



Provider Third-Party Risk Management Council Charter

The Provider Third Party Risk Management (TPRM) Council recognizes that healthcare providers are becoming increasingly dependent upon services controlled or hosted by third parties to deliver vital services. As a result, ensuring the security, integrity and availability of services provided by all third parties and all of the associated sensitive information they handle, is vital for healthcare providers to deliver care to patients. Unfortunately, methods employed today to manage this third-party risk are cumbersome and generally, not effective.

By requiring all third-party service providers that handle sensitive information to adopt a single information security and privacy assessment and certification program based on the HITRUST CSF®, healthcare organizations are better equipped to manage risk associated with these third-party service providers. In addition, providing clarity around what practices third parties must adhere to delivers a clear message regarding what it takes to do business with members of the Council and healthcare providers in general.

Commitments of Provider TPRM Council Members:

- ✓ Establish effective, consistent, repeatable and accepted expectations and programs for managing third-party service providers that require access to Protected Health Information (PHI) or Personally Identifiable Information (PII);
- ✓ Accept HITRUST Certification from our third-party service providers in lieu of any other assessment, questionnaire, audit or certification report;
- ✓ Share knowledge, resources and investments in order to further the Council's initiatives, programs and outcomes;
- ✓ Support HITRUST in defining and executing its third-party risk and assurance programs;
- ✓ Hold our third-party service providers and each other accountable to these commitments to ensure that the shared objectives are met.

Benefits for Healthcare Providers:

- ✓ Ensure the quality, safety, and security of third-party services procured to treat patients and manage data from threats while further complying with State and federal laws;
- ✓ Improve the quality of governance processes while reducing the amount of time and resources spent by healthcare providers understanding and managing risks when using third party service providers;
- ✓ Ensure that third-party service providers have consistent and complete information security and privacy related risk information at all times throughout the business relationships;
- ✓ Provide a transparent and streamlined method for engaging businesses which will reduce the complexity and variation in contracting, onboarding and oversight.

Provider Council Members



BA/Vendor Council Members



Benefits for Third-Party Service Providers:

- ✓ Allow third-party service providers to maximize the use of resources to provide differentiated products and services instead of determining how to address the myriad, overlapping, and uncoordinated requirements demanded of them by individual customers;
- ✓ Provide a streamlined method to prove the quality of information security and privacy programs in a straightforward and streamlined fashion;
- ✓ Allow third parties to be assessed and take advantage of the “audit once and use many” approach.

These benefits will contribute to effectively and efficiently managing contractual obligations without undue burden.

Roles and Responsibilities:

Governing Council Members

- ✓ Actively engage and participate in the definition of programs, providing input and support for decisions made by the group;
- ✓ Participate in all quarterly meetings of the TPRM Council Governing Body;
- ✓ Participate in an annual open meeting of the TPRM Council at the HITRUST annual conference;
- ✓ Participate in the outreach activities of the Provider TPRM Council;
- ✓ Composition – up to 10 organizations consisting of six (6) healthcare providers and four (4) third party service providers.

Council Participants (including Governing Members):

- ✓ All: Implement programs according to directions established by the TPRM Council;
- ✓ All: Implement uniform contractual obligations mandating conformance to this program wherever possible.
- ✓ For providers: Hold third-party service providers to the established standards and encourage uniformity across the industry;
- ✓ For providers: Accept current and appropriately scoped HITRUST Certifications;
- ✓ For third-party service providers: Agree to become HITRUST Certified, and to continuously maintain certification thereafter.
- ✓ Participate in the HITRUST Assessment Exchange.
- ✓ Composition – healthcare providers and third-party service providers who agree to commit to the Provider TPRM Council principles.

HITRUST:

- ✓ Implement feedback and requirements to enable healthcare providers to adopt this program;
- ✓ Establish and execute ongoing education and awareness campaigns to the healthcare providers and third-party service providers;
- ✓ Maintain the HITRUST Suite of programs and services in a manner that does not create undue financial and operational burdens on all stakeholders. At all times, seek to reduce complexity and costs associated with achieving and maintaining HITRUST Certification;
- ✓ Continuously improve the HITRUST CSF and its Assurance Program to meet the needs of healthcare providers and third-party service providers;
- ✓ Maintain the quality and integrity of these programs by ensuring all parties (Third-Party service providers, participants, assessor organizations and HITRUST) are appropriately vetted and monitored for conformance to the commitments;
- ✓ Continue advocacy efforts within the international healthcare industry and its regulators to promote adoption of the HITRUST CSF.