Health3PT – Third Party Risk Management Health Industry Recommended Practices

There should be no debate that third parties pose 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 inherent 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 health 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 PHI and other sensitive Information by business associates. Furthermore, out-of-date approaches in understanding TPRM risk have not evolved to keep pace with the use of cloud and other technological innovations in the healthcare industry. Such practices 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 and class action lawsuits that ultimately slows down innovations that are transforming the delivery of care.

The Ineffective state of TPRM practices used by health plans and health systems today include:

1. No overarching methodology for risk tiering vendors
2. Over-reliance on verbose contract terms
3. Extensive and inconsistent questionnaires that attempt to 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

Time is of the essence for healthcare organizations to revolutionize TPRM practices to keep up with emerging cyber threats and the adoption of Cloud, AI and other solutions in the industry. In response to this urgent situation, leaders in healthcare established the Health3PT council to transform TPRM practices to align with modern-day risks. Many of the industry’s largest Covered Entities as well as globally recognized technology and healthcare solution providers have come together to affirm these practices and develop guidance for proper implementation.

The industry has ratified these TPRM Health Industry Recommended Practices:

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

Establishing and adopting these TPRM HIRP will transition TPRM in healthcare from a mostly check-the-box exercise that is exposing organizations to unnecessary risks and slowing down healthcare innovation to a function that is effectively and efficiently managing third party risk and clearing away obstacles for the rapid adoption of technological advancements.

Adoption will also help ensure organizations meet both 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 as well as help qualify for potential mitigations from regulatory fines and penalties when these practices are used to address TPRM outcomes.

To ensure consistent and appropriate implementation of the HIRP, a prescriptive implementation guidance document is being developed.