



Health3PT

Vendor Risk Management Summit

June 7, 2023



What We'll Cover

01

Introduction to the Health
3rd Party Trust Initiative

02

Panel Discussion - TPRM
through the lens of Relying
Parties

03

Panel Discussion - TPRM through
the lens of Business Associates /
Suppliers/ Vendors Organization

04

TPRM –
A Better Way Forward

05

How to Get Started

06

Q&A

Introduction

Health 3rd Party Trust Initiative



John Houston, J.D.
VP, Information Security and Privacy
Founding Member, Provider Third Party Risk Initiative
Founding Member, Health 3rd Party Trust Initiative



Why We're Here

Third Party Cyber Risk Management is **BROKEN!**

We're here to identify efficient and effective approaches to **reduce risk in the healthcare industry's third-party ecosystem.**



Credible assurances | Efficient workflows | Ecosystem-wide standards

We Have a Serious Problem

55%

of healthcare organizations experienced a third-party breach in the past year¹

1. HIPPA <https://www.hipaajournal.com/55-of-healthcare-organizations-suffered-a-third-party-data-breach-in-the-past-year/>

\$10.1M

is the average cost of a healthcare data breach²

2. <https://www.ibm.com/reports/data-breach>

90%

of the largest healthcare breaches in 2022 were tied to vendors³

3. <https://www.scmagazine.com/feature/breach/most-of-the-10-largest-healthcare-data-breaches-in-2022-are-tied-to-vendors>

\$23.7B

is the healthcare industry's average spending on vendor risk management per year⁴

4. <https://www.healthcarefinancenews.com/news/third-party-risk-costs-healthcare-industry-237-billion-year-report-finds>

Health3PT - Where We Started → Where We're Going



Health3PT is the next generation of the **Provider Third-Party Risk Management Initiative**, founded in 2018.



The original council was **integral in defining SOPs and best practices for vendors**, including:

- Methodology for assessing vendor risk
- Templates for communications with vendors
- Common legal language on assurance requirements for contracts



Health3PT builds upon the mission of the original council while **expanding beyond providers** to include other key stakeholders.



Our goal is to find **innovative approaches to addressing third-party risk** by bringing the best minds together in one dedicated time and space.

The Council for the Health3PT Initiative

20

Leading Organizations
Committed to Council Initiative

100+

New Participating Organizations
in Health3PT Initiative

Patricia Yarabinec, **AmeriHealth Caritas**

Cindy Shuna, **Amerisource Bergen**

Rick Kratz, **Amerisource Bergen**

Glen Braden, **Attest Health Care Advisors**

Shenny Sheth, **Centura Health**

Natalie Henderson, **CVS**

Eric Sinclair, **Evolent Health**

Brad Carvellas, **Guthrie**

Matthew Webb, **HCA Healthcare**

Brenda Callaway, **Health Care Service Corporation (HCSC)**

John Chow, **Healthix**

Jeff Lockwood, **HealthStream**

Karin Balsley, **HealthStream**

Heather Ryan, **Highmark BCBS**

Joe Dylewski, **Humana**

Dr. Omar Sangurima, **Memorial Sloan Kettering Cancer Center**

Purvik Shah, **Memorial Sloan Kettering Cancer Center**

Walsy Saez-Aguirre, **Memorial Sloan Kettering Cancer Center**

Monique Hart, **Piedmont Healthcare**

Dr. Adrian Mayers, **Premera Blue Cross**

Joel Seymour, **Premera Blue Cross**

Brian Cayer, **Tufts Medicine**

Alan Labianca-Campbell, **Tufts Medicine**

John Houston, **UPMC**

Ryan George, **UPMC**

Alex Zhivov, **Virtual Health**

Bhavesh Merai, **Walgreens**

TPRM is Broken

In more ways than one. Here are some of the things we have heard from clients.



**Too much,
too fast**



**Lack of resources,
scalability, and coverage**



**Limited follow
through on remediation**



**Partial inventories and
blind spots**



**Inadequate risk reporting
to key stakeholders**



**Vendors are
overwhelmed**



**High variance with no "gold
standard"**

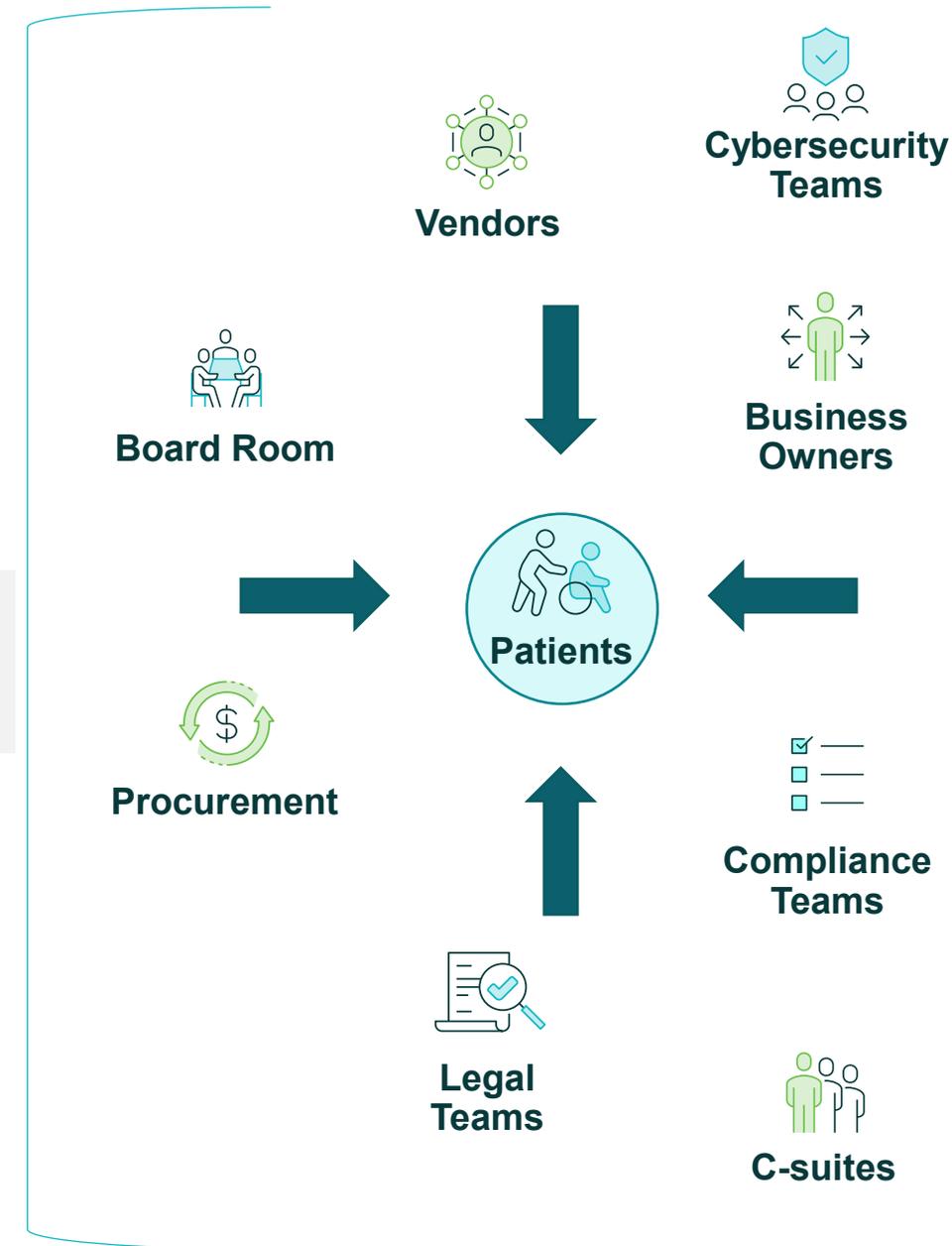


**Insufficient adoption
of assurance models**



**TPRM solutions don't fully
solve the problem**

Many Stakeholders, Many Obstacles



What's Wrong with the Current Process?

Health3PT Survey: Preliminary Results

Covered Entities (Relying Parties)

- Getting vendors to respond
- Not receiving transparent assurances that satisfy the request the first time
- Handling a high volume of assessments
- Turnaround time takes too long
- Getting vendors to address deficiencies

82% Process is inefficient

62% Process is ineffective

Business Associates (Vendors/Suppliers)

- Variability of questionnaires
- Ability to provide quality responses
- Customers not accepting validated assurances in lieu of questionnaires

81% Process is inefficient

72% Process is ineffective

Key Actions to Make the Process More Efficient and Effective

Health3PT Survey: Preliminary Results

Covered Entities

- Creating norms around inherent risk and vendor tiering
- Standardized, validated assessments over questionnaires
- Receiving assessment results from vendors electronically
- Continuous monitoring and remediation reporting

Business Associates

- Collaborative approach to providing assurances based on inherent risk
- Standardized, validated assessments over questionnaires
- Sharing assessment results electronically with their customers

TPRM is a Huge Problem

Here are the principles that guide Health3PT.



Incremental progress is important.



True partnerships with vendors are key.



Collaboration and standardization move us forward.



Some compromise will be necessary to make progress.

Health3PT is Already Making Progress

- Recommended Practices mapped to solutions to start removing the pain, waste and risk - starting today
- Council is committed to implementation and execution of these best practices
 - Recommended contract language that supports the risk and represents both sides of the transaction
 - Proper use of risk tiering
 - Use of standardized assurances that are accepted and encouraged by the Council - HITRUST® e1 - i1 - r2 assessments and eliminate redundant questionnaires
- Over 140 leading organizations are engaged in the Initiative – we all need to work together to adopt these practices for the benefit of all

Panel Discussion #1

TPRM Through the Lens of Relying Parties



TPRM Panel Discussion - *Through the Lens of Relying Parties that Rely on Cyber Assurances from Vendors*



Facilitator
Matthew Webb, AVP –
Product Security; Chief Product
Security Officer



Brenda Callaway, Divisional
VP, Operations Performance
Management



Dr. Omar Sangurima, Principal
Technical Program Manager
Security Governance, Risk, &
Program Management
department



Memorial Sloan Kettering
Cancer Center



Justin Heyl, Director, Enterprise
Cybersecurity Risk
Management



10 Minute Break

Provide your feedback now:

1. Go to Health3PT.org
2. Take the TPRM Survey



Health3PT

[About Us](#)

[Benefits](#)

[Join Us](#)

[Newsroom](#)

[Events](#)

[Take the survey](#)



A stylized graphic on the right side of the slide shows a hand holding a globe. The hand is composed of thick, dark teal outlines, and the globe is a lighter teal color with a grid of latitude and longitude lines. The background of the entire slide is a solid dark teal color.

Panel Discussion #2
TPRM through the Lens of
Business Associates, Suppliers,
Vendor Organizations

TPRM Panel Discussion - *Through the Lens of Business Associates / Suppliers / Vendor Organizations*



Facilitator
Matthew Webb, AVP Product Security; Chief Product Security Officer



David Houlding, Director, Global Healthcare Business Strategy, Health & Life Sciences



Glen Braden, Principal and CFO/ CIO



Pamela Nigro, VP, Security Chair, Board of Directors, ISACA



Panel #3
TPRM – A Better Way
Forward



TPRM Panel Discussion - A Better Way Forward



Facilitator
Matthew Webb, AVP –
Product Security, Chief Product
Security Officer



John Houston,
VP, Information Security and Privacy



Britton Burton,
Senior Director of Product Strategy



Brenda Callaway, Divisional VP
Operations Performance Management



Jeremy Huval, Chief Innovation Officer



Health3PT Accomplishments

- Have united cyber leaders in healthcare to address critical challenges of vendor cyber risk
- Developed a Health3PT - Health Industry Recommended Practices for Cyber Risk
- Finalizing the Health3PT - Recommended Practices Implementation Guide
 1. Concise contract language tying financial terms to a vendor's transparency, assurance and collaboration on security matters
 2. Risk tiering strategy that drives frequency of reviews, extent of due diligence and urgency of remediation
 3. Appropriate, reliable, and consistent assurance of the vendor's security capabilities
 4. Follow-up through to closure of identified gaps and CAPS
 5. Recurring updates of assurance of the vendor's security capabilities
 6. Metrics and reporting on organization-wide vendor risks
- Working with CORL Technologies and HITRUST to enable the Initiative and Recommended Practices

How to Get Started

- Join the Health3PT Initiative
- Express your opinions in the Health3PT TPRM Survey
- Promote your organization's HITRUST Certification on the Health3PT Vendor Directory
- Adopt the Health3PT Initiative Recommended Practices
 - Relying Parties – If your vendor provides you with a validated assessment such as a HITRUST Certification, then eliminate the redundant surveys and questionnaires
 - Vendors - Start today by leveraging the HITRUST traversable assessment portfolio e1, i1, and r2
 - Relying Parties and Vendors can leverage CORL Technologies' CORLcleared™ platform that will enable much of the Health3PT Recommended Practices and integrates the HITRUST Assessments
- Formation of key committees – Standards, Education, Events, Membership
- Look for the next Health3PT Summit in October

Q&A



Thank you

