspx?id=YSZl7iDhjEqs_ICzVbYzoqmlH89zfFNPhDWTC9uAhXZUM005SVNTVVVM3Qkg5SktXNzBPM1E4VklJNC4u



Thank you!

