Health Catalyst, Inc.

South Jordan, Utah

System and Organization Controls Report Relevant to the Population Health Applications Suite, Patient Engagement, and Clinical Quality Improvement System

SOC 3 Report

July 1, 2023 to May 31, 2024

WIPFLI

Health Catalyst, Inc.

SOC 3 Report

July 1, 2023 to May 31, 2024

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, Inc.'s ("Health Catalyst") Population Health Applications Suite, Patient Engagement, and Clinical Quality Improvement System (the "system") throughout the period July 1, 2023 to May 31, 2024, 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 July 1, 2023 to May 31, 2024, 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. The principal service commitments and system requirements related to the applicable trust services criteria are presented in Attachment B.

Health Catalyst uses subservice organizations for cloud hosting, data center services, and security operations 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. The description presents Health Catalyst's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Health Catalyst, Inc.'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. The description presents Health Catalyst's controls, the applicable trust services criteria, 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 July1, 2023 to May 31, 2024, to provide reasonable assurance that Health Catalyst's service commitments and system requirements were achieved based on the applicable trust services criteria.

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, Inc.'s Assertion" (the "assertion") that the controls within Health Catalyst's Population Health Applications Suite, Patient Engagement, and Clinical Quality Improvement System (the "system") were effective throughout the period July 1, 2023 to May 31, 2024, 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 uses subservice organizations for cloud hosting, data center services, and security operations 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. The description presents Health Catalyst's controls, the applicable trust services criteria, 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. The description presents Health Catalyst's controls, the applicable trust services criteria, 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 also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, Health Catalyst 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 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'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'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's Population Health Applications Suite, Patient Engagement, and Clinical Quality Improvement System were effective throughout the period July 1, 2023 to May 31, 2024, to provide reasonable assurance that Health Catalyst's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

Wipfli LLP

Wipfli LLP

Philadelphia, Pennsylvania
October 17, 2024

Attachment A - Description of the Population Health Applications Suite, Patient Engagement and Clinical Quality Improvement System Provided by Health Catalyst, Inc.

Attachment A - Description of the Population Health Applications Suite, Patient Engagement and Clinical Quality Improvement 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 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 Population Health Applications Suite, Patient Engagement, and Clinical Quality Improvement System supports clients with non-DOS-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. The Population Health Applications Suite, Patient Engagement, and Clinical Quality Improvement System handles routine, repeatable and non-reimbursable time-consuming tasks/work that plagues physicians and their staff. The Population Health Applications Suite, Patient Engagement, and Clinical Quality Improvement System leverages the EMR data to automate these tasks, which is enabled by a robust rules engine and evidence-based content, like medication protocols. The Population Health Applications Suite, Patient Engagement, and Clinical Quality Improvement System includes an automated staff augmentation tool. It improves response time to patient requests, identifies and acts upon gaps in care, and safely handles routine tasks.

Health Catalyst has clients sign agreements for services, including a master services agreement (MSA), business associate agreements (BAA), 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 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.

The scope of the report includes the infrastructure supporting the Population Health Applications Suite, Patient Engagement, and Clinical Quality Improvement System products, including the Embedded application, Measurable, and Twistle.

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).

Attachment A - Description of the Population Health Applications Suite, Patient Engagement and Clinical Quality Improvement System Provided by Health Catalyst, Inc.

Components of the System Used to Provide the Services

System Infrastructure and Software

Health Catalyst leverages AWS for Cloud-based infrastructure and services to house the Population Health Applications Suite, Patient Engagement, and Clinical Quality Improvement System. 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. Systems are physically housed in an AWS cloud offering leveraging SaaS offerings.

Applications in the Population Health Applications Suite, Patient Engagement, and Clinical Quality Improvement System are delivered through direct EMR or system integrations or data exchange systems.

Name	Applications	Operating System / Database Server Types	Residing Facilities
Population Health Applications Suite, Patient Engagement, and Clinical Quality Improvement System	• Health Catalyst Embedded Refills™ • Health Catalyst Embedded Care Gaps™ • Twistle by Health Catalyst™ Patient Engagement • MeasureAble™ • Care Management Suite™ • Analytics Accelerators • Pop Analyzer: Stratisfy™ • Value Optimizer™	• AWS EC2 • Linux • AWS SaaS	• Amazon Web Services (AWS) • Aptible

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. Health Catalyst has various virtual servers in the production environment, including application servers and database servers.
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 asset management services that include mobile device management (MDM), using deployment automation.

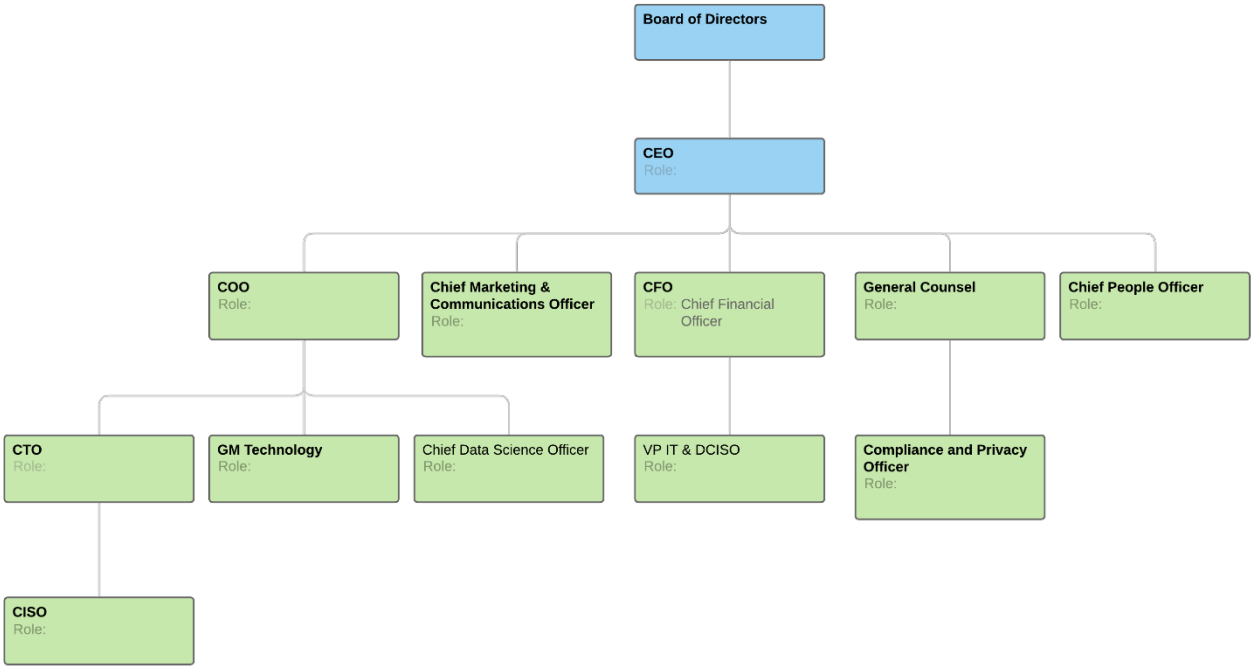
Attachment A - Description of the Population Health Applications Suite, Patient Engagement and Clinical Quality Improvement System Provided by Health Catalyst, Inc.

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 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 Chief Information Systems 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 information technology.

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. Data is classified according to its sensitivity by the application owner and approved by a designated member of senior management using the below criteria:

- Confidential: A significant negative impact to the Organization could occur if data is disclosed but not Private.

- Covered: A significant negative impact to the Organization could occur if data is disclosed and is Private.
- Private: A significant negative impact to the individual could occur if data is disclosed.
- Sensitive: A negative impact could occur if data is disclosed.
- Public: Disclosure has no impact.

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, application programming interface (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 AWS best practices. Data storage never physically leaves the Organization's colocation or cloud service facilities on media. Transmissions across networks are protected through encryption using Secure Sockets Layer (SSL), 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

Subservice Organizations

The Population Health Applications Suite, Patient Engagement, and Clinical Quality Improvement System uses subservice organizations to perform a range of functions. The following describes the subservice organizations used by the Population Health Applications Suite, Patient Engagement, and Clinical Quality Improvement System:

Subservice Organization	Function
Amazon Web Services (AWS)	Cloud-based infrastructure and virtual desktop services for Bastian Hosts within the covered environment
Microsoft Azure	Cloud-based infrastructure and services
Dell SecureWorks	Managed Service Provider for Extended Detect and Response (XDR) and Incident Management
Aptible	Platform as a service used by MeasureAble

Attachment A - Description of the Population Health Applications Suite, Patient Engagement and Clinical Quality Improvement System Provided by Health Catalyst, Inc.

Complementary User Entity Control Considerations

Health Catalyst's 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 stated in the description of Health Catalyst's system. The table below identifies the criteria the complementary user entity controls relate to. User entities should determine whether adequate controls have been established to provide reasonable assurance that:

Complementary User Entity Controls
User organizations should implement sound and consistent internal controls regarding general IT system access and system usage appropriateness for internal user organization components associated with Health Catalyst.
User organizations should 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, including changes to personnel directly involved with services performed by Health Catalyst, for user organizations relating to Health Catalyst's services should be appropriately authorized, and transactions should be secure, timely, and complete.
For user organizations sending data to Health Catalyst, data should be protected by appropriate methods to help ensure security, confidentiality, privacy, integrity, availability, and non-repudiation.
User organizations should implement controls requiring additional approval procedures for critical transactions relating to Health Catalyst's services.
User organizations should 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, Inc.
User organizations are responsible for adhering to the terms and conditions stated within 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.

Attachment A - Description of the Population Health Applications Suite, Patient Engagement and Clinical Quality Improvement System Provided by Health Catalyst, Inc.

Complementary Subservice Organization Controls

Health Catalyst's controls related to the Population Health Applications Suite, Patient Engagement, and Clinical Quality Improvement System cover only a portion of overall internal control for each user entity of Health Catalyst. It is not feasible for the trust services criteria related to the Population Health Applications Suite, Patient Engagement, and Clinical Quality Improvement 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 described in Section 4 of this report, 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.
Video surveillance cameras are used to monitor data center facilities.
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.

Attachment B - Service Commitments and System Requirements of the Population Health Applications Suite, Patient Engagement, and Clinical Quality Improvement System by Health Catalyst, Inc.

Attachment B – Service Commitments and System Requirements of the Population Health Applications Suite, Patient Engagement, and Clinical Quality Improvement System by Health Catalyst, Inc.

Health Catalyst designs its processes and procedures to ambulatory health systems to meet the objectives of delivering insights to the EMR. Those objectives are based on the service commitments Health Catalyst makes to clients, the laws and regulations that govern the provision of the services, and the financial, operational, and compliance requirements the Population Health Applications Suite, Patient Engagement, and Clinical Quality Improvement System has established for the services. The services of the Population Health Applications Suite, Patient Engagement, and Clinical Quality Improvement System are subject to the security and privacy requirements of HIPAA, as well as state privacy security laws and regulations in the jurisdictions in which the Population Health Applications Suite, Patient Engagement, and Clinical Quality Improvement System operates.

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

- Security commitments include principles within the fundamental designs of the Population Health Applications Suite, Patient Engagement, and Clinical Quality Improvement System that are designed 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 customer 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.

The Population Health Applications Suite, Patient Engagement, and Clinical Quality Improvement System establishes operational requirements that support the achievement of security, availability, and confidentiality commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in the Population Health Applications Suite, Patient Engagement, and Clinical Quality Improvement System policies and procedures, system design documentation, and contracts with customers. 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 services related to the Population Health Applications Suite, Patient Engagement, and Clinical Quality Improvement 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 adheres to varying levels of service commitments based on the division and application of its services. MSA and other supporting contractual documentation are used to outline the Organization's response time commitments to its customers, based on security and availability

commitments. The Organization's MSA contains the binding agreement with Amazon Web Services, Microsoft, and Aptible, 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. 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.