Health3PT Recommended Practices

There should be no debate that third parties pose a risk to the healthcare industry with the potential to compromise privacy and safety. To manage this third-party risk, health industry organizations must effectively manage third-party information risk. This requires that they understand the risk from third parties, obtain relevant information about the controls in place to mitigate those risks, and have assurances that the information is accurate.

There is a wide range of Third-Party Risk Management (TPRM) practices adopted across the healthcare industry—many that 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. Out-of-date approaches to TPRM have not evolved to keep pace with the use of cloud and other technological innovations in the healthcare industry. They also fall short of the floor set by the Office for Civil Rights for reasonable and appropriate safeguards and practices. These ineffective risk management processes, coupled with an increase in vendor-related breaches, continue to undermine member and patient confidence. This leads to an increase in litigation, including class action lawsuits, that ultimately slow down or prevent innovations that are transforming the delivery of care.

The shortcomings of today's TPRM practices in healthcare include

1. No overarching methodology for risk-tiering vendors
2. Over-reliance on verbose contract terms
3. Extensive and inconsistent questionnaires that try to identify or evaluate control weaknesses
4. Limited and inconsistent validation of information collected
5. Limited follow-up and resolution of identified gaps
6. Point-in-time assessments that are rarely updated
7. Limited organization-wide insight into vendor security risk

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, leaders in healthcare established the Health 3rd Party Trust ("Health3PT") Initiative to transform TPRM practices to align with modern-day risks. Many of the industry's largest covered entities and globally recognized technology and healthcare solution providers have come together to affirm a series of practices and develop guidance for proper implementation.

The practices ratified by Health3PT include

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 assurances about the vendors' security capabilities
4. Follow-up through to closure of identified gaps and corrective action plans (CAPS)
5. Recurring updates of assurance of the vendors' security capabilities
6. Metrics and reporting on organization-wide vendor risks

TPRM in healthcare is now mostly a check-the-box exercise that exposes organizations to unnecessary risk and slows down innovation. Establishing and adopting these practices will transition it to become effective and efficient in managing third-party risk and clearing away obstacles for the rapid adoption of technological advancements.

Adoption will help ensure organizations meet the spirit and the letter of Health Insurance Portability and Accountability Act (HIPAA) Security Rule requirements regarding the provision of 'satisfactory assurances' from their third parties and help qualify for potential mitigations from regulatory fines and penalties.

Health3PT Implementation Guide

Purpose: An implementation guide to help organizations implement and operationalize the recommended practices created by the Health3PT Initiative for the healthcare industry.

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 frequency of reviews, extent of due diligence, and 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

Implementation Approach: Health3PT has approved HITRUST as the first assurance supplier supporting these recommended practices for the healthcare industry. The HITRUST e1, i1 and r2 assessments all support healthcare industry organizations seeking to collect evidence of appropriate, reliable, and consistent assurance of their vendor's security capabilities. And the HITRUST Assurance Program provides the supporting infrastructure needed for the industry to collect assurances, report-on risk, track risk, and manage risk across the industry.

Implementing Consistent and Appropriate Contract Language

The industry is seeking relationships including ***concise contract language tying financial terms to a vendor's transparency, assurance, and collaboration on security matters.***

Clarity is essential. When all healthcare industry stakeholders and those they serve share a clear and common set of expectations, complexity will be reduced, and transparency enhanced. Historically, companies have all had their own, different expectations with suppliers, vendors, and customers—all requiring various levels of engagement about security maturity. Consistent and appropriate contract language provides the foundation for security outcomes and is required to achieve and sustain required security outcomes. Defining the expectations between parties, the mechanisms acceptable in defining what is being protected, and the measures acceptable in assessing and validating security maturity will lead to this much-needed clarity for all participants in the healthcare industry.

As importantly, the healthcare industry can reduce overhead for security by gaining efficiencies through common expectations, while preserving organizations' independence. This will allow a higher percentage of every security dollar to be invested in security outcomes.

Unambiguous language between parties provides a needed foundation for security risk management and assurance. Contracts should include the following considerations to support consistent expectations. Illustrative language for members of the healthcare industry is available from Health3PT members at health3pt.org/resources. This language includes a framework for recommended definitions and terms.

Some healthcare industry companies have observed that a discussion and calculation of inherent risk and identification of assurance levels using guidance presented in this document will support contract negotiation. Companies are, therefore, encouraged to consider an integrated approach instead of approaching contracting and consideration of inherent risk as sequential steps. This may create efficiencies and ease the clarity of understanding importance to the relationship between the companies and selection of the required assurance level by the healthcare industry company.

At a minimum, contracts between vendors and suppliers should address the following.

1. **Scope of the System and Data**
   The scope and characteristics of the systems or services used in support of the healthcare entity should be specified clearly and in a manner understood by all parties. This supports risk assessment of the healthcare entity and the data supported by the system. It also ensures that all parties understand assurance expectations. The scope description should include all data that requires protection and the technology supporting the system. At a minimum, the contract should specify

   I. The **classification of data,** including whether the data is public, confidential, and/or protected by one or more regulatory expectations. For example, the contract should specify if the scope of the system stores or processes data that is Personally Identifiable Information (PII) or Protected Health Information (PHI/e-PHI).

II. The **characteristics of the system(s),** including where the data is stored, when/if the data is transmitted within the system and across system boundaries, and processing locations. More specifically, the use and location of cloud services should be identified. Cloud services distribute security expectations and may create opportunities to gain efficiency by using the security engineering, security maturity, and security assurance already provided by relevant service providers. It is also important to specify the allowed physical locations where data may be stored and the allowed locations of staff supporting the system (such as only in the United States), if necessary.

III. **Regulatory requirements,** such as obligations to comply with HIPAA must be identified. This includes the HIPAA Security Rule, where Protected Health Information (PHI/e-PHI) is present as well as relevant state regulations which must be specified in the contract. Where other forms of regulated or protected data exist, other obligations may be needed and should also be specified (e.g., PCI obligations where payment card data is present).

2. Data Ownership, Use, Disclosure, and Management Requirements

It is important to consider the ownership and confidentiality of all data in scope for the relationship and to identify expectations for governance of the data. Clarity reduces the risk of data being used or reused in a manner other than intended by the scope of the relationship. For example, contracts should consider unambiguous language permitting or restricting the reuse, transfer, or sale of data. Other considerations include

I. Data management and use of the data during the relationship term
II. Mechanisms to secure data
III. What data updates are required of the healthcare industry company during the relationship term
IV. Process for returning or destroying data at the end of the relationship

3. Risk Management and Security Expectations and Safeguards

The expectations for protecting the system and data in scope for the relationship, the control expectations, and requirements for administrative, physical, and technical safeguards should be specified. However, the desire to ensure that security requirements are specified clearly and completely creates a temptation to develop contracts that attempt to cover all security requirements and expectations. The complexity and breadth of modern technology systems make it challenging to define contract language that is both specific and broad enough to provide the spectrum of necessary security controls and safeguards.

Just as critically, the approach to security required by the contract must remain relevant as security needs and technology change. It is important that the contract requirements do not become obsolete as technology evolves and new risks are discovered.

The healthcare industry should, therefore, base security expectations on appropriate assurance systems referenced in contracts. This will allow for specificity and tailoring of security safeguards and control selection that are

I. Appropriate to the scope of the system
II. Suitable to the inherent risk based upon a documented risk analysis
III. Aligned with and fulfilling of regulatory expectations
IV. Continuously relevant as risks and threats evolve
V. Appropriate to the healthcare industry and between the parties

Such assurance systems allow controls to be selected based on risk, provide clarity of scope between all parties and—most importantly—provide a mechanism to assess controls and prove that controls are implemented and working at the expected level of maturity.

The security requirements, along with required assurance systems, will provide the health industry with the framework to protect systems and the data they contain. Scope and security expectations specified in the contract are important inputs to the use of an assurance system and include the following.

I. How data will be accessed? How access will be authenticated? What employee background checks and training are expected?
II. What foundational/core security capabilities are expected, including but not limited to software maintenance, patching, antivirus, encryption, and authentication?
III. What coverages and levels of cybersecurity insurance are required for the third party? What control systems or frameworks are required to prove security maturity, including assurance and reporting systems, such as the HITRUST CSF?
IV. What assessment expectations exist, such as the frequency and rigor of assessments and the timeliness, rigor, and consistency of approach?
V. What are the expectations for areas where security controls are not present or where required improvements in security maturity are observed, including timelines, evidence, and required retesting?
VI. What are the requirements or security event or breach reporting, response, notification, transparency, remediation, and communication?
VII. What performance guarantees and penalties in the case of security requirements not being achieved, sustained, or reported as specified?

Use Third-Party Characteristics to Identify and Assess Inherent Risk and Guide Required Level of Security Assurance

*The industry requires a **risk tiering strategy for third-party entities that drives frequency of reviews, extent of due diligence, and urgency of remediation.***

The unique requirements across the healthcare industry, along with variety among vendors and suppliers create complex challenges. Security expectations must be consistently met, but there must also be flexibility to address different risk levels. A consistent risk analysis and tiering system will allow for the application of security requirements and resources where risk is highest without discounting or ignoring relationships where risks may be lower.

Health3PT is seeking a risk tiering model for the healthcare industry that promotes engagement with ***all*** third-party relationships and not only those above a certain level of inherent risk. This is important because industry breach data indicates that third parties with lower inherent risk may be more likely to experience security events, often because they have not invested in a minimum level of foundational security.

There are many ways that stakeholders can assess and measure risk between parties in the healthcare industry. Health3PT has developed a system that is clear, easy to understand, and provides transparency between all parties. It uses a scoring model that reflects the inherent risk in the relationship that can be used to select an appropriate level of security assurance.

Enterprise risk management and information security leaders should collaborate with business stakeholders who own third-party relationships to understand and agree on the risks that require mitigation. This is critical to building a sustainable system. It allows business leaders to understand and consider risk management concerns and consider them throughout business negotiations and in engagements throughout their long-term relationships. The characteristics of the relationship can be assessed in three dimensions — organizational factors, compliance factors, and technical factors.

1. Questions asked using business terms can help lead conversations about organizational and compliance risk factors among stakeholders. What data does the third party access and process? How much of that data do they have?
2. How would we be impacted if that data were inappropriately accessed or disclosed?
3. How would others, including our patients or members, be impacted if that data were inappropriately disclosed or leaked?
4. How critical is the third party to our business? What happens if they have a security event that makes them unable to operate or perform work for us?
5. What are our responsibilities and liabilities if the third party has a security or compliance issue?

The business goal of risk analysis is to decide what level of risk management is appropriate based on the risks of the relationship and what measures should be taken to achieve the expected risk management outcomes. This is done by

1. Assessing the potential impact of the product and/or service on the organization
2. Evaluating the third party on specific risk factors
3. Classifying or tiering the third party based on inherent risk
4. Determining the type of risk assessment needed for appropriate assurance

Ultimately, the healthcare industry company owns the risk assessment and sets the required level of security assurance. However, the healthcare company and the third party will often need to collaborate on the identification and scoring of risk factors. For example

1. The healthcare company should address and score organizational and compliance factors such as the identification of data, the quantity and percentage of data, criticality of the relationship, and compliance expectations.
2. The third party may need to identify and characterize the technical factors—especially where they are running a system or platform.

Understanding each vendor's inherent risk level allows organizations to assign specific assurance requirements on a vendor-by-vendor basis. The level of assurance will be set in proportion to the level of inherent risk in the relationship, with higher levels of assurance being required of the highest-risk third parties to create broader and deeper coverage of security expectations. In general, third parties that pose low inherent risk require lower levels of assurance. They may be managed through a reliable self-assessment that affirms they have implemented foundational or essential cybersecurity. This also establishes the foundation for ongoing security risk management discussions between healthcare industry companies and all vendors including those with lower inherent risks.

Organizations with higher levels of inherent risk require a more robust, in-depth assessment and certification process.

Here is an example of this process using the HITRUST risk triage approach.

Inherent Risk Score	Inherent Risk	Required Level of Assurance/Score Range	Recommended HITRUST Assessment/Score
0	Negligible	Minimal 0 – 12.5	N/A
1	Very Low	Very Low 12.5 – 59	e1 Self/Readiness 56.4
2	Low	Low 60 – 69	e1 Cert., No CAPS 69.6
3	Moderate	Moderate 70 – 79	i1, CAPs Allowed 71.5
4	High	High 80 – 89	r2, CAPs Allowed 93.8
5	Very High	Very High 90 – 100	r2 Cert., No CAPs 93.8

It is important to note that risk tiering allows for engagement with ***all third-party relationships*** *and not only those above a certain level of inherent risk.*

Third parties with lower inherent risk may be those more likely to be impacted by security events.

Ensure Reliable and Transparent Assurances are Received from Third-Party Entities

*Evidence of **appropriate, reliable, and consistent assurance of the vendor's security capabilities** is essential to the management of third-party information risk.*

Clear and transparent understanding of security maturity is essential for healthcare industry stakeholders. This is described as assurance. It requires

1. Clear documentation of the requirements of the system
2. Appropriate validation mechanisms to test and document that controls are implemented and operating as designed
3. Scoring models that allow for consistency and repeatability of results between assessors
4. Infrastructure to collect assessment evidence for quality assurance purposes and securely share reports across the industry
5. Proper independence of testing and quality review equal to the rigor expected from the assurance system

Health3PT considers assurance an ongoing process with controls evaluated periodically based on assurance levels that correlate to inherent risk. The level of inherent risk drives the assurance level requirement. In some situations, health industry stakeholders may seek higher assurance levels.

1. Higher assurance levels could permit assurances to be valid for longer periods providing that a subset of controls are examined on an interim basis.
2. Alternatively, moderate levels of assurance may provide shorter assurance periods for a narrower scope of security controls appropriate to lower levels of inherent risk.
3. And, the lowest levels of inherent risk may be served by a narrower focus on assurance over the most essential and foundational cybersecurity controls.

Regardless of the required level, all assurance systems should be based on critical success factors that drive the quality of outcomes. This will enhance the overall quality and reliance on assurance reports across the healthcare industry. These critical success factors are underlying control specificity, testing rigor, and quality review of the assurance system. These factors include the assurance system's overall transparency, consistency, accuracy, and integrity.

What About Questionnaires?

Many industries rely on risk or control questionnaires to evaluate control coverage for third-party relationships. Health3PT members have extensive experience with questionnaire-based methodologies. They have concluded that questionnaires are *insufficient* for the healthcare industry given the potential risks to patient privacy and safety. Questionnaires also fall short of the expectations of industry stakeholders, including regulators.

Assurance Transparency

Transparency allows internal and external stakeholders to understand the framework used to satisfy core risk and compliance objectives. The framework should be publicly available, widely adopted, and well understood so that report recipients know how the controls were selected, evaluated, and scored. These questions can help evaluate whether the assurance is transparent.

1. Where do the controls come from? Are they based upon well-understood and well-documented systems?
2. How does the industry know if the control requirements are suitable? Are the controls well-reviewed?
3. Will the assurance effort and testing result in a certification?
4. Are the certification criteria and scoring clear?
5. Do industry stakeholders recognize the control system?

Assurance Consistency

Consistency is achieved through clear and well-documented control specifications, clarity on how maturity is demonstrated, and established scoring methodologies. Frameworks that are vague, subjective, or based on control expectations that lack clear success criteria are ineffective. They make it difficult to understand an organization's maturity compared to other companies, another framework, or an industry baseline.

Consistency also requires that assessment activities be reviewed for quality and integrity by an independent, third-party assessor or certification body.

These questions can help determine whether an assurance report provides reliable results.

1. Would the assessment results be the same, regardless of which professional services firm is conducting the evaluation?
2. How does the process ensure that individuals performing the work are evaluating and documenting their findings?
3. Does the assessment approach minimize variance?
4. Are the specified controls able to be compared against an assurance report for a different organization? Can a relying party understand and compare results supported by different external assessors? Can the third party share the report and its details?
5. How many entities issue these certifications or opinions? Are different quality review methodologies and systems used by different organizations to validate testing and certify reports? Do reports from different entities vary in level of quality or coverage?

Assurance Accuracy

There are a variety of frameworks and reporting programs designed to assess controls and security outcomes. However, many are qualitative, judgment-based, rely upon the third party's choice of controls that meet broad principles, and lack quantitative measurements. Some have also not kept up with advances in the use of third-party services. For example, not all frameworks consider the assurance obligations and opportunities inherent in the use of cloud service providers, where shared responsibilities and control inheritance increase the potential accuracy and transparency across the overall control system.

Assessment results should accurately reflect the state of an organization's controls. These questions can help in considering the accuracy of an assurance report.

1. Does it use a scoring and evaluation model that is sufficiently specific and granular, so that the industry can understand if controls are designed correctly and operating effectively?
2. Are there mechanisms in place to allow inheritance of results from vendor-performed controls?
3. Can shared responsibilities between the third party and their service providers be understood clearly?

Assurance Integrity

The testing methodology and rigor used by the external assessor determine the integrity of assurances and assessment reports. The assessor must evaluate each of the control requirements, verifying with proof that controls are implemented successfully, and must collect and catalog evidence. These questions can help consider the integrity of an assurance report.

1. Are processes in place to ensure the assessor conducted the assessment faithfully and reported the results truthfully? Can all conflicts of interest between the assessor, the assessed entity, and/or the certification body be avoided completely or eliminated?
2. How are the assessor's personnel trained? Is training consistent? Are training and quality assurance updates provided by the assessor or from a certifying or educational body? Are results developed and reported consistently with this training?
3. Are the assessor's methodology, testing, and deliverables reviewed by an accreditation and/or standards enforcement body?
4. What infrastructure exists to collect and catalog evidence between assessors or assessment cycles? Can the third party easily change assessors without having to re-enter or transfer previous assessment data?

Close the Loop on Identified Risks and Sustain the Relationship with Third-Party Entities

Remediation of issues, when identified, require appropriate and timely ***follow up to closure of identified gaps and corrective action plans (CAPS),*** *including relevant assurance that required activities are completed and risks are reduced.*

Health3PT is motivated to support third-party risk management to affect the implementation of controls needed to mitigate risk while also strengthening the business relationships needed to improve security in the healthcare industry. Healthcare industry companies and the third parties that support them must recognize that the industry is seeking transparency around the state of security. They must acknowledge that issues requiring remediation will be identified and that the needed remediation must be clear and transparent regarding the nature of the issue, and when and how it will be resolved.

Often, an assurance report will be issued with gaps noted. Controls not properly implemented will also be identified and CAPs will be needed to ensure improvements are made to drive a suitable level of maturity. Clear documentation of gaps and CAPs are indicators that there is transparency between parties. This is the desired outcome.

Documenting Gaps and CAPs

Third-party assessment reports will identify any gaps and CAPs that need to be addressed, and the third party will work with the healthcare industry companies who rely upon the report(s) to agree upon the timeline and steps needed to remediate identified gaps or CAPs.

Depending on the inherent risk of the third party and the corresponding level of assurance, some assurance reports will not include gaps or CAPs. The company will need to work with the third party on identified risks to ensure appropriate action plans are developed and executed.

At minimum, a complete gap or CAP will include

1. Identifier
2. Description of the issue
3. Date and how the weakness was identified (e.g., assessment, assessor)
4. Control mapping(s) specific to the identified issue
5. Point of contact accountable for resolving the issue
6. Resources required (dollars, time, and/or personnel)
7. Scheduled completion date
8. Actual completion date
9. Corrective action(s)
10. Status

Higher-level assurance reports, such as HITRUST r2 Assessment Reports, may include required CAPs that prevented certification. Those reports can also include CAPs that did not prevent certification but still represent risks that must be resolved.

Tracking and Relationship Management

Once CAPs are received from the third party, the organization must review them and ensure the actions and the timeline for their implementation are acceptable. If they are not acceptable, the organization will need to work with the third party on the resolution of remaining issues.

Gaps and CAPs should be documented in a technical system that allows the third party and their healthcare industry stakeholders to track continuous progress on remediation. Where a third party has relationships with multiple healthcare industry companies, a single reporting model for progress on remediation will reduce duplicated reporting and improve efficiency and security outcomes.

Remediation progress is a helpful tool for establishing and growing the strength of the relationship between healthcare industry companies and third parties. Regular levels of reporting and dialogue are encouraged between industry stakeholders.

Manage the Ongoing Relationship and Seek New Information as Risks and New Security Requirements Emerge

---

The industry views security and risk management as a continually changing environment and is seeking ***recurring updates of assurance of the vendor's security capabilities.***

Different risk factors result in differing inherent risks, and result in specific recommendations for distinct levels of assurance. As inherent risk and required assurance levels increase, Health3PT seeks assurance systems that allow third parties to increase their level of assurance without losing the investments made to obtain prior levels of assurance.

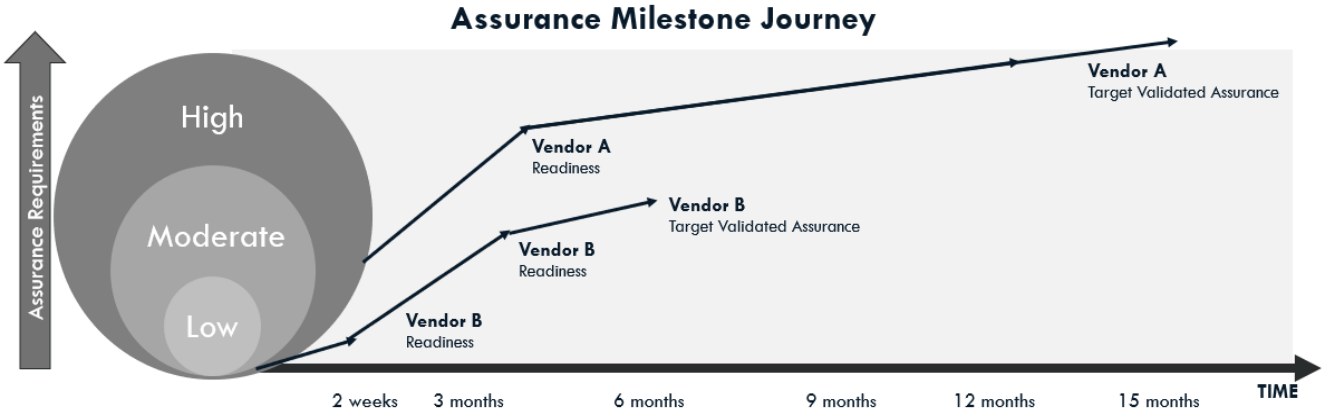
Health3PT also views security requirements as fluid and continuously changing. New threats and vulnerabilities may require implementation of new safeguards, including increased monitoring of existing controls. The healthcare industry should prioritize the use of control frameworks that adapt actively and regularly in response to changes in the threat and risk landscape.

For these and other reasons, assurance reports will be accepted only for a specific period based on the report and assurance level. Third parties are expected to implement management programs to sustain their security environment and adapt to changes in the threat environment. Assurance reports, therefore, require periodic updates with progress reported for the industry. Higher levels of assurance may be, in some cases, extended through interim updates. In all cases, remediation of identified CAPs must be completed within the negotiated timeframes.

There are several business scenarios that may lead the company or a third party to change the assurance level needed.

1. **Changes in inherent risk**
   Health3PT fosters an approach to third-party risk management that recognizes relationships evolve. Healthcare industry companies should track the lifecycle of third-party relationships over time, instead of treating assurance reports as a single event or using the same assurance level for all third parties. They should be prepared to increase or decrease levels of assurance from time to time, as appropriate. Third parties also are encouraged to consider proactively using higher levels of assurance than required and internal inheritance to stay ahead of evolving industry requirements.

2. **Progress to higher levels of assurance**
   In some cases, companies and third parties may negotiate milestones in their journey to a targeted level of assurance. For example, a healthcare industry company may require that a new third party immediately demonstrate foundational or essential security control with documented assurance while tracking their progress towards a more comprehensive, higher level of assurance over a longer period. This prioritizes the working relationship of both parties, ensures the most essential controls are in place quickly, and paves the way to stronger assurances across the entire industry.



3. **Shared responsibilities and inheritance**
   Third parties that choose to use services from others, such as cloud service providers, as elements of their overall security program are encouraged to inherit security controls where they are available and appropriate. Healthcare industry companies should encourage this practice.

Track the System of Third-Party Risk across Multiple Vendors for the Organization

*Documentation of **metrics and reporting on organization-wide vendor risks** supports transparency and regulatory expectations for the industry.*

Healthcare is a complex industry, with tens of thousands of relationships between companies and third-party vendors and suppliers. It is a many-to-many model. Each company has dozens of relationships with third parties, and the largest companies have thousands. Some of these serve multiple types of organizations within healthcare, as well as other industries. Healthcare is made up of relationships between covered entities and business associates. In many cases, business associates may support other business associates across a supply chain.

Effective third-party risk management requires a series of practices designed to set clear requirements, achieve security assurance based on documented inherent risk, remediate identified issues, and remain relevant as requirements change. Achieving these requirements across the exponential scale of the healthcare industry is impossible without a systematic approach that includes clear expectations and is supported by technology. The technology should check progress across stakeholders, distribute results systematically, integrate with existing systems, and support business relationships. Systematic sharing of metrics and assurance system results provides business value and promotes understanding of risk.

Examples include the following.

1. Healthcare industry companies may find it valuable to assess maturity scores in specific areas of the control system. For example, they may wish to analyze a response to specific threats or events. The ability to efficiently narrow the analysis can be more effective than manual correlation and inspection processes based on legacy reporting and assurance systems.
2. Similarly, third-party suppliers find it valuable to communicate their security efforts and security assurances to all companies they support through a common system.
3. Organizations on both sides of the relationship will find it valuable to create automated reporting and analysis systems for their work together. For example, they may want to report on risks for specific, shared technical systems, or develop shared scorecards.

Health3PT is committed to supporting all the above approaches in support of a system that is sustainable, efficient, and meets the needs of the healthcare industry and its stakeholders, including regulators.

Summary of Benefits

The healthcare system is dependent on viable, trusted business relationships between all parties across the industry. Those include industry companies, the third parties who support them, covered entities, and business associates. Health3PT is dedicated to working across the healthcare industry to supply the latest tools and mechanisms available to support all participants.

The practices and implementation guidance detailed in this document are critical to the sustainability and protection of the healthcare industry. Benefits are outlined here.

Health3PT Implementation Guidance	Industry Action	Benefits
Implement Consistent and Appropriate Contract Language	Use unambiguous and clear language between healthcare industry companies and third parties.	1. Document the scope and characteristics of the systems or services supporting the healthcare industry. 2. Define the ownership and confidentiality of data in scope for the system, management requirements, and disclosure expectations. 3. Clarify risk management, security, and assurance expectations.
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 that own third-party relationships to understand and clearly agree on risks and support negotiation and engagement. 4. Clarify security assurance requirements that fit each relationship and support the industry as a whole.
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.

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.
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.
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.