



HITRUST Central: Enhancing knowledge, fostering collaboration and building trust

The destination for healthcare information security professionals wishing to more efficiently and cost-effectively enhance the security of their organizations, comply with standards and regulations, and collaborate with industry peers.

Built on a strong foundation.

The foundation for HITRUST Central is the Common Security Framework (CSF), a certifiable security control framework that can be used by all healthcare organizations that create, access, store or exchange electronic health and other sensitive information. The CSF leverages and cross-references the security requirements of healthcare organizations, including federal (e.g., HITECH Act and HIPAA), state, third party (e.g., PCI and COBIT) and government (e.g., NIST, FTC and CMS). The CSF normalizes these sources in such a way that organizations can quickly understand their compliance status across a wide range of standards and authoritative sources. In addition, the CSF includes a prescriptive set of controls and supporting requirements that clearly define how organizations are to implement information security to meet the objectives of the framework. The controls scale according to type, size and complexity of the organization and its systems through multiple levels of implementation requirements based on risk-contributing factors. This provides organizations with a risk-based approach to adopting the appropriate level of information security control.

HITRUST has also developed a CSF Assurance Toolkit that leverages the CSF and serves as the only practical means for an organization to perform a self assessment or undergo an assessment conducted by a CSF Assessor. Available only through a Professional subscription to HITRUST Central, organizations can use the toolkit as an approach for performing a compliance assessment and reporting against HIPAA, HITECH, state and other third-party requirements. Included in the toolkit are the Common Health Information Protection (CHIP) Questionnaire and the CSF Compliance Worksheet, along with optional templates for scoping an environment and managing a test plan. Any and all organizations adopting the CSF internally, or requesting business associates adopt the CSF, should use the toolkit in effectively protecting sensitive health information and managing compliance.

HITRUST Central is the managed online community for healthcare information security professionals. The resources available are meant to enhance knowledge, foster collaboration and build trust among users and the healthcare community overall. Resources include:

CSF Access the CSF, including all controls, control objective, alternate controls and authoritative sources.

CSF Assurance Toolkit Serves as the only practical means for an organization to perform a self assessment or undergo an assessment conducted by a CSF Assessor. Includes the Common Health Information Protection (CHIP) Questionnaire, CSF Compliance Worksheet and supplemental assessment templates.

Alternate Controls Learn about currently accepted alternate controls to address control failures of healthcare systems and devices relative to CSF requirements. Users also may submit known control failures and request approval of their risk mitigation approaches as new alternative controls.

HITRUST CSF Products and Services Guide Search for solutions that will help address general security requirements and remediate security deficiencies.

Blogs Retrieve news and commentary from guest bloggers and industry leaders on topics relevant to healthcare IT security and compliance professionals. HITRUST Central subscribers can further stimulate discussion on key topics by posting their own comments and views.

Forums Collaborate with other subscribers via moderated forums where topics include general security and compliance, CSF specifics and vendor application forums. Users can post ideas, ask questions, request support and exchange best practices.

Calendar View upcoming HITRUST and healthcare information security events, including training sessions, webcasts and industry tradeshows.

Downloads Access a library of online materials, including training documents, reference guides, presentations and data sheets, available only to HITRUST Central subscribers.

Subscribe to HITRUST Central.

Subscribing to HITRUST Central is the only way to access the CSF and the CSF Assurance Toolkit, but it also represents a great way to learn more about other information security regulatory and healthcare issues as well as network with other professionals in the industry. Individuals can register for one of two annual subscription options to HITRUST Central – Standard and Professional. A Standard subscription, which includes access to the core CSF, is available at no charge to individuals from qualified organizations* and Professional subscriptions are available for an annual fee based on organization type.

Subscriptions include:

Description	Standard	Professional	Professional
Available to:	Qualified Organization*	Qualified Organization*	Non-qualified Organization
Common Security Framework (CSF)	PDF download	PDF download & online access	PDF download & online access
CSF Assurance Toolkit		✓	✓
CSF Validated Report with Self Assessment	Limited distribution available for additional cost	Unlimited distribution	Unlimited distribution
CSF Authoritative Sources, including updates			
• HIPAA – Including HITECH		✓	✓
• NIST		✓	✓
• ISO		✓	✓
• PCI		✓	✓
• FTC		✓	✓
• CMS		✓	✓
• COBIT		✓	✓
• New Sources		✓	✓
Security Configuration Packs		✓	✓
Customer Support		Submit up to 10 questions annually	Submit up to 10 questions annually
CSF Products and Services Guide	✓	✓	✓
Forums	✓	✓	✓
Blogs	✓	✓	✓
CSF Alternate Controls	Forum only	Forum & online	Forum & online
Working Group Participation	CSF commenting only	CSF & other programs	CSF & other programs
Integrated Third-Party Services	Dependant on service	Dependant on service	Dependant on service
Annual subscription fee	No charge	\$2,375	\$3,375

* A qualified organization is any organization employing a function or activity involving the use or disclosure of individually identifiable health information, **provided that said organization does not provide technology or security products or services**. Additionally, any federal, state, or local agency or department may qualify for a Standard subscription. HITRUST has the right to verify eligibility.

Perform a Self Assessment and Receive a CSF Validated Report

Organizations choosing to conduct a self assessment and receive a CSF Validated report can do so by purchasing a Professional subscription to HITRUST Central, which includes access to the CSF Assurance Toolkit, or by licensing only the HITRUST Common Health Information Protection (CHIP) Questionnaire. The self-assessment option removes any potential barriers for organizations that lack the resources for a remote or onsite assessment, but nonetheless must still implement data protection controls, maintain HIPAA/HITECH compliance, and report to external parties. Upon submission of the completed questionnaire to HITRUST, organizations will receive a CSF Validated report with the assessment results that can be used to report the state of their security to multiple internal and external parties.

HITRUST offers two pricing options based on the reporting needs for organizations choosing to conduct self assessments. For \$500, qualified organizations* can purchase a license to the CHIP Questionnaire, submit the completed questionnaire to HITRUST, and receive a CSF Validated report that may be distributed one time. Qualified organizations wishing to have unlimited distribution of the report to their business partners and other third parties can purchase a Professional subscription to HITRUST Central. To learn more, visit www.hitrustalliance.net/selfassessment.

To register for a Standard subscription to HITRUST Central, visit www.HITRUSTcentral.net, or to purchase a Professional subscription, visit www.HITRUSTalliance.net/purchase.

For more information about HITRUST, the HITRUST CSF and other HITRUST offerings and programs, visit www.HITRUSTalliance.net.