Guide

Clinical Data Privacy and Security Best Practices

QCentrix

Introduction

Efficient delivery of patient care is the principal objective for any healthcare provider. Central to their successful achievement of this goal is the simple and immediate access to patient information for care providers. However, healthcare data provisioning is anything but simple. In fact, the risk associated with data access is among the most challenging issues facing health care executives today—known more commonly as cyber security.

The healthcare industry is facing a significant rise in cyberattacks.[1] From 2018 to 2023, the rate of healthcare data breaches (comprising 500 or more records) has nearly doubled.[2] The financial impact is substantial: a data breach costs a typical healthcare organization about $9.8 million.[3]

Adding gravity to an already complex issue for healthcare executives is the documented relationship between data breach remediation efforts and the quality of patient care. On average, a data breach at a nonfederal acute-care inpatient hospital was associated with an additional 23-36 deaths per 10,000 acute myocardial infarction (AMI) discharges per year.[4]

1 U.S. Department of Health and Human Services. "HHS Announces Next Steps in Ongoing Work to Enhance Cybersecurity for Health Care and Public Health Sectors" (December 6, 2023 https://www.hhs.gov/about/news/2023/12/06/hhs-announces-next-steps-ongoing-work-enhance-cybersecurity-health-care-public-health-sectors.html.

2 Steve Adler. "Healthcare Data Breach Statistics." The HIPAA Journal (September 24, 2024). https://www.hipaajournal.com/healthcare-data-breach-statistics/.

3 Emily Olsen. "Average Cost of Healthcare Data Breach Nearly $10M in 2024: Report." Healthcare Dive (August 1, 2024). https://www.healthcaredive.com/news/healthcare-data-breach-costs-2024-ibm-ponemon-institute/722958/.

4 Sung J. Choi, M. Eric Johnson, and Christoph U. Lehmann. "Data Breach Remediation Efforts and Their Implications for Hospital Quality." Health Services Research 54(5): 971-980 (October 2019). https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6736905/.

There Are Two Issues Here

First, the issue of an evolving landscape of cyber threats characterized by botnets, malware as a service (MaaS), distributed denial of service (DDoS), the increasing price tag, and lifespan of a patient record. Security breaches no longer require an engineering background. As a result, cyber resilience becomes virtually unattainable and leading organizations shift their focus to speed of detection, containment, and remediation.[5]

The second issue facing healthcare executives are the expansive ecosystems in which providers now exist. As care requirements become more complex, third-party partnerships throughout the organization deliver innovation as well as an additional entry path to data. As a result, healthcare executives are often forced to choose between innovation or data security.

The good news is that there are existing guidelines and assessments for third-party healthcare organizations' protective measures against current cyber threats. Verification of their successful completion of such guidelines are intended to offer healthcare executives needed assurances that partners will safeguard data. The most common example of this is SOC 2 for information technology organizations.

As a leader in the clinical quality data space, Q-Centrix appreciates that the cost of a data breach is far too high. Accordingly, the organization sought greater privacy and security assurance for its partners than SOC 2 alone. Instead, Q-Centrix was the first clinical quality data management organization to receive SOC 2 + HITRUST recognition. This briefing is organized to assist healthcare executives in understanding current healthcare partner security and privacy guidelines and recognition.

5 Third Annual State of Cyber Resilience: Innovate for Cyber Resilience; Accenture, 2020

The Health Insurance Portability and Accountability Act (HIPAA)

The Health Insurance Portability and Accountability Act (HIPAA) was passed in 1996 to safeguard electronic health information. Any business or organization is bound by HIPAA if it functions within healthcare ecosystems. The Act includes two main regulations, the Security Rule and the Privacy Rule.

The Security Rule protects individuals' medical records and other personal health information (PHI) that is created, received, used, or stored. Within this rule there are regulations that cover three different areas of business: physical, technical, and administrative environments. In addition, it addresses some ancillary organizational requirements, policies, and procedures.

Alternatively, the Privacy Rule offers guidelines for usage in treatment, payment, and similar activities while maintaining the confidentiality of the data. This rule covers security and confidentiality of PHI in all of its forms: electronic, print, and verbal.

While all healthcare organizations are responsible for the protection of personal health information based on HIPAA, the exact security protections are often misunderstood based on a simple terminology distinction.[6]

- **HIPAA Certification** is the process to obtain or be awarded a document or designation to attest that a person has completed an educational course.
- **HIPAA Compliance** refers to an adherence to the rules and requirements set forth by the Department of Health and Human Services (DHHS) policies and guidelines.

Importantly, the DHHS does not endorse or recognize HIPAA certification as a way to absolve organizations from the legal obligations of the HIPAA Security Rule.[7] Instead, HIPAA compliant companies are required to perform a periodic evaluation including both technical and non-technical audits to validate that security policies and procedures meet HIPAA requirements.

6 Official 2020 HIPAA Compliance Checklist, HIPAA Journal

7 HHS.gov; HIPAA Compliance and enforcement

Health Information Technology for Economic and Clinical Health (HITECH)

The HITECH Act was passed as part of the American Recovery and Reinvestment Act of 2009 to encourage the implementation of electronic health records. In anticipation of the expansion in the exchange of electronic protected health information (ePHI), the HITECH Act increased the potential legal liability for non-compliance and provided stricter enforcement of the guidelines. The act offered healthcare providers financial incentives for demonstrating meaningful use of EHRs until 2015, after which penalties were levied for failing to demonstrate it.[8]

System and Organization Controls (SOC)

In 2002, the Sarbanes-Oxley Act made public companies responsible for the maintenance of an effective system of controls over financial reporting. As such, organizations made their vendors obtain a System and Organization Controls (SOC) attestation report. A SOC report is a verifiable auditing report performed by a Certified Public Accountant (CPA) designated by the American Institute of Certified Public Accountants (AICPA). It is a collection of safeguards built within the control base of the data and also a check as to whether or not those safeguards work.

Frequently, SOC 1, 2, and 3 are misinterpreted to be different levels of the same report. In fact, they are completely different reports.

SOC 1- an audit of a third-party vendor's accounting and financial controls. It is the metric of how well they keep their books of accounts.

- SOC 1 Type I is based on a point in time audit.
- SOC 1 Type II is based on a testing of controls over a duration of time.

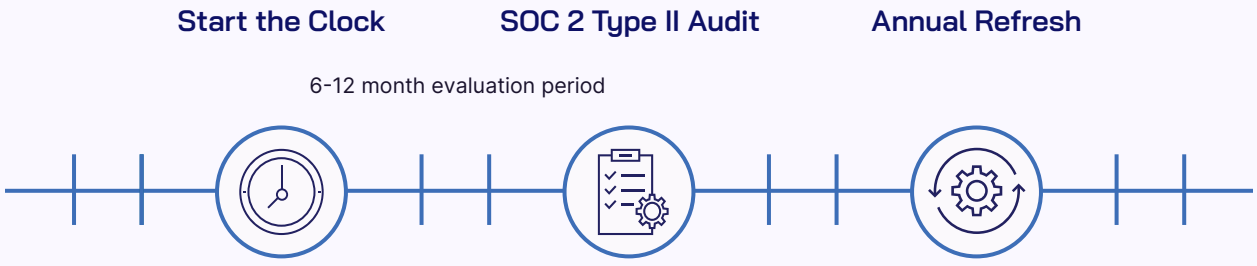
SOC 2- the preferred report for an information technology vendor. SOC 2 examines the controls of a service organization over, one or more of the ensuing Trust Service Criteria:

- Privacy
- Confidentiality
- Processing Integrity
- Availability
- Security

8 What is the HITECH Act? HIPAA Journal

Similar to SOC 1, SOC 2 has two types. Type I confirms that the controls exist. Type II validates that the controls are in place and working correctly. To maintain SOC 2 certification, organizations are required to demonstrate compliance annually through additional review, testing, and documentation.

Typical SOC 2 Timeline



Prepare

~1-3 months

Create Policies + Procedures Docs Update internal processes Employee training + education.

SOC 2 Type I

Optional

Get a Type 1 audit if you need. This is an additional cost, but is a helpful tool if you need for deals.

Doc Prep

2-3 weeks before audit

Organize documents and evidence for your auditors. Process will depend on the auditor.

Real-Time Observation

~2 days

Final Report

2-3 weeks after audit

You'll get a draft report to review a few weeks after audit, then you're ready to share with customers!

Repeat the process annually, though future audits tend to be more efficient.

SOC 3 is a summarize report of SOC 2 Type II. It is intended to be less detailed and technical than the SOC 2 Type II report.[9]

HITRUST

HITRUST Stands for the Health Information Trust Alliance. It was founded in 2007 to help organizations effectively manage data, information risk, and compliance. HITRUST certification by the HITRUST Alliance involves an independent assessment of compliance to HIPAA requirements based on a standardized framework. The length of the assessment depends upon the size and complexity of an organization as well as its scope and the amount of counseling.

9 SOC 1, 2, & 3 Audit Reports, and Why You Need One, InfoSecurity, October 23, 2019

HITRUST CSF

The HITRUST Common Security Framework (CSF) assessment is intended for businesses that create, access, store, or exchange sensitive information. The CSF is certified by security assessors and is designed as a risk-based approach to organizational security based on 156 required HITRUST controls. The HITRUST CSF unifies recognized standards and regulatory requirements from the International Organization for Standardization (ISO), National Institute of Standards and Technology (NIST), Payment Card Industry (PCI), Control Objectives for Information and Related Technology (COBIT), and HIPAA/HITECH.[10]

The Building Blocks of HITRUST

- COBIT
- HITECH
- HIPAA
- ISO 27001/2
- NIST 800-53
- PCI
- Meaningful Use

The HITRUST CSF Certification Process [11]

SOC 2 + HITRUST

The AICPA collaborated with HITRUST to align their reporting frameworks and develop a combined assurance program known as SOC 2 + HITRUST. The program maps between the HISTRUST CSF requirements and the AICPA's Trust Services Criteria. Audited by a CPA, the integration between the two reports creates a more complex and reliable assessment.[12] For example, the effectiveness of one set of controls impacts the other. Therefore, if an organization has all the controls necessary to meet the SOC 2 criteria but fails any of the 156 required HITRUST controls, this could result in an unqualified opinion in the SOC 2+ HITRUST report. SOC 2+ HITRUST is a combined assessment that offers substantial value for forward, security-minded healthcare organizations.

10 Building an Effective Third-Party Risk Management Program, HITRUST Alliance

11 Hitrustalliance.net

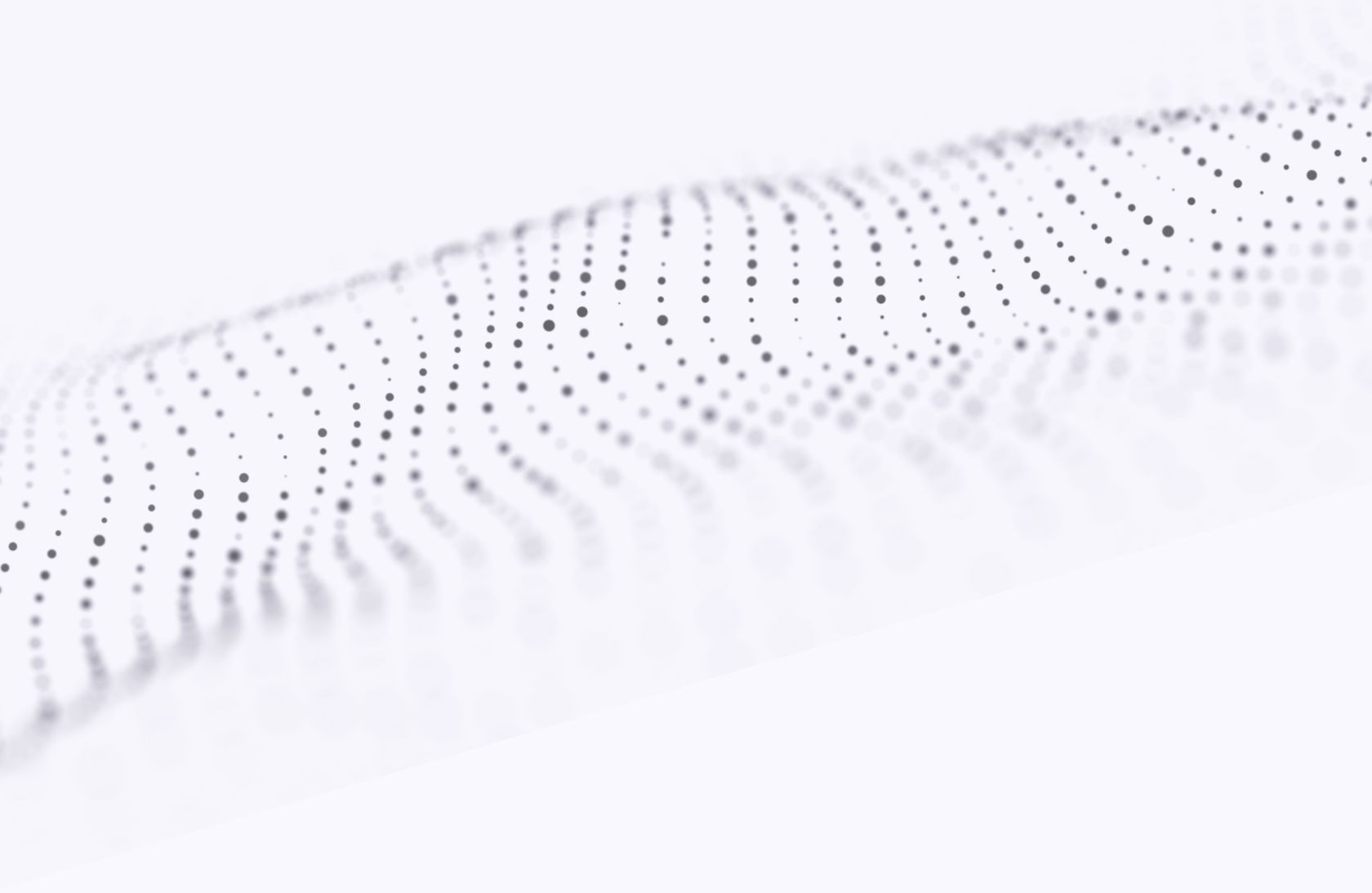
12 Hitrustalliance.net/soc2

SOC 2 + HITRUST Principles

- Information Security Management Program
- Access Control
- Human Resources Security
- Risk Management
- Security Policy
- Organization of Information Security
- Compliance
- Asset Management
- Physical and Environmental Security
- Communications and Operations Management
- Information Systems Acquisition, Development, and Maintenance
- Information Security Incident Management
- Business Continuity Management
- Privacy Practices

Leading in Clinical Quality Data Privacy & Security

Q-Centrix received its first SOC 2 + HITRUST report on October 7, 2020 and has been continuing to meet the report requirements ever since. The achievement added to an already-robust and multi-faceted set of data security best practices at Q-Centrix. In fact, the company maintains a strong security culture based on a perpetual focus on cyber security and the engagement of validation and authentication models. Accordingly, Q-Centrix is fully compliant with the HIPAA and HITECH laws, which establish provisions for safeguarding medical information. It also has a full security incident response plan with steps to identify, stop, evaluate, and contain a threat or breach, as well as prevent future similar incidents. Its additional established measures include encryption for all healthcare data stored and transmitted; data recovery and backup mechanisms; two-factor login authentication for anyone permitted to access information systems; workforce security training; and recommended physical security elements, such as secure entrances, restricted equipment areas, and video camera surveillance. Q-Centrix is at the forefront of cyber security in a quickly evolving ecosystem.



About Q-Centrix

Q-Centrix sees clinical data differently—as custom data sets with infinite possibilities.

Providing the industry's first Enterprise Clinical Data Management (eCDM™) approach, Q-Centrix combines AI-enabled technology, the largest and broadest team of clinical data experts, and insights from its more than 1,200 partners to help improve patient outcomes and drive process and performance improvement, strategic growth, and operational efficiency.

Its solutions address a variety of clinical data needs, including quality measurement and improvement, cardiovascular, oncology, trauma, research, and more.

One North Franklin
Suite 1800
Chicago, IL 60606
q-centrix.com

QCentrix