Health Catalyst, Inc.

South Jordan, Utah

System and Organization Controls Report Relevant to the Ignite Data and Analytics and Health Information Exchange Solutions System

SOC 3® Report

June 1, 2024 to May 31, 2025

The report, including the title page, table of contents, and sections, constitutes the entire report and should be referred to only in its entirety and not by its component parts. The report contains proprietary information and is considered confidential.

Health Catalyst, Inc. SOC 3 Report

June 1, 2024 to May 31, 2025

Table of Contents

Section 1
Health Catalyst Inc.’s Assertion

Health Catalyst, Inc.'s Assertion

We are responsible for designing, implementing, operating, and maintaining effective controls within Health Catalyst's ("Health Catalyst") Ignite Data and Analytics and Health Information Exchange Solutions System (the "system") throughout the period June 1, 2024 to May 31, 2025, to provide reasonable assurance that Health Catalyst'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 Attachment 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, 2024 to May 31, 2025, to provide reasonable assurance that Health Catalyst's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, and confidentiality (the "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'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. In addition, the evaluation included the controls to meet the requirements 45 C.F.R. Sections 160.203 (Subpart B – Preemption of State Law), 160.316 (Subpart C – Refraining from Intimidation or Retaliation), PART 164 45 C.F.R. Sections 164.308-314 (the "applicable HIPAA Security Rule Requirements"), and 164.400 – 164.414 (Subpart D – HIPAA Breach Notification Requirements), Sections 164.502-164.530 (Subpart E) (the "applicable HIPAA Privacy Rule Requirements") set forth in the U.S. Department of Health and Human Services' (HHS) Health Insurance Portability and Accountability Act (HIPAA). Health Catalyst's objectives for the system in applying the applicable trust services criteria and the HIPAA Security and Privacy Rule and 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 and HIPAA Security and Privacy Rule are presented in Attachment B.

Health Catalyst uses subservice organizations to provide cloud-based infrastructure and services, colocation facilities, data security platform services, and security operation center services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Health Catalyst, to achieve Health Catalyst's service commitments and system requirements based on the applicable trust services criteria and the applicable HIPAA Security and Privacy Rule Requirements. The description presents Health Catalyst's controls, the applicable trust services criteria, the applicable HIPAA Security and Privacy Rule Requirements, and the types of complementary subservice organization controls assumed in the design of Health Catalyst's controls. The description does not disclose the actual controls at the subservice organizations.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Health Catalyst, to achieve Health Catalyst's service commitments and system requirements based on the applicable trust services criteria and the applicable HIPAA Security and Privacy Rule Requirements. The description presents Health Catalyst's controls, the applicable trust services criteria, the applicable HIPAA Security and Privacy Rule Requirements, and the complementary user entity controls assumed in the design of Health Catalyst's controls.

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, 2024 to May 31, 2025, to provide reasonable assurance that Health Catalyst's service commitments and system requirements were achieved based on the applicable trust services criteria and the applicable HIPAA Security and Privacy Rule Requirements.

Section 2
Independent Service Auditor's Report

WIPFLI

Independent Service Auditor's Report

Management of Health Catalyst, Inc.
South Jordan, Utah

Scope

We have examined Health Catalyst Inc.'s (Health Catalyst) accompanying assertion titled " Health Catalyst's Assertion" (the "assertion") that the controls within Health Catalyst's Ignite Data and Analytics and Health Information Exchange Solutions System (the "system") were effective throughout the period June 1, 2024 to May 31, 2025, to provide reasonable assurance that Health Catalyst's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, and confidentiality (the "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*). We have also evaluated the suitability of the design and operating effectiveness of controls to meet the requirements of 45 C.F.R. Sections 160.203 (Subpart B – Preemption of State Law), 160.316 (Subpart C – Refraining from Intimidation or Retaliation), PART 164 45 C.F.R. Sections 164.308-314 (the "applicable HIPAA Security Rule Requirements"), 164.400 – 164.414 (Subpart D – HIPAA Breach Notification Requirements), Sections 164.502-164.530 (Subpart E) (the "applicable HIPAA Privacy Rule Requirements") set forth in the U.S. Department of Health and Human Services' (HHS) Health Insurance Portability and Accountability Act (HIPAA).

Health Catalyst uses subservice organizations to provide cloud-based infrastructure and services, colocation facilities, data security platform services, and security operation center services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Health Catalyst, to achieve Health Catalyst's service commitments and system requirements based on the applicable trust services criteria and the applicable HIPAA Security and Privacy Rule Requirements. The description presents Health Catalyst's controls, the applicable trust services criteria, the applicable HIPAA Security and Privacy Rule Requirements, and the types of complementary subservice organization controls assumed in the design of Health Catalyst's controls. The description does not disclose the actual controls at the subservice organizations, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with the controls at Health Catalyst, to achieve Health Catalyst's service commitments and system requirements based on the applicable trust services criteria and the applicable HIPAA Security and Privacy Rule Requirements. The description presents Health Catalyst's controls, the applicable trust services criteria, the applicable HIPAA Security and Privacy Rule Requirements, and the complementary user entity controls assumed in the design of Health Catalyst's controls. Our examination did not include such complementary user entity controls, and we have not evaluated the suitability of the design and operating effectiveness of such controls.

Service Organization's Responsibilities

Health Catalyst is responsible for its service commitments and system requirements and for designing,

implementing, and operating effective controls within the system to provide reasonable assurance that Health Catalyst's service commitments and system requirements were achieved. Health Catalyst has provided the accompanying assertion in Section 1 titled "Health Catalyst, Inc.'s Assertion" (the "assertion") about the description and the suitability of the design and operating effectiveness of controls stated therein. Health Catalyst is also responsible for preparing the description and assertion, including the completeness, accuracy, and method of presentation of the description and assertion; providing the services covered by the description; selecting the applicable trust services criteria, and the applicable HIPAA Security and Privacy Rule Requirements, and stating the related controls in the description; and identifying the risks that threaten the achievement of the service organization's service commitments and system requirements.

Service Auditor's Responsibilities

Our responsibility is to express an opinion, based on our examination, on 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 and the applicable HIPAA Security and Privacy Rule Requirements. 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's service commitments and system requirements based on the applicable trust services criteria and the applicable HIPAA Security and Privacy Rule Requirements.
- Performing procedures to obtain evidence about whether controls within the system were effective to achieve Health Catalyst's service commitments and system requirements based on the applicable trust services criteria and the applicable HIPAA Security and Privacy Rule Requirements.

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 and the applicable HIPAA Security and Privacy Rule Requirements. 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's Ignite Data and Analytics and Health Information Exchange Solutions System were effective throughout the period June 1, 2024 to May 31, 2025, to provide reasonable assurance that Health Catalyst's service commitments and system requirements were achieved based on the applicable trust services criteria and the applicable HIPAA Security and Privacy Rule Requirements is fairly stated, in all material respects.

Wipfli LLP

Philadelphia, Pennsylvania
October 7, 2025

Attachment A – Description of the Ignite Data and Analytics and Health Information Exchange Solutions System Provided by Health Catalyst, Inc.

Description of the Ignite Data and Analytics and Health Information Exchange Solutions System Provided by Health Catalyst, Inc.

Company Overview

Services Provided

Health Catalyst, Inc. (Health Catalyst or the Organization) 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 platforms that are 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 Ignite based services, Health Catalyst's Interoperability (HCI) and KPI Ninja division supports clients with non-Ignite-based data sources and delivery. These services are defined and designed for the client's needs. Health Catalyst then provides additional services to help organizations through clinical improvement processes. 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 agreement, and an order form outlining general and specific delivery requirements. The Organization's client service and account management teams work with clients during onboarding to define appropriate services to provide 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 clients in implementing and operating the systems provided. The Organization's agreements outline general security, confidentiality, and compliance commitments.

The scope of the report includes the infrastructure supporting the Ignite Data and Analytics and Interoperability Platform. Health Catalyst is considered a business associate and not a covered entity.

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).

Description of the Ignite Data and Analytics and Health Information Exchange Solutions System Provided by Health Catalyst, Inc.

Description of the Population Health Suite, Patient Engagement, Clinical Quality Improvement Accelerators, and Revenue Cycle Management

Infrastructure and Software

Health Catalyst leverages Microsoft Azure for cloud-based infrastructure and services and Flexential's colocation facilities for HCI-hosted clients. KPI Ninja is a solution that is merged together with HCI and is hosted on the Amazon Web Services platform with future intent to move Flexential into this environment. 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 cloud services.

Name	Applications	Scope	Operating System / Database Server Types	Residing Facilities
Ignite Data & Analytics	• Source Mart Designer (SMD) • Subject Area Mart Designer (SAMD) • Atlas • Operations Console • Instant Data Entry Application (IDEA) • Pop Analyzer, • Pop Insights • PowerCosting • PowerLabor • Value Optimizer • Care Flow • COVID-19 • Data Quality and Performance • Healthcare.AI **<u>Data Management Tools</u>** • Health Catalyst source templates • Job Scheduling • Data profiling • Identity Management **<u>Data Products</u>** • Expert Data Collections • Terminology • Data Quality Rules	• Ignite Data and Analytics • Decision Support • Machine Learning & AI	• Microsoft Windows • SQL Server • Azure SaaS • Databricks • Snowflake • Azure Data Lake Storage (ADLS) • PostgreSQL • Azure Functions • Fivetran • Azure Key Vault • Immuta	• Microsoft Azure • Immuta • Snowflake

Description of the Ignite Data and Analytics and Health Information Exchange Solutions System Provided by Health Catalyst, Inc.

Name	Applications	Scope	Operating System / Database Server Types	Residing Facilities
	Self-Service Tools • Pop Analyzer • Healthcare.AI • Data Entry • Visualization Tools			
Interoperability	○ Clinical Messaging / HISP ○ Community Health Record (CHR) • Referrals ○ Community Interchange ○ Community Orchestrate ○ DataMart & Reporting Services ○ Exchange Orders & Results ○ Foundational Services - Nexus / MPI ○ Notify	• Health Information Exchange Solutions	• Microsoft Windows • Linux • SQL Server	• Flexential (Salt Lake City, Utah & Denver, Colorado)
KPI Ninja	• Ninja Universe	• Health Information Exchange Solutions	• Microsoft Windows • AWS EC2	• Amazon Web Services (AWS)

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.

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 Information Technology (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 and production environments that use automatically updated deployment automation.

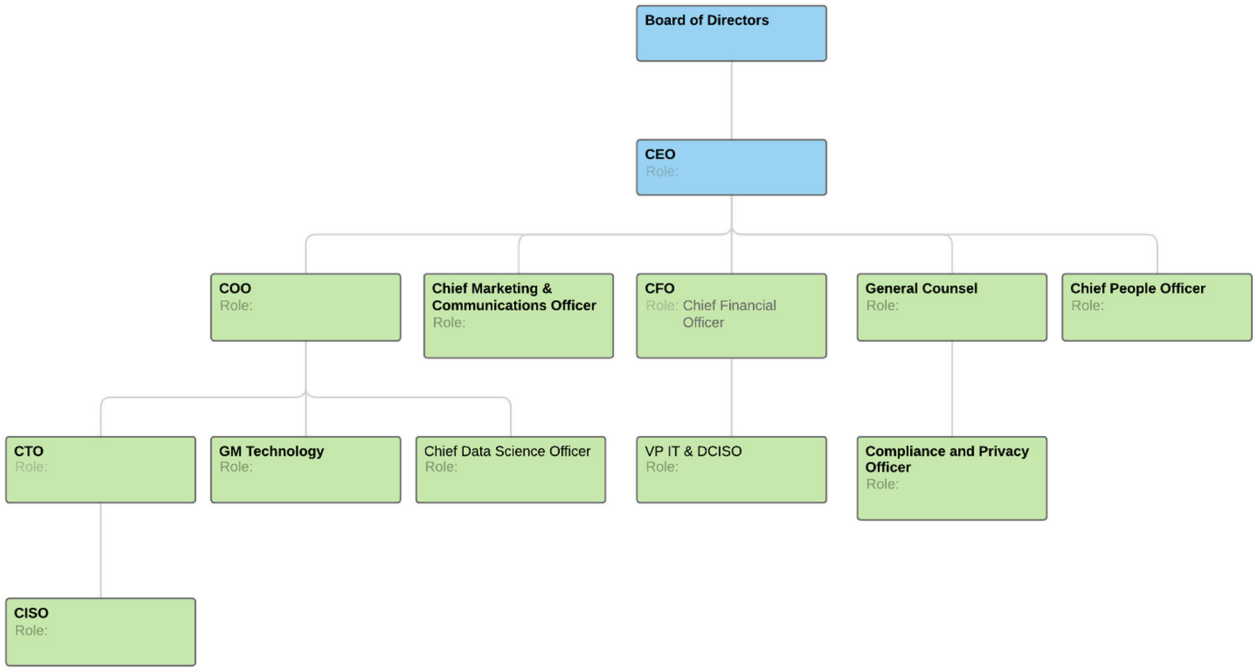
Description of the Ignite Data and Analytics and Health Information Exchange Solutions System Provided by Health Catalyst, Inc.

People

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 organizational 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 Chief Information Security Officer (CISO) who reports to the CTO under the Organization's operational arm of the Organization headed by the COO, 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 CISO oversees the security and compliance efforts for product lines, business units, and corporate IT.

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 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

Attachment A – Description of the Ignite Data and Analytics and Health Information Exchange Solutions System Provided by Health Catalyst, Inc.

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 client 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 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 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. Transmissions across networks are protected by hypertext transfer protocol secure (HTTPS), secure shell protocol (SSH), and IPsec tunnels.

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 of 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

Subservice Organizations

The Ignite Data and Analytics and Health Information Exchange Solutions System uses subservice organizations to perform a range of functions. The following describes the subservice organizations used by the platforms:

Subservice Organization	Function
Microsoft Azure	Cloud-based infrastructure and services
Amazon Web Services	Cloud-based infrastructure and services
Flexential	Colocation facilities
Immuta	Data security platform services, helping Ignite customers protect their cloud data and providing secure access to it
Dell SecureWorks	Security operation center services
Snowflake	Cloud-based data platform used by Ignite that offers a variety of data services, including storage, processing, analytics, and sharing

Attachment A – Description of the Ignite Data and Analytics and Health Information Exchange Solutions System Provided by Health Catalyst, Inc.

Complementary User Entity Control Considerations

Health Catalyst controls were designed with the assumption that certain complementary user entity controls would be operating effectively at user entities. The controls described in this report occur at Health Catalyst and cover only a portion of a comprehensive internal controls structure. Each user entity must address the various aspects of internal control that may be unique to its particular system. This section describes the complementary user entity controls that should be developed, placed in operation, and maintained at user entities as necessary to meet the trust services criteria and the applicable HIPAA Security and Privacy Rule Requirements stated in the description of Health Catalyst's system. User entities should determine whether adequate controls have been established to provide reasonable assurance that:

Complementary User Entity Controls
User organizations implement sound and consistent internal controls regarding general IT system access and system usage appropriateness for all internal user organization components associated with Health Catalyst.
User organizations practice removal of user accounts for any users who have been terminated and were previously involved in any material functions or activities associated with Health Catalyst's services.
Transactions for user organizations relating to Health Catalyst's services are appropriately authorized, and user entities are also responsible to ensure that transactions are secure, timely, accurate, and complete.
For user organizations sending data to Health Catalyst, data is protected by appropriate methods to ensure confidentiality, privacy, integrity, availability, and nonrepudiation.
User organizations implement controls requiring additional approval procedures for critical transactions relating to Health Catalyst's services.
User organizations report to Health Catalyst in a timely manner any material changes to their overall control environment that may adversely affect services being performed by Health Catalyst.
User organizations are responsible for notifying Health Catalyst in a timely manner of any changes to personnel directly involved with services performed by Health Catalyst. These personnel may be involved in financial, technical, or ancillary administrative functions directly associated with services provided by Health Catalyst.
User organizations are responsible for adhering to the terms and conditions stated in their contracts with Health Catalyst.
User organizations are responsible for developing and, if necessary, implementing a business continuity and disaster recovery plan that will aid in the continuation of services provided by Health Catalyst.
User organizations providing information to Health Catalyst are responsible for its accuracy.
User organizations are responsible for reporting any identified security, availability, and confidentiality incidents.

Attachment A – Description of the Ignite Data and Analytics and Health Information Exchange Solutions System Provided by Health Catalyst, Inc.

Complementary Subservice Organization Controls

Health Catalyst's controls related to the Ignite Data and Analytics and Health Information Exchange Solutions System covers only a portion of overall internal control for each user entity of Health Catalyst. It is not feasible for the trust services criteria and the applicable HIPAA Security and Privacy Rule Requirements related to the Ignite Data and Analytics and Health Information Exchange Solutions System to be achieved solely by Health Catalyst. Therefore, each user entity's internal control must be evaluated in conjunction with Health Catalyst's controls and the related tests and results, taking into account the related complementary subservice organization controls expected to be implemented at the subservice organizations as described below.

Complementary Subservice Organization Controls
Subservice organizations are responsible for notifying Health Catalyst of security, availability, and confidentiality incidents.
Subservice organizations are responsible to adhering to the agreements signed with Health Catalyst.
Logical access controls have been implemented at subservice organizations through firewalls, network security, and monitoring tool security.
Subservice organizations providing hosting services have implemented procedures to provide physical and environmental controls for any of Health Catalyst's infrastructure.
Environmental protections, including the following, have been installed: • Cooling systems • Battery and generator backup in the event of power failure • Smoke and Water Detection • Fire extinguishers and suppression system The UPS systems are tested at least annually. The fire suppression systems are tested on an annual basis. Backup generators are tested at least annually.
Subservice organizations are responsible for providing security monitoring alerting over Health Catalyst infrastructure and corresponding data.
Subservice organizations have implemented procedures for identifying, investigating, remediating, and communicating security incidents.
Subservice organizations have implemented procedures to safeguard any of Health Catalyst's corporate and client data used in the provision of their services.
Subservice organization have implemented antivirus and anti-malware protection to safeguard any of Health Catalyst's corporate and client data used in the provision of their services.

Attachment B – Service Commitments and System Requirements of the Health Catalyst Ignite Data and Analytics and Health Information Exchange Solutions System

Attachment B – Service Commitments and System Requirements of the Health Catalyst Ignite Data and Analytics and Health Information Exchange Solutions System

Health Catalyst designs its processes and procedures related to its Ignite Data and Analytics and Health Information Exchange Solutions System (the System) to meet its objectives for the successful delivery of the Ignite Data and Analytics and Health Information Exchange Solutions System. Those objectives are based on the service commitments Health Catalyst makes to user entities, the laws and regulations that govern the provision of the Ignite Data and Analytics and Health Information Exchange Solutions System, and the financial, operational, and compliance requirements Health Catalyst has established for the services. The services of Health Catalyst are subject to the security and privacy requirements of HIPAA, as well as state privacy security laws and regulations in the jurisdictions in which Health Catalyst operates.

Security and confidentiality commitments to user entities are documented and communicated in service level agreements (SLA) and other client agreements, as well as in the description of the service offering provided online. Privacy commitments are provided on the website as well.

- Security commitments include principles within the fundamental designs to permit system users to access the information they need based on their roles in the System, while restricting them from accessing information not needed for their role.
- Confidentiality commitments include the use of encryption technologies to protect client data both at rest and in transit.
- Health Catalyst commits to SLAs or provides a service where reasonable uptimes are expected.
- The Organization maintains business continuity plans and disaster recovery plans.

Health Catalyst establishes operational requirements that support the achievement of security commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in Health Catalyst's system policies and procedures, system design documentation, and contracts with clients. Information security policies define an organization-wide approach to how systems and data are protected. These include policies related to how the service is designed and developed, the system is operated, the internal business systems and networks are managed, and employees are hired and trained. In addition to these policies, standard operating procedures have been documented on how to carry out specific manual and automated processes required when providing the Ignite Data and Analytics and Health Information Exchange Solutions System.

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 clients, based on severity and availability commitments. The Organization's MSA contains the binding agreement with Microsoft and Amazon. 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, and these vary based on the services provided. Contracts established by Health Catalyst include commitments to security and confidentiality.

Attachment B – Service Commitments and System Requirements of the Health Catalyst Ignite Data and Analytics and Health Information Exchange Solutions System

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 services 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.