Summary of Changes
Version 9.5.0

Incorporates modifications necessary to support the introduction of the MyCSF Compliance & Reporting Pack for HIPAA

September 2021

Fundamental to HITRUST's mission is the availability of a common security and privacy framework, the HITRUST CSF ("CSF"), which provides the needed structure, transparency, guidance, and cross-references to authoritative sources organizations globally need to be certain of their data protection compliance. The initial development of the CSF leveraged nationally and internationally accepted security and privacy related regulations, standards, and frameworks—including ISO, NIST, PCI, HIPAA, and COBIT—to ensure a comprehensive set of security and privacy controls. The CSF standardizes these requirements, providing clarity and consistency and reducing the burden of compliance.

In developing a framework that can meet the needs of organizations locally, nationally, and globally, HITRUST recognizes that various organizations may have requirements imposed as a result of being part of a smaller community—such as a subset of an industry group, a State Agency, or by a cooperative sharing agreement. In many cases, these may not be new security or privacy controls but more specific implementation requirements. HITRUST provides the capability for these requirements to be incorporated, harmonized, and selected for inclusion during the assessment process and then included in the HITRUST CSF Assessment Report, utilizing the MyCSF platform. The intent is to reduce any additional assessments by enabling organizations to Assess Once, Report Many™. The HITRUST CSF includes such community-specific authoritative sources, referred to as supplemental requirements (SR) or community supplemental requirements (CSR). Organizations required or choosing to include community-specific authoritative sources may select them with other regulatory factors under the Admin & Scoping section of the MyCSF platform. HITRUST continues to evaluate the inclusion of others based on market demand.

HITRUST ensures the CSF stays relevant and current to the needs of organizations by regularly updating the CSF to integrate and normalize applicable requirements and best practices as authoritative sources and community supplemental requirements.

This release incorporates modifications necessary to support the introduction of the MyCSF Compliance & Reporting Pack for HIPAA and miscellaneous corrections. These updates reflect HITRUST's commitment to provide a framework fitting for any organization globally. Minor administrative updates, such as the correction of grammar or formatting errors, are generally not reflected in the Summary of Changes.

The table below provides a summary of the changes to the CSF broken down by Control Reference and Implementation Requirement Level.

CSF Control Reference	Requirement Level	Summary of Changes	Remarks
11.a	HIPAA	Added: Notifications to individuals affected by security events are written in plain language.	Necessitates new Implementation Language.
11.c	HIPAA	Added: For the purposes of determining when external parties must be notified, the organization treats security events as discovered on the first day in which the security event is or would have been known by the organization through exercising reasonable due diligence.	Necessitates new Implementation Language.