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, 2019 through May 31, 2020.

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, 2019, to May 31, 2020, 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, 2019, to May 31, 2020, 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, 2019, to May 31, 2020, 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

INDEPENDENT SERVICE AUDITOR'S REPORT

Board of Directors
Health Catalyst, Inc.
3165 Millrock Drive #400
Salt Lake City, UT 84121

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, 2019, to May 31, 2020, 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, 2019, to May 31, 2020, 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

July 22, 2020

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. The organization's core platform is known as the Data Operating System (DOS). 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.

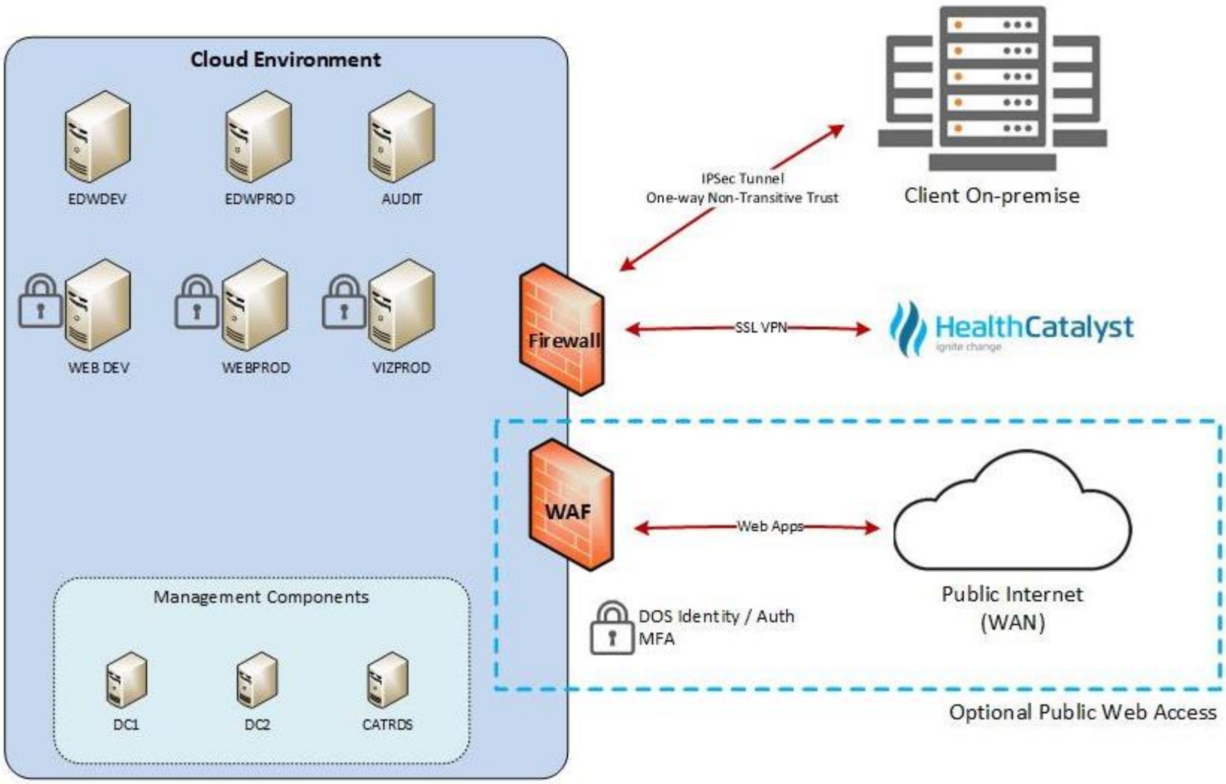
The organization uses a data warehouse, which runs currently on a Microsoft SQL Server stack, to bring in healthcare delivery related data into a single source. A set of applications running on the analytics platform QlikView are then used to help healthcare organizations find the right opportunity for quality improvement. Health Catalyst then provides additional services to help organizations through clinical improvement processes.

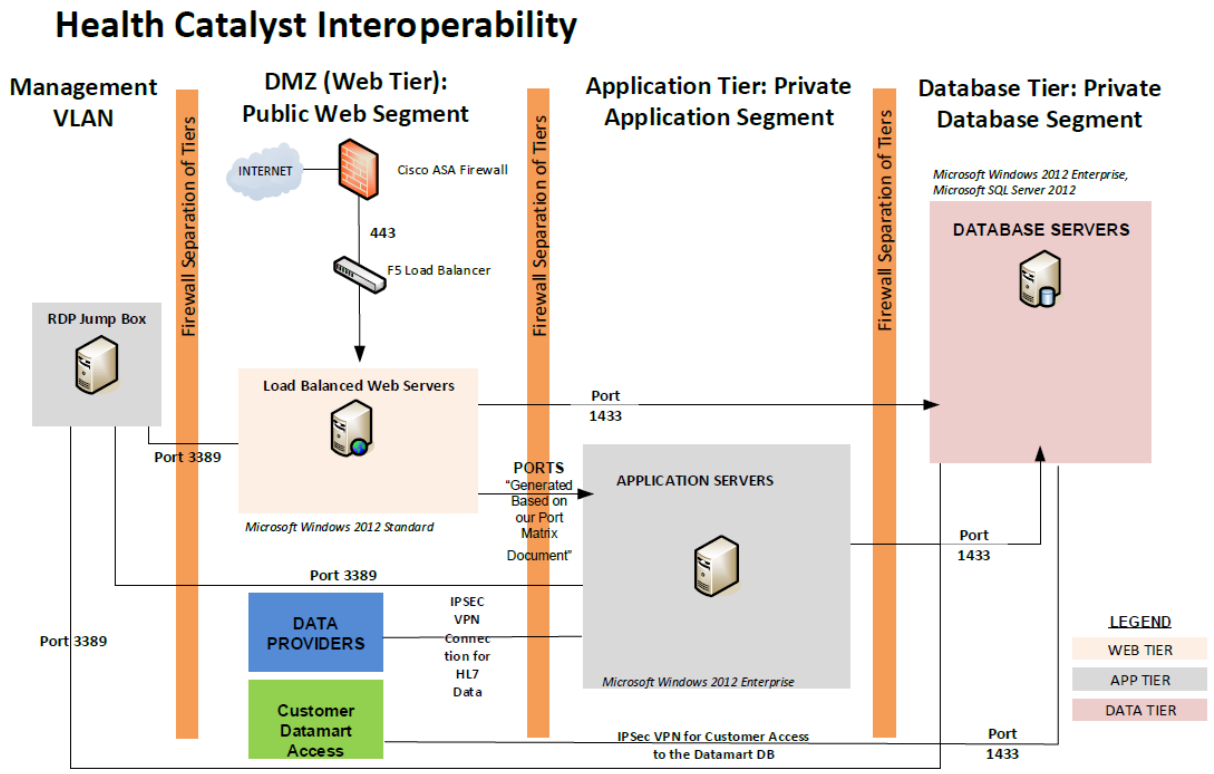
In July 2018, Health Catalyst acquired Health Catalyst Interoperability (HCI), which integrates with DOS, offering next-generation interoperability capabilities by enabling the complete exchange of clinical data without special effort or extra steps. HCI collects patient data from any and all connected 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 health care workflows. This "analytic interoperability" unites providers and creates a larger data asset for the community of care.

Infrastructure and Software

An inventory of systems is required by policy to be maintained by Health Catalyst; it is maintained automatically through the use of system management platforms. Additionally, a software inventory is maintained by the organization through the use of reporting tools. Manual methods are used for license tracking.

Network diagrams are maintained to illustrate the critical network infrastructure in use, as well as the isolation of sensitive systems from other systems. The diagrams are required to be updated at least annually, or whenever significant changes are made. The diagrams are maintained by the Senior Security Architect and the Software Engineering Director and are required to be reviewed and approved by the Chief Information Security Officer (CISO). The Health Catalyst and HCI network diagrams are shown below.


Cloud Environment
EDWDEV
EDWPROD
AUDIT
WEB DEV
WEBPROD
VIZPROD
Management Components
DC1
DC2
CATRDS
Firewall
WAF
IPSec Tunnel
One-way Non-Transitive Trust
Client On-premise
SSL VPN
HealthCatalyst
ignite change
Web Apps
Public Internet
(WAN)
DOS Identity / Auth
MFA
Optional Public Web Access


Health Catalyst Interoperability
Management VLAN
DMZ (Web Tier): Public Web Segment
Application Tier: Private Application Segment
Database Tier: Private Database Segment
Firewall Separation of Tiers
Firewall Separation of Tiers
Firewall Separation of Tiers
INTERNET
Cisco ASA Firewall
443
F5 Load Balancer
RDP Jump Box
Load Balanced Web Servers
Microsoft Windows 2012 Standard
Port 3389
Port 3389
Port 3389
Port 1433
PORTS "Generated Based on our Port Matrix Document"
APPLICATION SERVERS
Microsoft Windows 2012 Enterprise
Microsoft Windows 2012 Enterprise, Microsoft SQL Server 2012
DATABASE SERVERS
Port 1433
DATA PROVIDERS
IPSEC VPN Connection for HL7 Data
Customer Datamart Access
IPSec VPN for Customer Access to the Datamart DB
Port 1433
LEGEND
WEB TIER
APP TIER
DATA TIER

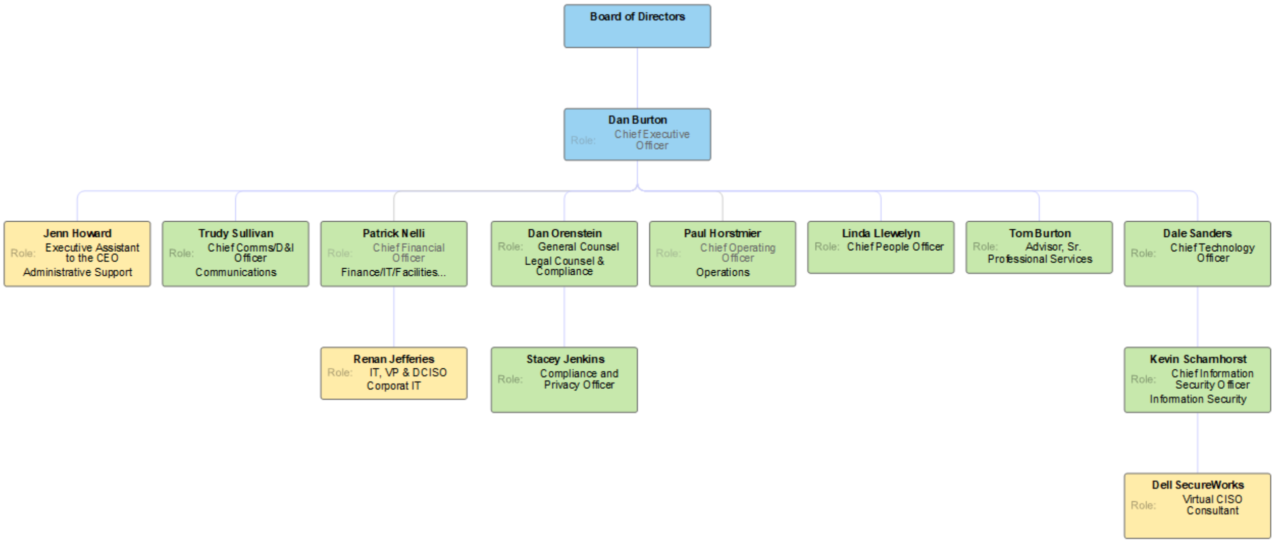
Description:	Page Title: HCI Hosted Network	HealthCatalyst	
This diagram represents the hosted client environments within the Health Catalyst Interoperability data centers.	Author: Brandon Jones	Date Revised: 14 April, 2020	Page: 1 of 1
	Reviewed By Brandon Jones	Date Reviewed: 14 April, 2020	

People

A Board of Directors is in place within Health Catalyst and is responsible for all final decision-making authority and appointing the Chief Executive Officer (CEO). The Board governs the organizational policies and objectives that guide Health Catalyst's mission and purpose at the advice of the CEO. Committees are chaired by members of the Board, who have a variety of experience for the committee they head. Different parts of the organization participate in the committees and report to them on a quarterly basis on the objectives assigned to the individuals that serve on those committees. Health Catalyst is a publicly traded company on NASDAQ with symbol HCAT.

Both business divisions within the organization report to the same executive team, which consists of the CEO, the Chief Operating Officer (COO), and the Chief Technology Officer (CTO), as well as other officers and leaders. Operations includes the IT teams responsible for providing services and service-providing technology to clients. Technology includes the Chief Information Security Officer (CISO) and other support roles. Security oversight is provided by the CISO, who reports to the CTO, and the remainder of IT is overseen by the COO. Both the CTO and COO report to the CEO, and this division allows the CISO to report objectively to the CTO and CEO. The Compliance and Privacy Officer reports up to management through General Counsel.

A traditional hierarchy is maintained within the organization, and an Organization Chart, shown below, is documented to illustrate this structure and the defined reporting relationships.


Board of Directors
Dan Burton
Role: Chief Executive Officer
Jenn Howard
Role: Executive Assistant to the CEO
Administrative Support
Trudy Sullivan
Role: Chief Comms/D&I Officer
Communications
Patrick Nelli
Role: Chief Financial Officer
Finance/IT/Facilities...
Dan Orenstein
Role: General Counsel
Legal Counsel & Compliance
Paul Horstmier
Role: Chief Operating Officer
Operations
Linda Llewelyn
Role: Chief People Officer
Tom Burton
Role: Advisor, Sr. Professional Services
Dale Sanders
Role: Chief Technology Officer
Renan Jefferies
Role: IT, VP & DCISO
Corporat IT
Stacey Jenkins
Role: Compliance and Privacy Officer
Kevin Scharnhorst
Role: Chief Information Security Officer
Information Security
Dell SecureWorks
Role: Virtual CISO Consultant

The following personnel were interviewed as part of the audit engagement:

- CISO
- Senior Security Architect
- Senior Human Resources (HR) Generalist

Data

Data classification requirements and data handling requirements are documented in policy and include the following classifications: Confidential, Internal, and Public. All data and services that are housed within the data centers are considered to be confidential, and classifications are reviewed on an annual basis, as well as continuously through the change control procedure when any changes are made, or new systems are introduced.

Client commitments for data retention are documented in contracts and are addressed by specific configurations in dedicated client environments. Data retention in the client environments is under the control of clients; however, the organization is required to consider HIPAA requirements in regard to their data retention practices.

A key management system is required to be implemented within the organization, and keys are to be protected accordingly. Keys used by the organization include disk encryption keys and file encryption keys and are generally protected by native encryption systems. All access to the management modules where the keys are stored is tracked.

Data that is stored, processed, and transmitted by the organization is sensitive in nature and can include both ePHI and personally identifiable information (PII) data that is pulled from client source systems. Sensitive data is collocated in the Health Catalyst Enterprise Data Warehouse over a secured IPsec tunnel or from a secure file transfer protocol (SFTP) connection. The data is only allowed in the cloud services environment, and data transmission is limited to HTTPS and SFTP.

Policies are in place to prohibit the transfer of data outside of the cloud services environment by those connected via secure sockets layer virtual private network (SSL VPN) connections over remote desktop protocol (RDP). The SSL VPN requires the use of multi-factor authentication to establish the connection. Training about these policies is required to be annually refreshed by personnel working within the client environments.

Sensitive data is not allowed on any corporate laptops or in the corporate environment, per company policy. As an additional safeguard, laptops have their hard drives encrypted using BitLocker, and data within these environments is encrypted in two ways. Any data tied directly to the database servers is inherently encrypted at rest with self-encrypting storage. Strong encryption methods are used in both cases, including the use of AES 256. HCI follows similar practices to ensure that data at rest and in transit is encrypted by the same means. Additionally, HCI does not allow connectivity into the hosted environment except by authorized personnel who administrate the environment.

Data flow diagrams are documented and maintained to illustrate how data moves throughout the organization, including the use of secure file transfer, data exchange protocols, and web applications and APIs.

Processes and Procedures

Management has developed and communicated processes and procedures to employees to ensure the execution of policy documentation and critical business processes. Changes to these procedures are performed annually and are 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 the 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, necessary backup, and offline storage
- Incident response
- Maintenance of restricted access to system configurations, user functionality, passwords, powerful utilities, and security devices

SECTION B:
PRINCIPLE SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS

Regulatory Commitments

The organization is subject to regulatory requirements under the Sarbanes–Oxley Act (SOX), Code of Federal Regulations (CFR) 11, and the Health Insurance Portability and Accountability Act (HIPAA). The Health Catalyst security, risk management, and compliance program is structured around National Institute of Standards and Technology (NIST) frameworks, and the organization undergoes a HITRUST certification that includes Electronic Healthcare Network Accreditation Commission (EHNAC) accreditation. Government-managed exclusion list checks are also conducted on a monthly basis for all employees.

Contractual Commitments

Master service agreements (MSAs) and other supporting contractual documentation are used to outline the organization's response time commitments to their customers, based on severity and availability commitments. The organization commits to 99.5% uptime for Health Catalyst services and 99.9% for HCI, as documented within contracts. The contracts include requirements for the provision of appropriate security controls to protect the confidentiality and integrity of the data processed, and these security provisions include typical business associate agreement (BAA) language.

System Design

To meet its availability and performance commitments, Health Catalyst selects top tier cloud and colocation providers to host data procession environments. Deployments leverage modern hypervisor clustering or server clustering to provide a redundant platform. A robust change management and application development lifecycle ensure changes to environments are well designed and tested prior to production deployment. To meet its confidentiality and integrity commitments, Health Catalysts implements layered approach of preventative and detective controls in addition to a robust access control process.