Health3PT

VENDOR RISK MANAGEMENT SUMMIT

Monday, October 2, 2023

10:00 AM – 4:00 PM

Gaylord Texan Resort and Convention Center Grapevine, TX

These informational sessions are open to the public. Participants have no expectation of confidentiality.

Opening remarks

“The future is now”

Matthew Webb
AVP – Product Security; Chief Product Security Officer

HCA Healthcare

TPRM IS BROKEN

Using Collaboration to Remodel Vendor Risk Programs

VENDOR BREACHES ARE DETERIORATING HEALTHCARE'S DIGITAL FOUNDATIONS

55%

percentage of healthcare organizations suffered a third-party data breach in the past year[2]

$10.1m

average cost of a breach for healthcare organizations[3]

100

number of covered entities impacted by the recent breach of Avamere vendor

1.1 million

patients impacted by breach of OneTouchPoint vendor involving over 37 prominent healthcare organizations

2.8 GB

amount of data stolen in a recent cyber breach from Cisco, a prominent provider of network services for healthcare organizations

>1,000

average number of vendors under contract by each healthcare provider in the U.S.

49%

of organizations have a comprehensive inventory of all third parties that have access to their systems[4]

Health3PT Initiative

What is the Health 3rd Party Trust (Health3PT) Initiative?

- A proactive group committed to reducing third-party information security risk with more reliable and efficient assurances
- Established to evaluate, identify, and implement actionable and practical solutions that healthcare organizations can adopt to provide more reliable assurances, consistent information security program reporting, and better visibility into downstream relationships with third parties and beyond

Who leads the Health3PT Initiative?

- Professionals from leading care providers, health systems, and other healthcare organizations
- The Health3PT Council is committed to developing, recommending, and promoting a series of practices and solutions to effectively manage information security-related risks with supply chain vendors and service providers to protect patient information, electronic medical records, and business information.

Health3PT Council Organizations

These informational sessions are open to the public. Participants have no expectation of confidentiality.

Health3PT Council Members

Patricia Yarabinetz, AmeriHealth Caritas
Cindy Shuna, Amerisource Bergen
Rick Kratz, Amerisource Bergen
Glen Braden, Attest Health Care Advisors
Dr. Omar Sangurima, Memorial Sloan Kettering Cancer Center
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
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

State of the Health3PT Initiative

- 1700 individuals have engaged with Health3PT
- >220 relying parties and vendors are participating organizations
- 109 HITRUST certified organizations are listed on the Health3PT Vendor Directory
- Developed *Health Industry Recommended Practices and Implementation Guidance* for TPRM
- HITRUST Assurance Program selected by Health3PT in alignment with Recommended Practices

Health3PT Vendor Summit Agenda

Time	Topic	Presenters
10:00 - 10:20	Open and Welcome	Matthew Webb, HCA
10:20 - 11:00	Health3PT TPRM solutions “Implementing the Health3PT Recommended Practices”	Brenda Callaway, HCSC
11:00 - 11:30	Building an IT Security partnership with your customer	Lee Penn, PDHI (panel)
11:30 - 12:15	Best practices for risk triage and leveraging HITRUST assessments, and the HITRUST Assessment XChange for your vendor risk program	Ryan George, UPMC
12:15 - 1:15	**LUNCH BREAK**	
1:15 - 2:00	Best Practice end-to-end process leveraging CORLcleared	Matthew Webb, HCA Britton Burton, CORL Technologies Lee Penn, PDHI
2:00 - 3:00	Vendor Feedback Session and Q&A session with Health3PT Council	Matthew Webb, HCA
3:00 - 3:15	Final Q&A and Wrap-up	Matthew Webb, HCA
3:15 - 3:30	**BREAK**	
3:00 - 5:00	**Health3PT Networking**	

Implementing the Health3PT Recommended Practices

Brenda Callaway

Divisional VP, Operations Performance Management

HCSC Health Care Service Corporation

Health3PT Recommended Practices

There is a wide range of Third-Party Risk Management (TPRM) practices adopted across the healthcare industry.

- TPRM practices adopted across the healthcare industry are decades old and adopted from processes used by other industries.
- The variety in approaches results in inconsistent and unclear risk management outcomes, as evidenced by vendor-related security events and breaches of Protected Health Information (PHI) and other sensitive information by business associates.
- Urgent need for new standards that are consistent, repeatable, and reliable
- It is critical that healthcare organizations act now to revolutionize TPRM practices to keep up with emerging cyber threats and the adoption of cloud, AI, and other innovations.
- In response to this urgent situation, healthcare leaders established the Health3PT Initiative to transform TPRM practices to align with modern-day risks.

Health3PT Recommended Practices

Health3PT has ratified Recommended Practices to drive:

1. Concise contract language tying financial terms to a vendor's transparency, assurance, and collaboration on security matters
2. Risk tiering strategy that drives the frequency of reviews, the extent of due diligence, and the urgency of remediation
3. Appropriate, reliable, and consistent assurances about 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

(1) Concise contract language tying financial terms to a vendor's transparency, assurance, and collaboration on security matters

Health3PT Implementation Guidance	Industry Action	Benefits
Implement Consistent and Appropriate Contract Language	Use unambiguous language between healthcare industry companies and third parties.	1. Documented scope and characteristics of the systems or services supporting the healthcare industry. 2. Defined the ownership and confidentiality of data in scope for the system, management requirements, and disclosure expectations. 3. Clarify risk management, security, and assurance expectations.

(2) Risk tiering strategy that drives frequency of reviews, extent of due diligence, and urgency of remediation

Health3PT Implementation Guidance	Industry Action	Benefits
Use Third-Party Characteristics to Identify and Assess Inherent Risk and Guide Required Level of Security Assurance	Use business and technical characteristics to assess and classify risk and to specify appropriate levels of security assurance.	1. Engage all third-party relationships and not only those above a certain level of inherent risk. 2. Provide flexibility for different risk levels. 3. Invite partnerships with business stakeholders with third-party relationships to understand and agree on risks and support negotiation and engagement. 4. Clarify security assurance requirements that fit each relationship and support the industry.

(3) Appropriate, reliable, and consistent assurances about the vendor's security capabilities

Health3PT Implementation Guidance	Industry Action	Benefits
Ensure Reliable and Transparent Assurances are Received from Third-Party Entities	Document the security requirements of the system and acceptable validation mechanisms to test and document that controls are operating as intended. Collect consistent and repeatable security assurances from third-party companies.	1. Drive collaboration between all parties on risk management expectations and sharing of assurance outcomes. 2. Provide transparency for internal and external stakeholders on control specifications, maturity requirements, and scoring expectations. 3. Enable results that are consistent and available to all health industry participants without regard to status as an assessed entity, relying party, or which assessor(s) are used. 4. Ensure applicability, repeatability, and consistency of assurance results.

(4) Follow-up through to closure of identified gaps and CAPS

Health3PT Implementation Guidance	Industry Action	Benefits
Close the Loop on Identified Risks and Sustain the Relationship with Third-Party Entities	Ensure that gaps and CAPs, where identified, are shared and that progress towards addressing issues is known and understood.	1. Clarify remediation expectations, where found, and offer an understanding where remediation is not needed. 2. Promote maturity and transparency in the long-term relationship between health industry companies and third parties.

(5) Recurring updates of assurance of the vendor's security capabilities

Health3PT Implementation Guidance	Industry Action	Benefits
Manage the Ongoing Relationship and Seek New Information as Risks and New Security Requirements Emerge	Rely on assurance systems that remain relevant as risks and threats evolve and adjust risk expectations and assurance requirements accordingly.	1. Ensure assurance requirements evolve as risks and threats evolve. 2. Understand how changes in inherent risk and progress towards higher levels of assurance add value to relationships and the industry. 3. Leverage capabilities from service providers to inherit security capabilities and document shared responsibilities.

(6) Metrics and reporting on organization-wide vendor risks

Health3PT Implementation Guidance	Industry Action	Benefits
Track the System of Third-Party Risk across Multiple Vendors for the Organization	Use technology to meet the scale of the healthcare industry while also enabling wider and more specific risk management.	1. Improve the efficiency of healthcare companies and third-party suppliers through systematic sharing of metrics. 2. Drill down into specific control areas across a network of third-party suppliers. 3. Reduce effort for third-party suppliers in sharing security assurances with multiple health industry companies.

Key learnings and actions

- Health3PT has established a template that truly solves the third-party risk.
- Problems that once seemed unsolvable are now solvable.
- By working with HITRUST and CORL, solutions are now available to the market that were not there before.

The future is now –
We must unite and take action together to beat the 'bad guys.'

Building an IT security partnership with your customer

Lee Penn
Chief Financial Officer

pdhi

Building an IT security partnership with your customer

Begins with leadership commitment to building a culture of security and compliance

1. Declare that the company's security posture is a key component of its value proposition
2. Put responsibility for security explicitly into everyone's role
3. Create solutions where security is a fundamental part of solution design and doing the "right thing" is automatic (e.g., always-on VPN, MFA)
4. Expect every function to use the company's robust security posture to its advantage
5. Make your customer aware of the benefit it receives from this security posture
6. Ask your customer to work together with you to maintain and improve it

A quick history of PDHI

PDHI is a small company that provides SaaS deliverables from its ConXus Platform to entities that deliver employee wellness and population health management programs.

It is often the case that our client's IT security or third-party risk management groups have more people than all of PDHI.

In 2013, I came away from that year's HITRUST conference understanding that HITRUST made a promise to me and PDHI that the HITRUST CSF would:

- Eliminate questionnaires
- Enable small healthcare companies to work with big healthcare payors and providers
- Allow covered entities and business associates to work together to "beat the bad guys"
- Improve the limits and costs of cyber security insurance
- Allow company IT security dollars to be returned to other functions

Elements of the “big picture” to consider are:

- The bad guys only need to succeed occasionally, but the good guys need to **win at every encounter.**
- Individual entities cannot be successful on a stand-alone basis
- PDHI having a robust IT security posture is necessary to be accepted and successful as a service provider in the healthcare market
- Having our clients be confident and comfortable with PDHI’s security posture allows:
  - More effort to be dedicated to the development and delivery of PDHI’s service solutions
  - Shrinkage of the time needed to get from first introduction to the implemented solution
  - More reasonable contract terms
  - A measure of **trust between the parties** to grow from the beginning of the relationship

Obtaining HITRUST certification is just one element of the “big picture”

How it is used is another...

...and what you can accomplish with it yet another.

Use Your HITRUST certification to eliminate size disparity

Embed your HITRUST-generated security posture into your company culture

- From the top down – whether it's the CEO or the customer support rep, security is part of their thinking every day
- Building the security posture into all functions (e.g., product development, marketing, customer support), not just the IT functions
- Keeping in mind that employees' behaviors are a BIG part of the problem (e.g., human error, stolen credentials) and their attitude, level of awareness, training, and actions are MOST of the answer
- Pointing out to clients how features in your products and processes ease their IT security burden
- Making an explicit point of your security posture when marketing, selling, implementing, developing, and supporting your product

Uses to which your HITRUST assurance report can be put

- Evidence that your company is serious about its obligations to meet security and privacy requirements
- Enlightening discussions with clients and prospective clients about PDHI's security posture and how that allows them to achieve a better risk profile
- Arguing for improved limits and premiums with your cyber insurer
- Reassuring the company's board of directors and investors that cyber risk is being adequately addressed

Eliminating Questionnaires by Leveraging your HITRUST Certification

PDHI's answer is in its Services Agreement

- In the Section: Right to Conduct Assessments; PDHI Due Diligence Statement.
  - PDHI agrees to provide ABC Health Plan the PDHI HITRUST CSF Assurance Report as described above in the first section of this Attachment G HITRUST CSF CERTIFICATION RESPONSIBILITY whenever it is published or its status changes.
  - Additionally, if PDHI scores **at high risk** as determined by ABC Health Plan's third-party risk management procedure, PDHI agrees to fully cooperate with, and complete a Due Diligence/Security Assessment performed by ABC Health Plan and/or any designated representative or vendor.

Eliminating Questionnaires by Leveraging your HITRUST Certification

PDHI's Continuing Problems are:

- Many customers do not yet accept this approach
- The idea of partnering with a vendor about IT security is a foreign concept
- Third-party GRC organizations are usually more inflexible than customers themselves
- Reluctant clients must be pushed (sometimes hard)
- Not enough vendors push which makes it more difficult for those that do
- Too many customers require HITRUST certification but do not respect it

Responding to Questionnaires by Leveraging your HITRUST Certification

PDHI doesn't fill out questionnaires – we respond with our Security Package and begin a dialog on Security and Compliance.

- Questionnaires are not reliable assurances and create non-value-added work for both the customer and vendor.
- The PDHI Security package exceeds other forms of assurance. It is holistic and comprehensive. It provides:
    - Security and Compliance Overview
    - HITRUST Risk-based 2-year (r2) Certification Report
    - Azure YYYY - HITRUST Certification Letter (ConXus is in the Azure cloud)
    - Web Application Penetration Test Summary for MM/YYYY

Responding to Questionnaires by Leveraging your HITRUST Certification

We provide a Security and Compliance Overview in just seven pages with these sections:

- Introduction
  - What is ConXus
  - Information Stored and Processed in ConXus
  - Regulations Applicable to ConXus
- Information Security
  - Information Security Management
  - Corporate and Operational Security
  - Product Security
- Compliance (Regulations, Third Party Assurance, Certifications)
- Reliability (Multiple Data Centers, Backups, Business Continuity and Disaster Recovery)

Results from this approach with ABC Health, a prospective client:

The discussion is elevated to judging PDHI's security posture and the risk it is to be assigned by ABC Health's Third-Party Risk Management process - not grinding through answers to questions.

- Prospects can focus their questions because they are based on the PDHI Overview, the details of the service solution, PDHI's HITRUST CSF domain scores, and the controls that are most important to ABC Health.
- Prospects can understand that its TPRM program insights are welcomed by PDHI and that PDHI takes such input as another source of information about what it can do to make the ConXus Platform and the company's procedures more secure.
- Prospects can understand that PDHI is dependent on the prospect performing its obligations since, given the interconnected nature of the service solution, a mistake by the prospect can generate a security incident for PDHI (e.g., incorrect information in the eligibility file).
- PDHI ends up with the Attachment G wording in the contract because the prospect's TPRM team has come to trust PDHI enough to okay this approach.

Final Thought

Health3PT Objectives

- The Health3PT is committed to developing, recommending, and promoting a series of practices to establish trust by more effectively and consistently managing information security-related risks throughout the third-party ecosystem.

PDHI's Perspective

- PDHI uses its customer's third-party risk management process as one of many ways to build a relationship based on trust between PDHI and its customer!

Best practice for risk triage and leveraging HITRUST assessments and the HITRUST Assessment XChange for your vendor risk program

Ryan George

Senior Director of Information Security

UPMC

LIFE CHANGING MEDICINE

Agenda

- Background
- The problem and challenges of vendor risk
- Why UPMC Chose HITRUST
- Proper Risk Tiering
- Proper Contract language
- Vendor assurance journey
- On-going remediation and management of vendor risk

The Changing IT Landscape

Y2K

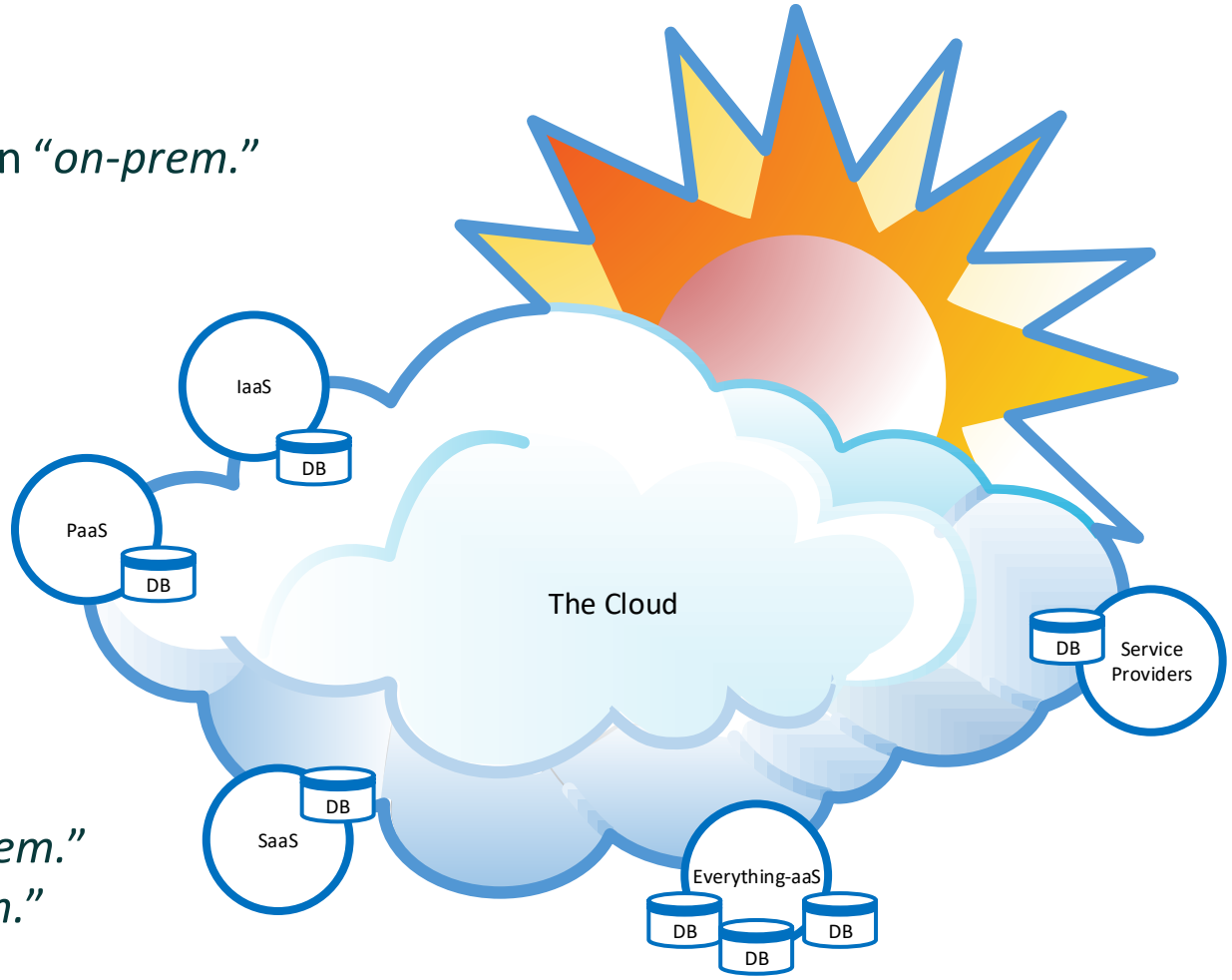
- 95% of all applications were run *"on-prem."*
- 95% of all newly-acquired applications were run *"on-prem."*
- Little data or *"workload"* was in the cloud.

Today

- 50% of all applications run *"on-prem."*
- < 20% of newly-acquired applications run *"on-prem."*
- Many copies of an organization's data is in the cloud.

2028

- At most, 25% of all applications will run *"on-prem."*
- < 10% of newly-acquired applications *"on-prem."*
- Most of these will be utility in nature.



Health3PT

The Stakes Are Changing

BECKER'S HEALTH IT

Health system to pay patients $4K each for data breach

Giles Bruce - Thursday, January 12th, 2023

Save Post Tweet Share Listen Text Size Print Email

Gallup, N.M.-based Rehoboth McKinley Christian Health Care Services has agreed to pay victims of a 2021 data breach up to $4,000 each, according to a recent federal court filing.

In February 2021, the health system discovered a cybersecurity incident where, in the weeks prior, hackers stole the data of 191,009 individuals. The data included Social Security numbers, driver's license numbers, and medical and financial information.

The proposed class-action settlement, which a judge approved Jan. 9, offers up to $3,500 for "extraordinary losses" and reimbursement for out-of-pocket expenses and lost time up to $500, as well as two years of free credit monitoring services. Rehoboth McKinley Christian also agreed to cybersecurity improvements.

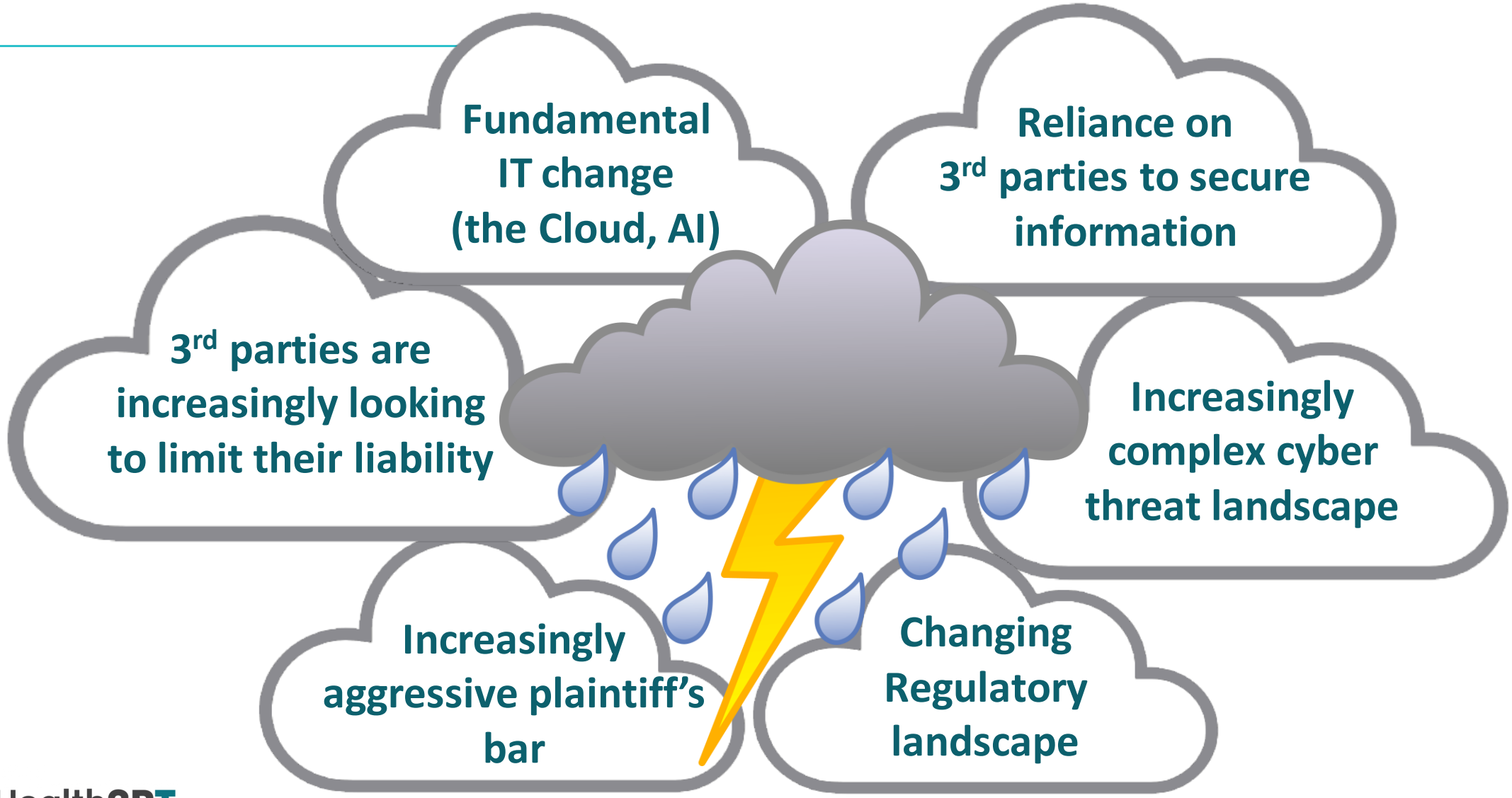
A final approval hearing for the settlement is set for May 24. The news was first reported Jan. 10 by *Bloomberg Law*.

The Math

The unanswered question is – how many of the 191,000 patients qualified for the full amount?

- **Worst-case scenario** (all class members get the full amount) - the Health System would pay **$764MM**
- If 10% receive the full amount and the others get $500, then the total would be **$162MM**
- If 5% receive the full amount and the others get $50, then the total would be **$47MM**

The Perfect Storm



Health3PT

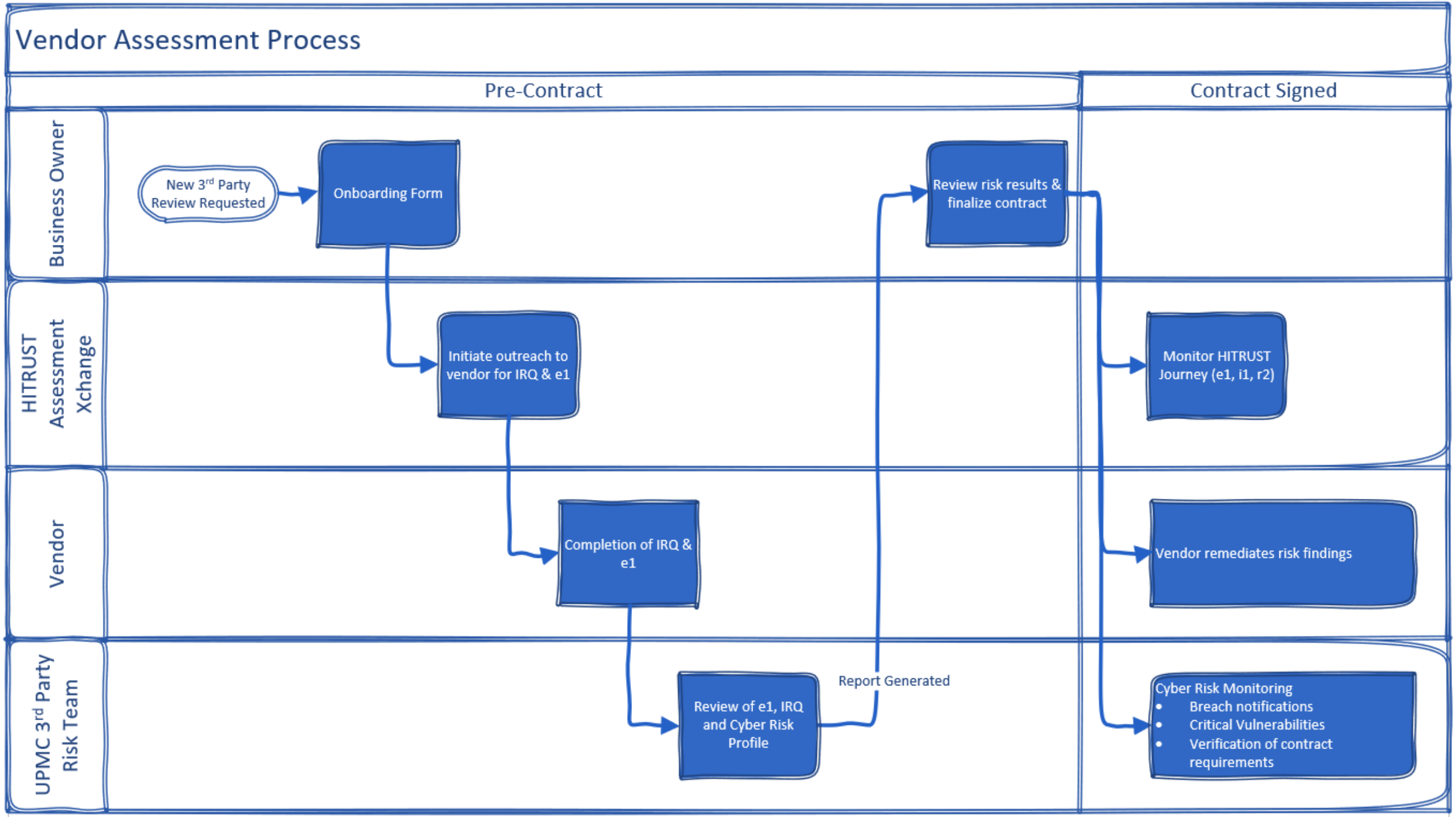
Why UPMC Chose HITRUST

UPMC had a need for a framework that incorporated security requirements from International (ISO), federal (HIPAA, FFIEC, HITECH), state, third party (PCI) and other government agencies (NIST, CMS).

81% of US Hospitals/ Health Systems use HITRUST CSF; 83% for Health Plans

e1 assessment ensures most critical cybersecurity controls are in place and helps demonstrates good cyber hygiene

Tiering of assessments allows UPMC to tailor our HITRUST assessment request based on Inherent Risk Factors

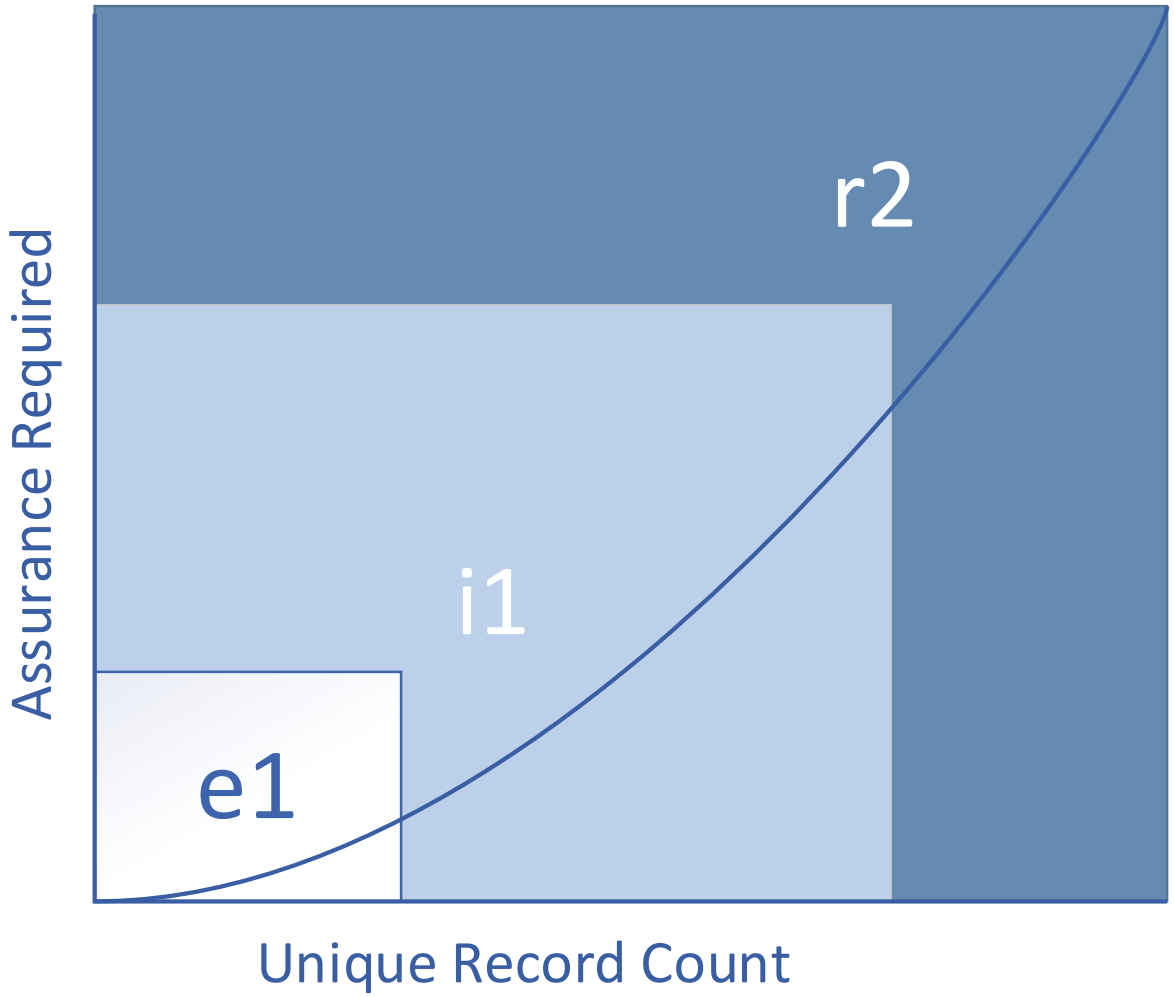

Vendor Assessment Process
Pre-Contract
Contract Signed
Business Owner
HITRUST Assessment Xchange
Vendor
UPMC 3rd Party Risk Team
New 3rd Party Review Requested
Onboarding Form
Initiate outreach to vendor for IRQ & e1
Completion of IRQ & e1
Review of e1, IRQ and Cyber Risk Profile
Report Generated
Review risk results & finalize contract
Monitor HITRUST Journey (e1, i1, r2)
Vendor remediates risk findings
Cyber Risk Monitoring
Breach notifications
Critical Vulnerabilities
Verification of contract requirements

Inherent Risk Questionnaire

- Number of Records (stored, processed, backed up)
- Data Retention – How long does vendor store, archive, or otherwise retain Data
- Any laws / regulations that require the vendor to retain Data for a specific period?
- Specify the location and type of environment where data is stored
- Which third-party tools / services used to manage, transfer, and/or maintain Data?
- Use of 4th Parties (similar questions asked above)

Proper Risk Tiering

After doing the e1 Self-Assessment, UPMC requests a HITRUST validated assessment based on several factors but mostly number of unique records



Contract language

- For any vendor holding sensitive information, the 3rd party must:
  - Participate in HAX e1 assessment process and receive & maintain a score of >90
  - Obtain and maintain HITRUST certification based on criteria set by UPMC
  - Penalties for not meeting deadlines or failing to maintain HITRUST certification

- E1 self-assessment prior to contract signing then, based on the level of assurance needed, vendors are tiered and given the associated timelines below:
  - e1 validated in 12 months
  - i1 validated in 12 months
  - r2 validated requires i1 in 12 months then r2 in 24 months

Continuous Monitoring

Data Breach Notifications (Black Kite)	• Alerts when dark web IOC are found for one of our vendors
Critical Vulnerabilities (Black Kite)	• Compare e1 response vs. reality • Communicate critical vulnerabilities and request remediation
HITRUST Status (HAX)	• Ensure vendors maintain expected level of certification • Track remediation and closure of CAPs
Data management	• Reducing the # of records that are shared • Challenging Vendors the retention requirements • Requesting more secure long-term storage when they must retain data

Time is of the essence

- Hackers are becoming bolder and more sophisticated.
- Cyber events are resulting in substantial higher financial impact (litigation, ransom, fines, etc.)
- UPMC has BoD level engagement and direction to address 3rd party risk (including protecting PHI and addressing financial risk).
- Partner with Health3PT and use the easy-to-follow “Recommended Practices” for relying parties and vendors

Health3PT

Lunch Break 12:15 - 1:15

Room Grapevine Ballroom A

These informational sessions are open to the public. Participants have no expectation of confidentiality.

Best practice end-to-end process leveraging CORLcleared

Matthew Webb

Associate Vice President, Product Security
HCA Healthcare

Lee Penn

Chief Financial Officer

PDHI

Britton Burton

Senior Director of Product Strategy,
CORL Technologies

Vendor feedback session and Q&A session with Health3PT Council

Matthew Webb,
AVP – Product Security; Chief Product Security Officer
HCA Healthcare

Vendor Feedback Session and Q&A session with Health3PT Council

Matthew Webb
AVP – Product Security, Chief Product Security Officer

HCA Healthcare

Joe Dylewski
Lead, Technology and Cybersecurity Risk

Humana

Ryan George
Senior Director of Information Security

UPMC
LIFE CHANGING MEDICINE

Glen Braden
Principal and CFO/ CIO

ATTEST

Brenda Callaway
Divisional VP Operations Performance Management

HCSC
Health Care Service Corporation

Amanda Gallagher
Manager, Security Risk Management

CVS Health

Q&A

Matthew Webb,
AVP – Product Security; Chief Product Security Officer
HCA Healthcare

Key Takeaways

- TPRM is broken and costs the industry hundreds of millions of dollars annually.
- Third-party vendors cause most incidents/breaches.
- Historical systems and processes for TPRM are failing and not scalable or reliable.
- The Health3PT Council has developed an effective and scalable approach to TPRM that solves this once unsolvable problem.
- Today, we demonstrated that effective TPRM is possible for both relying parties and vendors.

The future is now. We must act now with the tools and solutions being delivered by Health3PT.

Networking Session

Eric Rozier

Executive Director, Health3PT Initiative

Director, Client Development, HITRUST

HITRUST®