Health Catalyst, Inc.

System and Organization Controls Report (SOC 3)

Independent Report of the Controls to meet the criteria for the Security, Availability, and Confidentiality categories for the period of June 1, 2020 through May 31, 2021.

KirkpatrickPrice

4235 Hillsboro Pike
Suite 300
Nashville, TN 37215

TABLE OF CONTENTS

ASSERTION OF HEALTH CATALYST, INC. MANAGEMENT

ASSERTION OF HEALTH CATALYST, INC. MANAGEMENT

We are responsible for designing, implementing, operating, and maintaining effective controls within Health Catalyst, Inc.'s data, analytics, and decision support system (system) throughout the period June 1, 2020, to May 31, 2021, to provide reasonable assurance that Health Catalyst, Inc.'s service commitments and system requirements relevant to Security, Availability, and Confidentiality were achieved. Our description of the boundaries of the system is presented in section A and identifies the aspects of the system covered by our assertion.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period June 1, 2020, to May 31, 2021, to provide reasonable assurance that Health Catalyst, Inc.'s service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Availability, and Confidentiality (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*). Health Catalyst, Inc.'s objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented in section B.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of these inherent limitations, a service organization may achieve reasonable, but not absolute, assurance that its service commitments and system requirements are achieved.

We assert that the controls within the system were effective throughout the period June 1, 2020, to May 31, 2021, to provide reasonable assurance that Health Catalyst, Inc.'s service commitments and system requirements were achieved based on the applicable trust services criteria.

INDEPENDENT SERVICE AUDITOR'S REPORT

Board of Directors
Health Catalyst, Inc.
10897 South River Front Parkway, Suite #300
South Jordan, UT 84095

Scope

We have examined Health Catalyst, Inc.'s accompanying assertion titled "Assertion of Health Catalyst, Inc. Management" (assertion) that the controls within Health Catalyst, Inc.'s data, analytics, and decision support system (system) were effective throughout the period June 1, 2020, to May 31, 2021, to provide reasonable assurance that Health Catalyst, Inc.'s service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Availability, and Confidentiality (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

Service Organization's Responsibilities

Health Catalyst, Inc. is responsible for its service commitment and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that Health Catalyst, Inc.'s service commitments and system requirements were achieved. Health Catalyst, Inc. has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, Health Catalyst, Inc. is responsible for selecting, and identifying in its assertion, the applicable trust services criteria and for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls within the system.

Service Auditor's Responsibilities

Our responsibility is to express an opinion, based on our examination, on whether management's assertion that controls within the system were effective throughout the period to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Our examination included:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements
- Assessing the risks that controls were not effective to achieve Health Catalyst, Inc.'s service commitments and system requirements based on the applicable trust services criteria

- Performing procedures to obtain evidence about whether controls within the system were effective to achieve Health Catalyst, Inc.'s service commitments and system requirements based on the applicable trust services criteria

Our examination also included performing such other procedures as we considered necessary in the circumstances.

Inherent Limitations

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Opinion

In our opinion, management's assertion that the controls within Health Catalyst, Inc.'s data, analytics, and decision support system were effective throughout the period June 1, 2020, to May 31, 2021, to provide reasonable assurance that Health Catalyst, Inc.'s service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

Joseph Kirkpatrick
CPA, CISSP, CGEIT, CISA, CRISC, QSA
4235 Hillsboro Pike, Suite 300
Nashville, TN 37215

August 13, 2021

HEALTH CATALYST, INC.'S DESCRIPTION OF ITS DATA, ANALYTICS, AND DECISION SUPPORT SYSTEM

SECTION A:
HEALTH CATALYST, INC.'S DESCRIPTION OF THE BOUNDARIES OF ITS DATA, ANALYTICS, AND DECISION SUPPORT SYSTEM

Services Provided

Health Catalyst, Inc. (Health Catalyst) offers custom data analytics, decision support, and interoperability services solutions that help healthcare delivery organizations improve patient outcomes by facilitating the integration of disparate data sources. Health Catalyst offers a Data Operating System (DOS) that is designed to consume more than 100+ data sources, consolidate the data into subject- and purpose-specific data marts, and provide data access points for applications to provide several services to clients. Services to clients include data analysis, electronic medical record (EMR) integration, community health exchange integration, care management measures, dashboards, and workflows supporting patient care, billing, and revenue management processes for healthcare entities. The mix of applications delivered and data consumed is tailored to each client.

In addition to DOS-based services, the Healthfinch and Health Catalyst Interoperability divisions support clients with non-DOS-based data sources and delivery. These services are defined and designed for the clients' needs. Health Catalyst then provides additional services to help organizations through clinical improvement processes. Health Catalyst Interoperability (HCI) collects patient data from all connected external sources, allowing providers to access single, de-duplicated, comprehensive Continuity of Care Documents (CCDs) at a single click. This clinical intelligence supports point-of-care decision making using a process of data aggregation that normalizes the data and transforms it into a usable document, streamlining healthcare workflows. This "analytic interoperability" unites providers and creates a larger data asset for the community of care.

Foundational Applications encourage the broad use of the data warehouse by presenting dashboards, reports, and basic registries across clinical and departmental areas. Discovery Applications allow users to discover patterns and trends within data that inform prioritization, generate new hypotheses, and define populations for management. Advanced Applications provide deep insights into evidence-based metrics that drive improvement in quality and cost reduction through managing populations, workflows, and patient injury prevention.

Health Catalyst has clients sign agreements for services, including a master services agreement (MSA), business associate agreements, and an order form outlining general and specific delivery requirements. The organization's customer service and account management teams work with clients during onboarding to define appropriate services to provide and specifications for data inflows and outflows from the system. Professional services are available in some business lines to provide additional onboarding or ongoing services to assist customers in implementing and operating the systems provided. The organization's agreements outline general security, confidentiality, and compliance commitments.

All applications are delivered through direct EMR or system integrations, data exchange systems, or web-based applications.

Client access to systems is facilitated through Internet Protocol security (IPsec) virtual private network (VPN) tunnels, Whitelisted Internet Protocol (IP) File Transfer Protocol (FTP) and Hypertext Transfer Protocol (HTTP) services, and generally available web-based applications.

The organization has systems housed in the United States that support the services it provides. Primary development and support activities for the systems are located within the United States, and additional support and development staff are in Central and South America as well as India. Systems are physically housed in colocation facilities or hosted by Azure or Amazon Web Services (AWS) cloud providers.

The organization has a single third party that was acquired by Health Catalyst that is provided access to specific clients' data. Health Catalyst DOS clients are configured to send data to Able Health, the third party that is provided access to client data. The Able Health service processes provided data and generates measures relevant to the data to allow for appropriate decision making and reporting. Able Health hosts its data services in AWS within the United States regions.

Health Catalyst has business processes that address typical information security best practices for software-as-a-service (SaaS) and data-hosting services. The organization's controls are also in compliance with the Health Insurance Portability and Accountability Act (HIPAA).

Infrastructure and Software

Health Catalyst maintains a network diagram that represents the organization's critical network infrastructure. The network diagram is updated annually or when changes are made and is reviewed and approved by the IT management division. Health Catalyst isolates sensitive systems from other systems by implementing firewalls or network security groups.

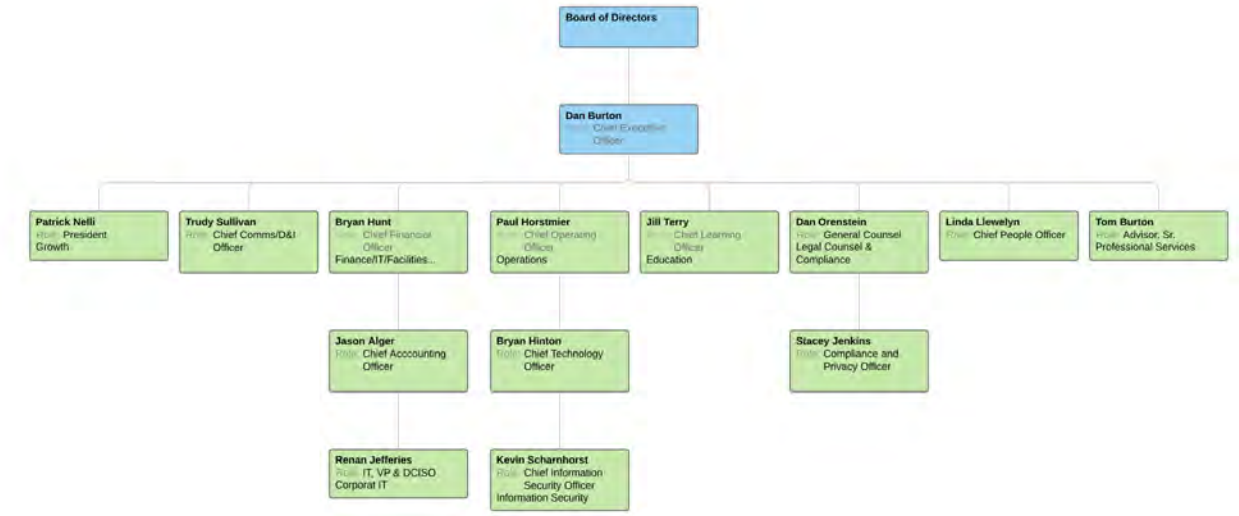
The organization has an Information Security Management System (ISMS) Policy that requires maintenance of an inventory of systems. The system inventory is maintained through methods that vary based on division. Each division uses automated systems to track assets that are in production or assigned to employees.

The organization maintains its software inventory through workstation management services that include Active Directory (AD) and production environments that use automatically updated deployment automation.

People

Health Catalyst and HCI have achieved greater merging of team structures where one core team maintains the infrastructure behind the customer-facing application and services. In 2020, Health Catalyst acquired Able Health, Healthfinch, and Vitalware business entities and is treating these newly acquired business entities as business units or divisions. A new business line, Population Health, has been formed and has nine total products, two of which are Able Health and Healthfinch. The Vitalware business unit folds up under Health Catalyst's financial services business unit.

The organization is structured in a traditional hierarchy. Health Catalyst has an organizational chart that distinguishes the various divisions and their operation under respective executive leadership. The organization's executive leadership reports to the Chief Executive Officer (CEO). Health Catalyst's organization chart shows the relationship between executive management and information security oversight conducted by the Chief Technology Officer (CTO) under the Chief Operating Officer (COO).



The organization's security team reports to the same division as the DOS operations team, while other application and service teams report to different divisional leadership based on the alignment of the service with the organization's strategic vision. The security team is led by the Chief Information Security Officer (CISO) and oversees the security and compliance efforts for all product lines and business units.

Health Catalyst is publicly traded, and its board of directors consists of appointed members who are responsible for the direction of the organization and are the final decision-making authority. The organization's board of directors is kept informed about information security controls and issues.

Data

Health Catalyst has an Information Classification Policy that classifies data to determine data handling parameters including retention and storage requirements. The policy identifies the three ways in which data is classified and captured by the organization: confidentially, internally, and publicly. Data handled by the organization is related to healthcare and includes electronic protected health information (ePHI) and the client activities. Health Catalyst identifies data flows and handles data in compliance with its data classification policies and general best practices. The organization's data includes the following:

- Data entry and uploading
- Data analytics
- Data exchange with client-side systems

- Data reporting and extracts, including application programming interface (API) and secure file-transfer delivery

The organization stores, processes, and transmits data related to medical records and claims and is subject to HIPAA and contract requirements with clients. Client commitments are documented in contracts and addressed by customer configurations in client environments, when applicable.

Health Catalyst generally accepts data through multiple channels, which vary by division and application. Data processing results in data outputs in web application screens, reports, API available data sets, and file transfers.

The organization's data flow diagram (below) shows how data enters and leaves the control of the organization, including user interfaces, file transfers, and APIs.

The organization's ISMS Policy requires storage of sensitive data in data centers and encryption of all transmissions across public or untrusted networks. The ISMS Policy specifies the use of strong encryption and industry acceptance as guidance for encryption standards or practices. The organization bases its encryption standards on Azure and AWS best practices. Data storage never physically leaves the organization's colocation or cloud service facilities on media. All transmissions across networks are protected by hypertext transfer protocol secure (HTTPS), Secure Shell protocol (SSH), and Internet Protocol Security (IPsec) tunnels.

Processes and Procedures

Management has developed and communicated procedures to guide the provision of the organization's services. Changes to procedures are performed annually and authorized by management. These procedures cover the following key security life cycle areas:

- Data classification
- Categorization of information
- Assessment of the business impact resulting from proposed security approaches
- Selection, documentation, and implementation of security controls
- Performance of annual management self-assessments to assess security controls
- Authorization, changes to, and termination of information system access
- Monitoring security controls
- Management of access and roles
- Maintenance and support of the security system and necessary backup and offline storage
- Incident response
- Maintenance of restricted access to system configurations, user functionality, master passwords, powerful utilities, and security devices

SECTION B:
PRINCIPAL SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS

Regulatory Commitments

The organization is subject to regulatory requirements under HIPAA and supports these requirements through its security and compliance policies. Health Catalyst reviews regulatory compliance via HITRUST certification and annual compliance reviews conducted both internally and through a third party. The organization has a compliance program, assessments, and certifications that are designed to support compliance with HIPAA and general information security best practices.

Contractual Commitments

Health Catalyst commits to varying levels of service commitments based on the division and application of its services. MSAs and other supporting contractual documentation are used to outline the organization's response time commitments to its customers, based on severity and availability commitments. The organization's MSA contains the binding agreement with Microsoft and Microsoft's Cloud Agreement, specifies the agreement to Health Catalyst and includes its terms and agreements. The organization addresses specific uptime and response time in contracts, which vary based on the services provided. All contracts established by Health Catalyst include commitments to security and confidentiality.

Clients are promised different performance levels based on product line and client contract requirements. The organization has implemented systems and processes, internally and through critical third-party service providers, designed to meet the organization's service commitments to clients.

System Design

Health Catalyst designs its data, analytics, and decision support system to meet its regulatory and contractual commitments. These commitments are based on the services that Health Catalyst provides to its clients, the laws and regulations that govern the provision of those services, and the financial, operational, and compliance requirements that Health Catalyst has established for its services. Health Catalyst establishes operational requirements in its system design that support the achievement of its regulatory and contractual commitments. These requirements are communicated in Health Catalyst's system policies and procedures, system design documentation, and contracts with clients.