The Healthcare Cybersecurity Framework: A Top Defense Against Data Breaches and Attacks

Kevin Scharnhorst Chief Information Security Officer Health Catalyst

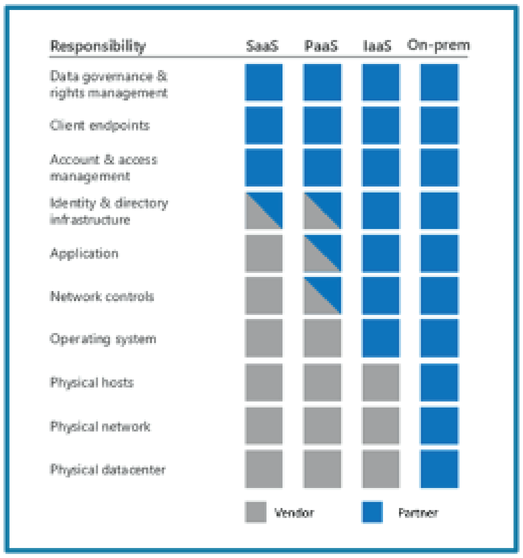
Healthcare IT vendors have an immense responsibility for an organization's cybersecurity when they partner on software and solutions, especially as breaches and cyberattacks are on the rise in the healthcare industry. Digital technology and connectivity have led to significant improvements in healthcare delivery, but increased integration enables more exposure to cyberattacks that can impact care delivery, safety, and privacy.

More than 93 percent of healthcare organizations experienced a data breach between 2017 and 2020, and 57 percent have had more than five data breaches during the same time frame. Furthermore, researcher Cybersecurity Ventures predicts healthcare will suffer two to three times more cyberattacks in 2021 than the average amount for other industries and that ransomware attacks on healthcare organizations will grow fivefold by 2021.

In response to healthcare's significant and growing cybersecurity threats, leading vendor organizations safeguard their systems and their partners by following a cybersecurity framework. A defensible protocol holds vendors accountable to routine audits and compliance measures at a regular cadence, ensuring both parties keep cybersecurity programs active and optimized.

Sharing Responsibility: The Cybersecurity Vendor-Partner Relationship

In a vendor-partner relationship, both parties often share the security responsibility, varying according to the type of hosted infrastructure. For example, in Figure 1, an on-premises (or self-hosted) solution, the responsibility and ownership fall more with the partner and move to the vendor as the hosted model moves towards software as a service (SaaS).



Responsibility	SaaS	PaaS	IaaS	On-prem
Data governance & rights management	🟦	🟦	🟦	🟦
Client endpoints	🟦	🟦	🟦	🟦
Account & access management	🟦	🟦	🟦	🟦
Identity & directory infrastructure	◩	◩	🟦	🟦
Application	⬜	◩	🟦	🟦
Network controls	⬜	◩	🟦	🟦
Operating system	⬜	⬜	🟦	🟦
Physical hosts	⬜	⬜	⬜	🟦
Physical network	⬜	⬜	⬜	🟦
Physical datacenter	⬜	⬜	⬜	🟦

⬜ Vendor 🟦 Partner

Figure 1: Vendor-partner hosting relationships.

In contrast to the SaaS model in Figure 1, a vendor (such as Health Catalyst and its hosted Data Operating System (DOS™)) platform uses a platform as a service (PaaS) model and move towards SaaS as capabilities allow. In a PaaS model, shared responsibilities between the vendor and partner exist in three main areas:

- Identity and directory infrastructure.
- Applications.
- Network controls.

Avoiding and Withstanding Attacks Requires a Hybrid Centralized and Decentralized Healthcare Cybersecurity Framework

A healthcare IT vendor cybersecurity framework aims to prevent data breaches from occurring. Sometimes, however, bad actors evade even the most robust measures. For example, on

December 13, 2020, the Cybersecurity & Infrastructure Security Agency (CISA) issued its second of five-ever-ordered directives for its federal civilian agencies to shut down an imminent threat involving software from a vendor. A nation-state attacker compromised this vendor's product code to impact the supply chain of organizations relying on the software to monitor and manage their network infrastructures. The effects of this attack are only in their first wave and will be long-lasting.

While even the most comprehensive security infrastructure can't guarantee to avert all threats, a security framework must be robust enough for healthcare cybersecurity teams to logically defend their cybersecurity practices, even amid the panic following a breach. In other words, the goal is to build a layered defense strategy so that a compromise in any one layer would not compromise the system as a whole.

To galvanize cybersecurity across the organization, C-suite leadership must support the program. The chief information security officer (CISO) establishes centralized security principles through a formalized organizational information security management program. The full C-suite supports processes and standards for decentralized execution and adherence.

In this hybrid centralized and decentralized healthcare cybersecurity model, the CISO is ultimately accountable for the cybersecurity program, which reaches through each of the other C-level business units to set prioritization for security and privacy compliance objectives. Strong C-suite and board alignment also helps align project investments.

The CISO can earn organizationwide support for centralized security principles with ongoing third-party audits and certifications. As external, objective checkpoints, third-party independent reports (versus self-audit) identify gaps and misaligned practices, holding security teams accountable to established standards and scheduled evaluations. The third-party independent perspective offers a credible reference point for from outside an organization's view and eliminates blind spots. Involving a third party also adds value to other external vendors with credibility to leverage in their own vendor security risk assessments.

Inside the Healthcare Cybersecurity Framework: Third-Party Audits and Certifications

The operational policies and procedures in place in a vendor-partner relationship are paramount in achieving compliance with the two entities' regulatory and certification strategies. In the security posture in a shared-responsibility model, the partner depends on its vendor. In the healthcare industry, the Health Insurance Portability and Accountability Act (HIPAA) is the prevailing regulatory framework. HIPAA typically defines the partner as the covered entity (CE) and its vendor as the business associate (BA). The CE is responsible for performing due diligence in vendor risk assessments on its BAs to assess inherited risk where third parties fulfill services or products.

The BA has a fiduciary duty to its partner, and in the context of HIPAA, to notify its partner when it discovers a security incident, breach, or disclosure under the terms defined in the business associate agreement (BAA). This arrangement allows the partner to fulfill its regulatory requirement of reporting such material events to appropriate authorities, following a strategic cybersecurity framework.

The following examples of ongoing third-party audits and certifications support the cybersecurity framework. These measures help organizations maintain cybersecurity standards and assure healthcare organizations that their vendors treat seriously the stewardship to protect the confidentiality, integrity, and availability of the data:

Service Organization Controls

Health Catalyst utilizes System and Organization Controls (SOC) compliance that comprises a cybersecurity risk management reporting framework. Organizations that comply demonstrate they are managing cybersecurity threats and have effective processes and controls in place to detect, respond to, mitigate, and recover from breaches and other security events.

- The SOC 1® reports provide information about a service organization's control environment relevant to the partner's internal controls over financial reporting. At Health Catalyst, for example, the SOC 1 report covers the design and operating effectiveness of controls relevant to the organization's cloud hosting solution. Vendor organizations receive SOC 1 Type II report per Statements on Standards of Attestation Engagements (SSAE) No. 18 (Reporting on Controls at a Service Organization) and the International Standard on Assurance Engagements (ISAE) 3402 (Assurance Reports on Controls at a Service Organization).
- The SOC 2® report is annual, third-party independent assessments of a control environment. The SOC 2 report is based on

the American Institute of CPAs' (AICPA) Trust Services Criteria and is issued annually following the AICPA AT Section 101 of its attest engagements. The report offers a retrospective 12-month audit. details the design and operating effectiveness of controls relevant to any system containing customer data as part of a healthcare cloud hosting solution. At Health Catalyst, the SOC 2 report addresses three of the five AICPA Trust Services Criteria (security, availability, and confidentiality).

HIPAA

Vendors may use HIPAA as a basis for their security and privacy framework. These third-party audits measure the compliance with HIPAA and assure that the organization has a HIPAA-compliance program with adequate measures for saving, accessing, and sharing individual medical and personal information.

Business Associate Agreements

Some organizations will sign BAAs at their partner's request. These agreements ensure that partners can meet the HIPAA and Health Information Technology for Economic and Clinical Health Act (HITECH) compliance requirements.

The Electronic Healthcare Network Accreditation Commission

Electronic Healthcare Network Accreditation Commission (EHNAC) is a national standard that indicates healthcare stakeholders have met or exceeded EHNAC's criteria. These stakeholders include electronic healthcare networks, financial services organizations, medical billers, third party administrators, outsourcers, ePrescribing networks, Healthcare Information Service Providers (HISP), Practice Management Systems vendors, and others.

The EHNAC criteria include conformance with federal healthcare reform legislation, including HIPAA, HITECH, American Recovery and Reinvestment Act, the Affordable Care Act, the HIPPA Omnibus Rule, and other applicable state legislation. Further, the criteria encompass privacy, security, and confidentiality; technical performance; business practices; and resources. EHNAC bases accreditation on independent peer evaluation of an entity's ability to perform at levels based on industry-established criteria. The accrediting process permits applicants to review their current performance levels and bring those levels according to industry-established minimums, best practices, and conformance with applicable federal and state healthcare reform legislation.

HITRUST

The HITRUST cybersecurity framework (CSF) leverages nationally and internationally accepted standards, including ISO, National Institute of Standards and Technology (NIST), PCI Security Standards Council, and HIPAA, to ensure a comprehensive set of baseline security controls. The CSF normalizes these security requirements and provides clarity and consistency, reducing the burden of compliance with the varied requirements that apply to organizations.

International Organization for Standardization

The International Organization for Standardization (ISO) 27001 is a globally recognized, standards-based approach to security that outlines requirements for an organization's cybersecurity management system.

The NIST Cybersecurity Framework

The NIST CSF guides organizations on how to improve their ability to prevent, detect, and respond to cybersecurity risks. The NIST 800-53 standard is a publication that recommends security controls for federal information systems and organizations and documents security controls for all federal information systems, except those designed for national security.

Inside the Healthcare Cybersecurity Framework: Third-Party Audits and Certifications

As statistics show, healthcare data breaches and cyberattacks are rarely isolated, infrequent events, but rather ongoing threats requiring constant vigilance. And with the mounting drive for more connectivity throughout the industry, health systems and their IT vendors must prioritize an active and optimized cybersecurity framework in their digital and operational strategies. The most secure protocols define the security responsibility in the vendor-partner relationship and hold vendors accountable to routine audits and compliance measures.

About the Author

Kevin is the Chief Information Security Officer at Health Catalyst. Prior to joining with Health Catalyst, he worked for Blue Cross of Idaho in Boise, Idaho as a Service Oriented Architecture (SOA) Development Manager and worked there for five years. Before Blue Cross of Idaho, Kevin worked in the Hi-Tech sector within e-commerce developing enabling technologies for Micron, a Semiconductor Manufacturer to sell and distribute their product portfolio to consumers. Kevin has an Associates in Political Science from BYI-Idaho, a Bachelor's in Business Administration in Computer Information Systems from Boise State University and a Master's of Science in Medical Informatics from Northwestern University. He continues to teach as an Instructor at Northwestern in the Masters of Medical Informatics Program and also Computer Science at a local community college.