



COMMUNITY
HEALTH CARE
ASSOCIATION
of New York State

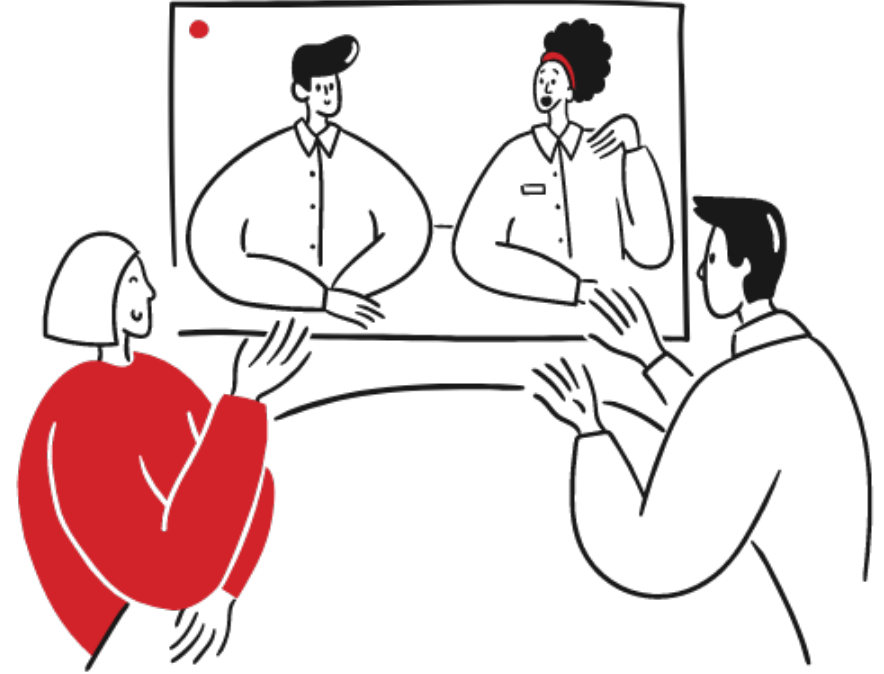
CHCANYS NYS-HCCN presents a three-part learning series with Online Business Systems

Third Party Vendor Security Best Practices 2024

Session 2
February 13, 2024

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



Third Party Vendor Security Best Practices 2024



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





2024 Session 2: Third Party Risk

Revisiting requirements, recent developments, and best practices

Agenda

❖ 3rd Parties and HIPAA, 405(d), PCI DSS, *etc.*

❖ 3rd, 4th, 5th ... *n*th Party Risk and Shadow HIT

❖ Recent developments

❖ Managing 3rd Party Risks

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.

 Results. Guaranteed.

BAAs, DPAs, RACIs, etc.

...but not *necessarily* in that order

In the beginning...

the *HIPAA Privacy Rule* [applied] only to **covered entities**...

however, most...**use the services** of a variety of **other persons or businesses.**



Wait, did 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

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

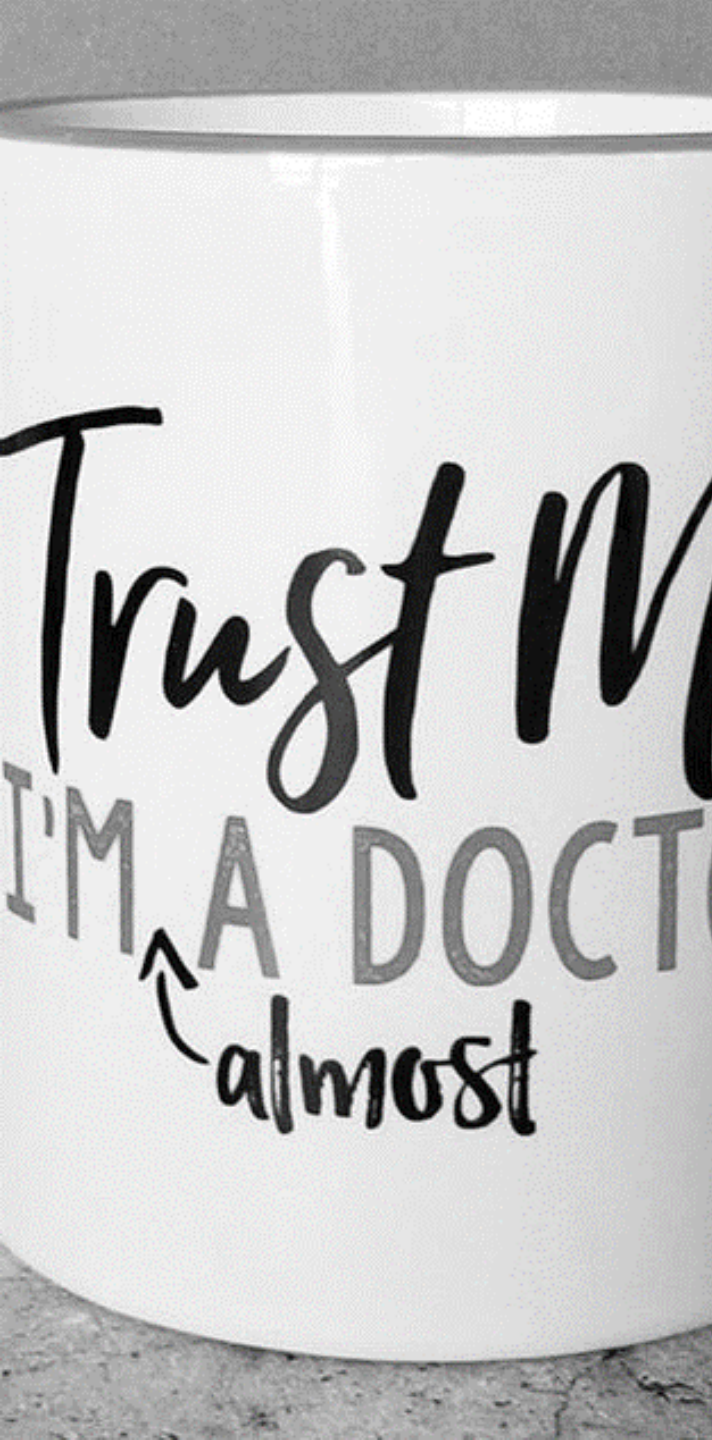
And the Business Associate must also promise to:

- 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

Results. Guaranteed.



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



Results. Guaranteed.

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



Is that it? Is it all *only* about HIPAA?



Results. Guaranteed.

No, it's not that simple

...it's a big twinkie.

In addition to HIPAA:

- Enhanced health data privacy laws:
SAMHSA, STDs, IRB rules, *etc.*
- GLBA, PCI, state PII privacy laws, *etc.*

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.

A moment more on 405(d)

Five prevailing cybersecurity threats to healthcare organizations

- ▀ Social Engineering
- ▀ Ransomware
- ▀ Loss or theft
- ▀ Insider threats
- ▀ Medical IoT attacks

A moment *more* on 405(d)

Cybersecurity practices to address the prevailing cybersecurity threats to healthcare organizations

- ▀ Email Protection
- ▀ Endpoint Protection
- ▀ Access Management
- ▀ Data Protection and LP
- ▀ Asset Management
- ▀ Network Management
- ▀ Vuln. Management
- ▀ Incident Response
- ▀ Medial Device Security
- ▀ Cybersecurity Governance

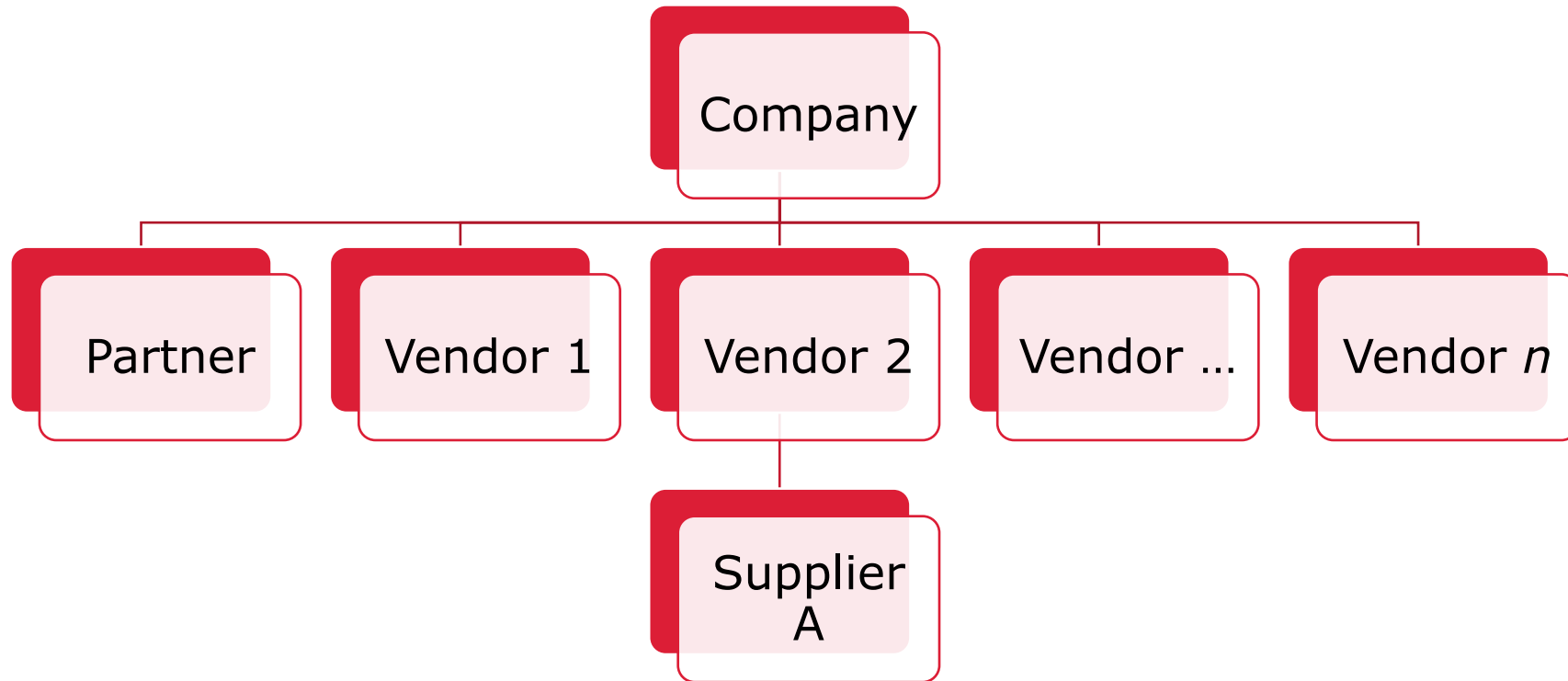
 Results. Guaranteed.

The advent of n^{th} party risk

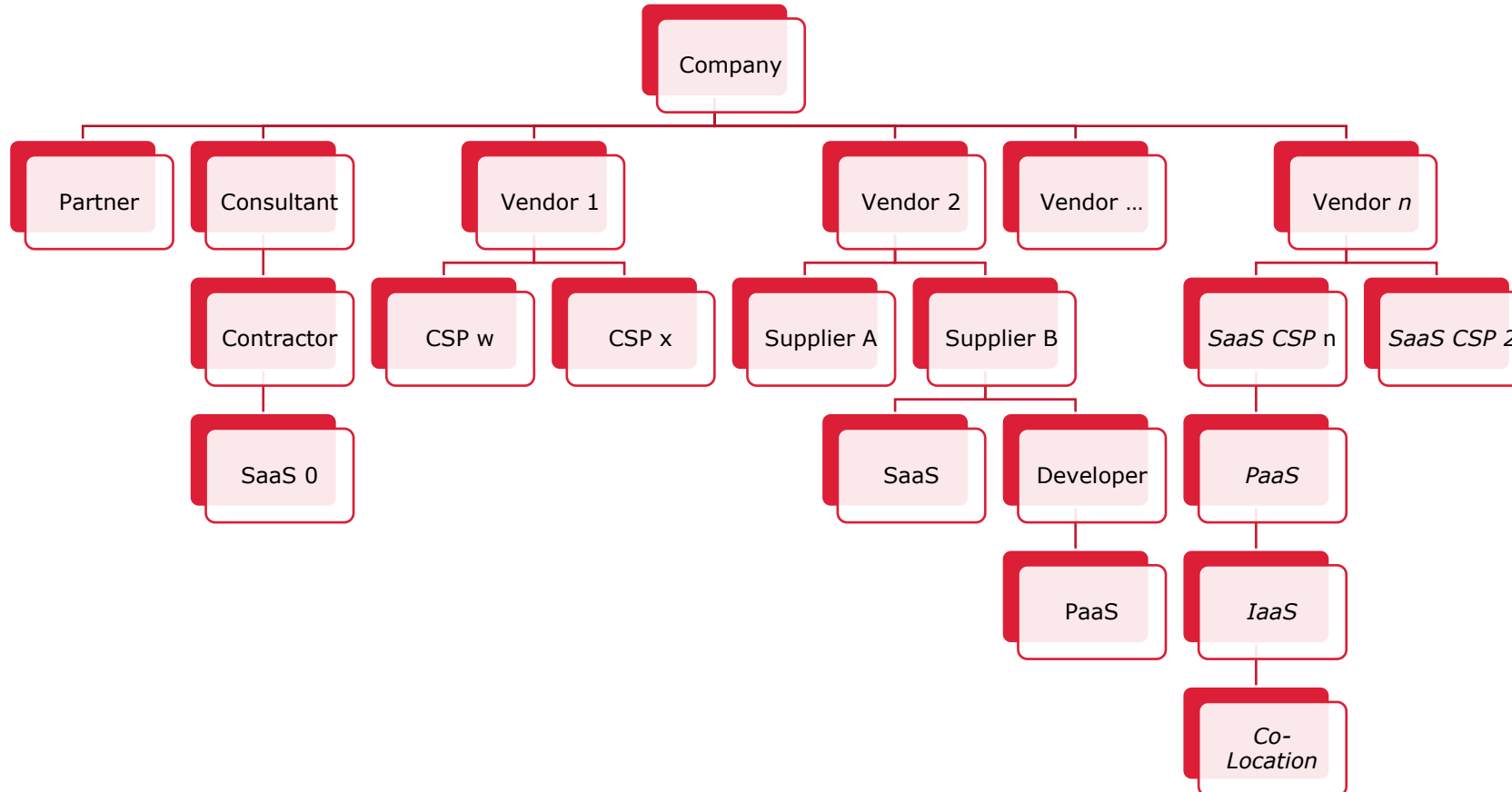
Supply chains, partner chains, and managing the unknowns

Modern **products and services** depend on
a worldwide network of...components...
that [might] contain malicious software
or be susceptible to cyberattack”

It used to be (mostly) just 3rd Party



But now...it's complicated.



Complexity
leads to
interesting
and scary
scenarios...

HHS 405(d) SBAR Brief: Kaseya VSA Supply Chain Ransomware Attack.pdf



Kaseya VSA Supply Chain Ransomware Attack HHS 405(d) Program SBAR Brief July 28, 2021

The 405(d) Situation, Background, Assessment, Recommendation (SBAR) is an HPH focused review of active cyber intelligence and alerts from across federal agencies. Mandated by the [Cybersecurity Act of 2015](#) with the goal of aligning industry security approaches, the 405(d) SBARs, backed with the knowledge and expertise of HHS and the 405(d) Task Group, provide the HPH sector with a clear HPH focused understanding, assessment, and recommended mitigations that HPH organizations can apply against these active cyber incidents.

A concise statement of the problem

SITUATION: Kaseya, an IT software company suffered a supply chain ransomware attack on July 2, 2021. Many small to medium sized businesses were affected due to ransomware deployed onto Managed Service Provider's (MSP's) customers' computers. Managed Service Provider's (MSP) provide active administrative support for application, infrastructure and network security. On-going hosting support is provided to customers on -site or in a third-party data center. Customers' data were encrypted and held for ransom due to the supply chain attack. It is not known at this time how many organizations have been affected. However, it is estimated that this attack will affect hundreds of companies that utilize the Kaseya Virtual System/Server Administrator (VSA) product. Kaseya's CEO stated in an interview that "between 50-60 of the company's 37,000 customers were compromised. But 70% were managed service providers who use the company's hacked VSA software to manage multiple customers."¹

Pertinent and brief information related to the situation

BACKGROUND: The MSP's used the Kaseya Virtual System/Server Administrator (VSA) product to assist them with managing their small to medium sized customer's IT infrastructure. In most situation's small to medium healthcare offices do not have an internal dedicated IT department. Therefore organizations can leverage the expertise of MSPs to assist with IT issues such as patching, backups, and maintaining multiple servers. Although MSP's provide useful infrastructure solutions; their software can be compromised which creates many vulnerabilities for small medical organizations. Vulnerabilities such as supply chain ransomware attacks can leave facilities without access to patient data or access to medical devices for days or even months.

Analysis and considerations of options—what we

ASSESSMENT: A supply chain attack is an attack where a cyber threat actor infiltrates a software vendor's network and employs malicious code to compromise the software before the vendor sends it to their customers."² The software comes from trusted sources



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

STRENGTHS

- Enabling health operations
- Supplements capabilities

WEAKNESNES

- Lack of oversight
- Reinforces silos

OPPORTUNITES

- Chance to optimize
- Cost savings

THREATS

- Failure to obtain a BAA
- Inadequate safeguards

Recent developments

Highlighting significant concerns related to third-party risks



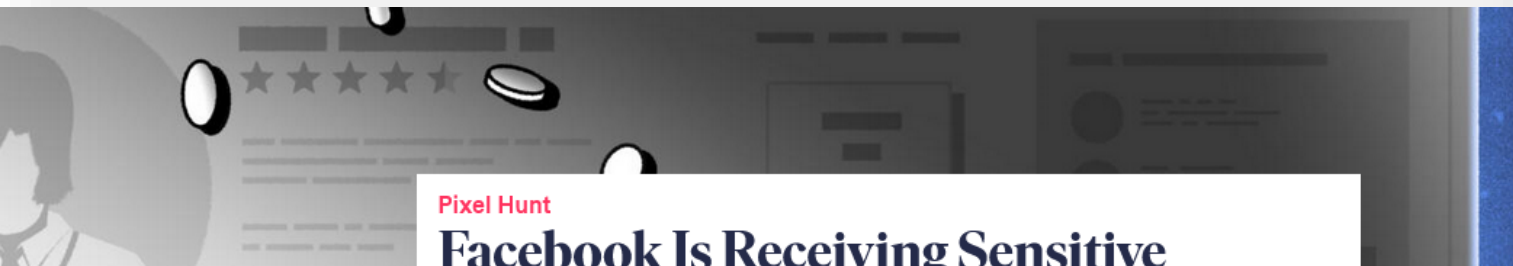
Predictably, Information Services is #1 on the list...

BUT

HEALTHCARE is #3

<https://www.businesswire.com/news/home/20230201005038/en/SecurityScorecard-Research-Shows-98-of-Organizations-Globally-Have-Relationships-With-At-Least-One-Breached-Third-Party>

https://www.businesswire.com/news/home/20230201005038/en/SecurityScorecard-Research-Shows-98-of-Organizations-Globally-Have-Relationships-With-At-Least-One-Breached-Third-Party



Pixel Hunt

Facebook Is Receiving Sensitive Medical Information from Hospital Websites

Anson Chan

June 16, 2022 06:00 ET
Updated July 19, 2023 09:29 ET

Experts say some hospitals' use of an ad tracking tool may violate a federal law protecting health information

By [Todd Feathers](#), [Simon Fondrie-Teitler](#), [Angie Waller](#), and [Surya Mattu](#)

Share This Article

Copy Link

Republish

This article is copublished with

STAT

A tracking tool installed on many hospitals' websites has been collecting patients' sensitive health information—including details about their medical conditions, prescriptions, and doctor's appointments—and sending it to Facebook.

The Markup tested the websites of [Newsweek's](#) top 100 hospitals in America. On 33 of them we found the tracker, called the Meta Pixel, sending Facebook a packet of data whenever a person clicked a button to schedule a doctor's

The Meta Pixel collects sensitive health information and shares it with Facebook

The Meta Pixel installed on Piedmont Healthcare's MyChart portal sent Facebook details about a real patient's upcoming doctor's appointment, including date, time, the patient's name, and the name of their doctor

- 1 Patient name
- 2 Date and time of appointment
- 3 Name of provider

```
{
  "classList": "Link_actionable+link_readOnlyText+InternalLink+main",
  "destination": "https://mychart.piedmont.org/PRD/app/communication-center/conversation?id=ID_REDACTED BY THE"
}
```

group associated with a particular disease—but the data collected by pixels on hospitals' websites is more direct. And in sharing it with Facebook, experts said, health care providers risk damaging patients' trust in an increasingly digitized health system.

See our data here.



The Markup found that filling out a survey through Novant Health shared sensitive information like sexual orientation with Facebook via the Meta Pixel. Source: [www.novantmychart.org](#), [www.novanthealth.org](#)

"Almost any patient would be shocked to find out that Facebook is being provided an easy way to associate their prescriptions with their name," said Glenn Cohen, faculty director of Harvard Law School's Petrie-Flom Center for Health Law Policy, Biotechnology, and Bioethics. "Even if perhaps there's



Existing Law:

- FTC Act
- Washington state's My Health My Data Act




Proposed:

- New York: Amendments to Privacy Standards for Electronic Health Products
- Massachusetts: Consumer Health Data Act
- Illinois: Health Data Privacy Bill



Insurance Requirements




You may be asked:

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

Breach Insurance is becoming expensive and harder to get!

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!

 Results. Guaranteed.

Managing 3rd party risks

Praxis, praxis, praxis your vendor risk management process.

Vendor Management Process

Establish a vendor security policy

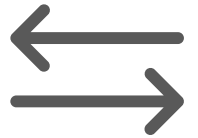


Recommended elements:

- ▀ 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

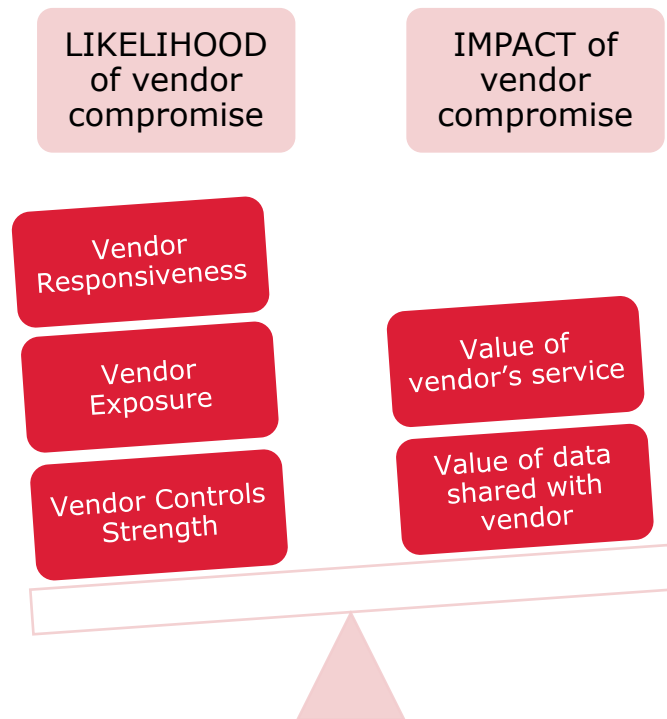
Assess vendor risks



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?

Vendor Management Process

Dress rehearse your IR/DR/BC plans



Recommended elements:

- ▀ Involve everyone possible
- ▀ Practice insider threats, e.g., data-theft on the Orient Express?
- ▀ Ransomware, public disclosures, and even malicious reporting are real
- ▀ Know how long it takes to investigate, contain, and restore

A blurred background image showing several people in a meeting or conference room. They appear to be sitting around a table, possibly engaged in a discussion or presentation. The image is out of focus, emphasizing the text in the foreground.

Thank You

Questions?



Next Cybersecurity Session:

Privacy and Security Aspects of Artificial Intelligence

Tuesday, March 19, 12-130PM

[Register for Session 3 Here](#)

Incident Response Tabletop Workshop

New York, NY In-Person Event

Tuesday, April 16, 10:30AM-3:30PM

[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=YSZI7iDhjEqs_ICzVbYzooHiZ0zMAXIKutjkObjvztFUNTZaVFdGQUpaVzNXQlITNIA2TlowWINNMC4u

Thank you!



CHCANYS - Online Business
Systems Eval for Third Party
Vendor Security Best Practices

