# SOC 2 for HITRUST/HIPAA

# SOC 2 for HITRUST/HIPAA

## Some terms used

a. PHI— Protected Health Information
b. ePHI—electronic PHI
c. PII—Personally Identifiable Information e.g SSN
d. PCI— Payment Card Industry
e. HIPAA- Health Insurance Portability and Accountability Act
f. HITECH- The Health Information Technology for Economic and Clinical Health Act
g. HITRUST- Health Information Trust Alliance


## The Context

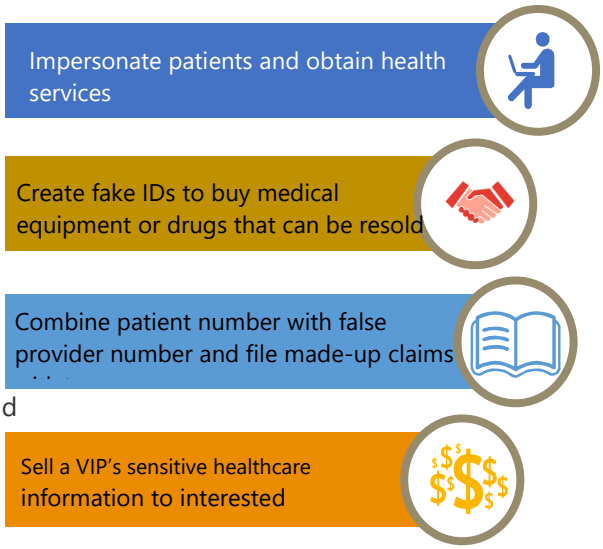
Privacy compromises and Cyberattacks have been on the rise and so States are tightening norms to protect this issue. If your company is handling any form of PHI, you need to be in compliance with HIPAA. This obviously applies to any health care provider, but it doesn't stop there. This law also applies to any data center or Business Associate that is storing ePHI. Simply by having PHI in your company's possession, your company needs to demonstrate its compliance.

## DEMAND FOR SOC 2 FOR HIPAA

## Cyber Attacks in Health Care

### The evolution of the healthcare industry has resulted in a rise in cyber crimes

- Healthcare service providers have huge databases with more extensive customer information than any other industry.
- Health information sold for more than credit card data and can be used for fraud or identity theft.



- Medical identity theft is often not immediately identified by a patient or their provider giving a fraudster enough time to milk the credentials
- Sensitive data easily accessible through connected devices
- Low security controls across the industry makes it easy for hackers to get large amount of personal data

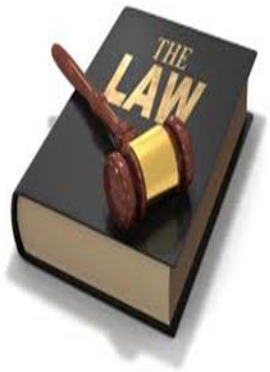
| Organization | Records Breached |
|---|---|
| **Anthem** | 78,800,000 |
| **Premera Blue Cross** | 11,000,000 |
| **Excellus** | 10,000,000 |
| **UCLA Health** | 4,500,000 |

Some of the large data breaches in Health Care are shown in the table. Incidents due to Business Associates were indicated to be at 56%


## Privacy compliance in Health Care

Cyber security and privacy compliance is at the top of the minds of management, boards and regulators. With the impact of recent regulatory oversight such as:

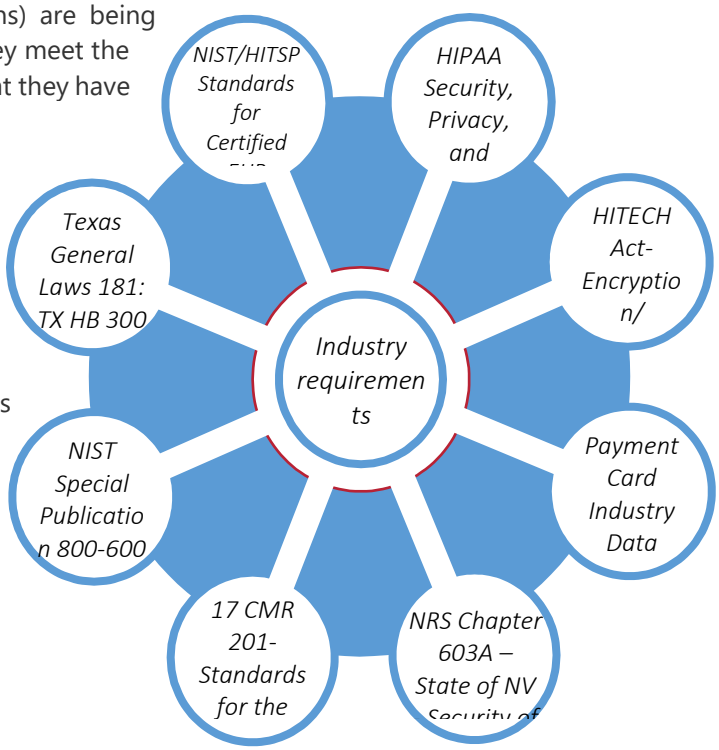
a. Department of Health and Human Services' (HHS)
b. HIPAA Omnibus rules
c. HITECH Act
d. Other State and Privacy laws
e. New EU GDPR rules




Health care entities and related business associates (BA e.g., health plans, health care clearinghouses, exchanges, health care providers, and organizations that conduct

certain financial, research, and administrative functions) are being asked with increased frequency to demonstrate that they meet the common security and privacy requirements of HIPAA that they have taken appropriate measures to:

- Secure their environment
- Be vigilant in anticipating what might occur in the evolving security landscape
- Implement appropriate measures to detect and react to existing and emerging threats
- Be resilient in their ability to recover operations when a security incident does occur




## Non-Compliance financial implications

Organizations that fail to properly implement required controls to protect PHI may experience severe financial penalties, the imposition of corrective action plans, or ongoing oversight by regulators over a multi-year period. Other risks include the adverse publicity of breaches and damage to their brand.

### HIPAA Rule

Mandates organizations to protect personal health information and requires that information shared with BA is appropiately protected

### HITECH Act

Hipaa privacy, security and breach notification laws apply directly to BA.

BA are regulated, subject to OCR Audit and may face civil, criminal penalties

### HIPAA Omnibus Rule

Expanded the defination of BA to include entities that transmit and need routine access to PHI (Contractactors, Sub-Contractors)

| HIPAA Violation | Minimum Penalty | Maximum Penalty |
|---|---|---|
| Individual did not know (and by exercising reasonable diligence would not have known) that he/she violated HIPAA | $100 per violation, with an annual maximum of $25,000 for repeat violations (Note: maximum that can be imposed by State Attorneys General regardless of the type of violation) | $50,000 per violation, with an annual maximum of $1.5 million |
| HIPAA violation due to reasonable cause and not due to willful neglect | $1,000 per violation, with an annual maximum of $100,000 for repeat violations | $50,000 per violation, with an annual maximum of $1.5 million |
| HIPAA violation due to willful neglect but violation is corrected within the required time period | $10,000 per violation, with an annual maximum of $250,000 for repeat violations | $50,000 per violation, with an annual maximum of $1.5 million |
| HIPAA violation is due to willful neglect and is not corrected | $50,000 per violation, with an annual maximum of $1.5 million | $50,000 per violation, with an annual maximum of $1.5 million |

# HOW SOC 2 PLUS HITRUST CAN HELP

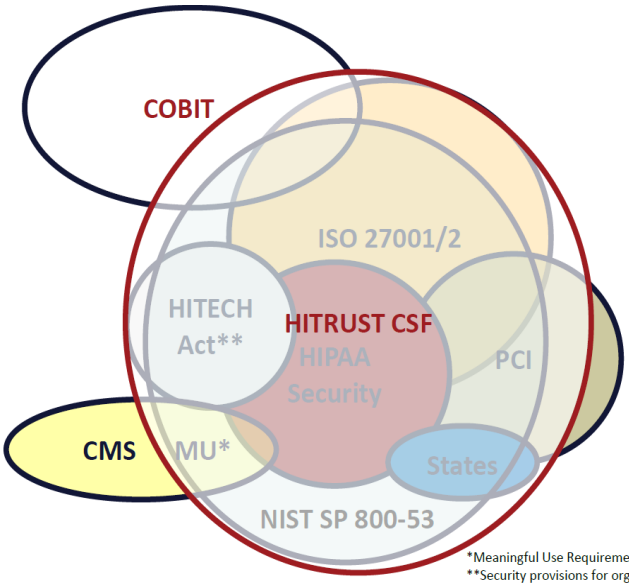
HITRUST and The American Institute of CPAs (AICPA) have collaborated to develop and publish a set of recommendations to streamline and simplify the process of leveraging the HITRUST CSF a CSF Assurance program and SOC 2 reporting.

## What is SOC 2

A SOC 2 report is intended to meet the needs of internal control at a service organization as it relates to one or more of the AICPA's Trust Services Criteria of Security, Availability, Processing Integrity, Confidentiality or Privacy. The reports are intended for use by stakeholders (e.g., customers, regulators, business partners, suppliers, directors) of the service organization. A SOC 2 examination is similar in structure and general approach to SOC 1 reporting (legacy SAS70), but also allows the flexibility to incorporate additional suitable criteria, for example, around adherence to public, industry-specific frameworks such as the HITRUST CSF.

## What is HIRUST CSF

The HITRUST CSF was developed to provide organizations with a framework specifically devoted to the protection of ePHI and PHI data in the healthcare industry. Unlike the HIPAA Security Rule, the CSF is not a new standard or regulation, rather, the CSF is a certifiable framework of security controls that scales according to the type, size, and complexity of the organization and its systems. The CSF streamlines the compliance process because it is built from existing standards and regulations that already apply to healthcare organizations, for securing the PHI, allowing organizations to assess once while simultaneously meeting multiple compliance initiatives.




## HITRUST, HIPAA and HITECH

The HITRUST CSF fully integrates the requirements of the HIPAA Security Rule with the standards of ISO, NIST and many other federal, state and business requirements. By selecting the characteristics of the organization(s) and system(s) to be evaluated, the CSF's control requirements scale based on risk. This allows small, medium and large organizations to leverage the CSF as the baseline for their security program or assessment process in a way that is appropriate for each unique environment and to attest to business partner, customer or third-party security requirements.

There is no official "compliance" designation or seal associated with the HIPAA Security Rule. Organizations can only attest to their compliance by providing a supporting risk assessment and evidence of their security controls such as the SOC 2 report specifically covering HIPAA/HITECH controls.

## SOC 2 + HITRUST CSF report for HIPAA Compliance

This option can be used when a service organization wants its service auditor to express an opinion on whether the controls at the service organization are suitably designed and operating effectively to meet the entire HITRUST CSF requirements in addition to the applicable trust services criteria. It provides the service organization with a service auditor's examination report that includes

- an opinion on the fairness of the presentation of the description based on the description criteria in the AICPA SOC 2 requirements and
- an opinion on the suitability of the design and operating effectiveness of the controls based on the applicable trust services criteria and the HITRUST CSF requirements.

The use of a SOC 2 report enables health care and other organizations to communicate information about their programs for complying with HIPAA regulatory requirements in a single report that provides information about the organization's controls over protected health information (PHI) based on the applicable trust services criteria and the HITRUST CSF requirements. This provides service organizations with

the ability to increase transparency and communicate through a single deliverable to customers, business partners, and stakeholders both in and outside the health care sector.

# WHY SOC 2 FOR HIPAA COMPLIANCE

## Faster, Efficient and Comprehensive reporting

Healthcare organizations can now effectively assert too many of the mandated provisions with the HIPAA Security Rule by undertaking annual SOC 2 assessments by a CPA firm such as ours. We have has developed a specific testing matrix that maps directly to the HIPAA Security Rule. Use of a SOC 2 report is an incredibly efficient and comprehensive process for showcasing compliance with the security rule requirements of HIPAA.

## Improved customer relationships


With a SOC 2 report you can provide your customers with a variety of internal control information, including information specific to controls over PHI, in a well-accepted reporting format. Additionally, information can be provided to customers quickly as you will already have one report to answer their questions as you are building customer satisfaction.

## Third Party Reporting Needs

The SOC 2 reporting model provides an efficient way of knowledge of controls to satisfy representation of risk exposure, compliance posture of security practices at the service organization. The SOC 2 Type II reports provide assurance that controls have operated, as designed, for a fixed and continuous period of time (e.g., a rolling six- or twelve-month reporting cycle).

## Internal controls reporting for SOX

The structure of reporting under the SOC 2 for HIPAA compliance can become a baseline method of reporting to compare with different service organizations. This is a good way of mapping Internal Controls for SOX compliance.

## Comprehensive CSF Framework

HITRUST has been accepted well within the healthcare industry. Now many customers outside the healthcare industry also use SOC 2 for HITRUST to be prepared to efficiently to be ready or meet other compliance needs.

**SOC 2 Type II can cover the entire year and the effectiveness of the controls in place can be reported**

**It is a Third Party Period- of-Time assessment and so has Accountability**

**Since it is a period of time assessment, it is more like a continuous compliance with low risk and high reliability**

**Most other assurance programs or audits are only, at a point in time**

**Comprehensive Framework for Privacy by AICPA**

**Provides a high reliability SOC 2 Seal by AICPA**

## KEY STEPS IN SOC 2 REPORTING FOR HIPAA


a. Gap Assessment
b. Remediation
c. Reporting

## HOW CAN WE HELP

We provide end to end SOC 2 reporting for HIPAA compliance. We cove all the 3 key steps listed above to make sure you are in compliance with the HIPAA requirements. Our proven methodology saves times as well as costs thus giving you the benefit of timely compliance with reasonable costs. In the SOC 2 report for HIPAA compliance, we can additionally use the HITRUST CSF framework to address your compliance needs. Our unique delivery method improves timelines and thus reduces costs of your compliance.

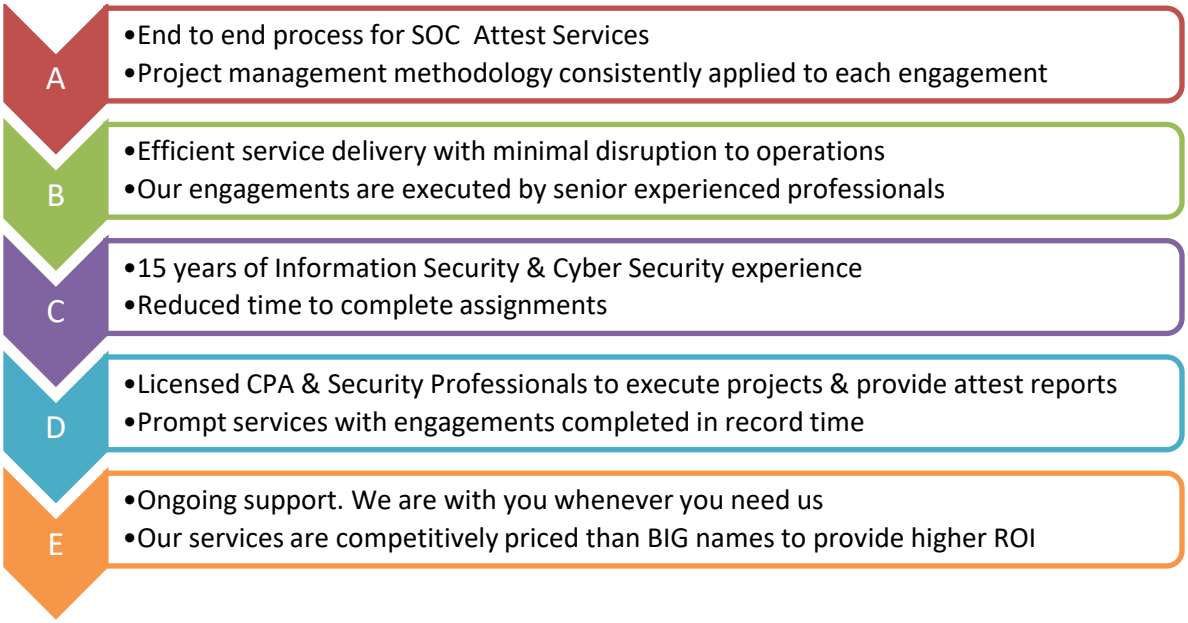
Additionally, we offer complimentary HIPAA specific information security policies and procedures professionally developed documentation specific to address the requirements of HIPAA. This satisfies one of the major challenges for HIPAA compliance.

## VALUE DELIVERY

Knowing how much extra value and assurance a SOC can deliver, many clients find that it makes sense to take steps to ensure a more successful outcome, including hiring experts who are skilled in helping organizations be more thorough and thoughtful in how they approach their engagement. Preparing for a SOC reporting engagement is a matter of clear thinking and smart planning. Working with a cyber security specialized consulting specialists such as ours, helps you dig into areas such as data security, incident response, and change management processes and much more.

We provide end to end process for SSAE 18, SOC reporting engagements. With the rapid Cloud adaption and increased use of BIG DATA, Cloud Security and Privacy concerns are on the rise. We can conduct integrated information security engagements with privacy engagements.

## SOME OF THE ADVANTAGES OF WORKING WITH US ARE:




**To discuss your specific need please email info@accedere.us**