Health Catalyst, Inc.
South Jordan, Utah

System and Organization Controls Report
Relevant to the Data Operating System (DOS), Interoperability Platform, Analytics, and Decision Support System

SOC 3® Report

June 1, 2021 to June 30, 2022

Health Catalyst, Inc.

SOC 3 Report

June 1, 2021 to June 30, 2022

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") Data Operating System (DOS), Interoperability Platform, Analytics, and Decision Support System (the "system") throughout the period June 1, 2021 to June 30, 2022, to provide reasonable assurance that Health Catalyst's service commitments and system requirements relevant to security, availability, confidentiality, and privacy 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, 2021 to June 30, 2022, 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, confidentiality and privacy (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**.**

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.

Health Catalyst states in the description of the Data Operating System (DOS), Interoperability Platform, Analytics, and Decision Support System that there are controls to ensure employee acknowledgements over acceptable use and code of conduct are made; to ensure there is a termination process that is followed when an employee is terminated; and to ensure new hires undergo a background check as part of the new hire process. Due to a lack of sufficient audit evidence, controls did not provide reasonable assurance that Health Catalyst's service commitments and system requirements were achieved based on criteria CC1.1 – *The entity demonstrates a commitment to integrity and ethical values* or CC2.2 – *The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.*

We assert, except for the matters described above, that the controls within the system were effective throughout the period June 1, 2021 to June 30, 2022, 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 Data Operating System (DOS), Interoperability Platform, Analytics, and Decision Support System (the "system") were effective throughout the period June 1, 2021 to June 30, 2022, 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, confidentiality, and privacy (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, Inc. uses Microsoft Azure for cloud hosting, Flexential for data center services for Health Catalyst Interoperability (HCI)-hosted clients, and Cognizant for staff augmentation 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.

Independent Service Auditor's Report (Continued)

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.

Service Auditor's Independence and Quality Control
We have complied with the independence and other ethical requirements of the Code of Professional Conduct established by the AICPA.

We applied the Statements on Quality Control Standards established by the AICPA and, accordingly, maintain a comprehensive system of quality control.

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.

Independent Service Auditor's Report (Continued)

Basis for Qualified Opinion
Health Catalyst states in its description of its Data Operating System (DOS), Interoperability Platform, Analytics, and Decision Support System that it has controls in place requiring employee acknowledgements over acceptable use and code of conduct; requiring there is a termination process that is followed when an employee is terminated; and requiring new hires undergo a background check as part of the new hire process. Due to a lack of sufficient audit evidence, controls did not provide reasonable assurance that Health Catalyst's service commitments and system requirements were achieved based on criteria CC1.1 – *The entity demonstrates a commitment to integrity and ethical values* or CC2.2 – *The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control*.

Opinion
In our opinion, except for the matters described above, management's assertion that the controls within Health Catalyst's Data Operating System (DOS), Interoperability Platform, Analytics, and Decision Support System were effective throughout the period June 1, 2021 to June 30, 2022, 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.

Restricted Use
This report, is intended solely for the information and use of Health Catalyst, user entities of Health Catalyst's Data Operating System (DOS), Interoperability Platform, Analytics, and Decision Support System during some or all of the period June 1, 2021 to June 30, 2022, business partners of Health Catalyst subject to risks arising from interactions with the Data Operating System (DOS), Interoperability Platform, Analytics, and Decision Support System, practitioners providing services to such user entities and business partners, prospective user entities and business partners, and regulators, all who have sufficient knowledge and understanding of the following:

- The nature of the service provided by the service organization
- How the service organization's system interacts with user entities, business partners, subservice organizations, and other parties as applicable
- Internal control and its limitations
- Complementary user entity controls and complementary subservice organization controls and how those controls interact with the controls at the service organization to achieve the service organization's service commitments and system requirements
- User entity responsibilities and how they may affect the user entity's ability to effectively use the service organization's services
- The applicable trust services criteria
- The risks that may threaten the achievement of the service organization's service commitments and system requirements and how controls address those risks
- This report does not contain the details of the specific controls in scope and tested which management has defined and provided responses for the criteria which were not met as mentioned above. To obtain those details, user entities are directed to request Health Catalyst Inc.'s SOC 2 Type 2 report for the Health Catalyst's Data Operating System (DOS), Interoperability Platform, Analytics, and Decision Support System

Independent Service Auditor's Report (Continued)

This report is not intended to be and should not be used by anyone other than these specified parties.

Wipfli LLP

Wipfli LLP

Philadelphia, Pennsylvania
October 3, 2022

Attachment A – Description of the Boundaries of Health Catalyst, Inc.'s Data Operating System (DOS), Interoperability Platform, Analytics, and Decision Support System

Attachment A – Description of the Boundaries of Health Catalyst, Inc.'s Data Operating System (DOS), Interoperability Platform, 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, Health Catalyst's Interoperability (HCI) division supports clients with non-DOS-based data sources and delivery. These services are defined and designed for clients' 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 agreements, 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.

Health Catalyst and Health Catalyst Interoperability (HCI) have achieved greater merging of team structures in which one core team maintains the infrastructure behind the client-facing application and services. In 2020, Health Catalyst acquired the MeasureAble, Healthfinch, and Vitalware business entities, and in 2022, it acquired both KPI Ninja and ARMUS. These acquired business entities are treated as business units or divisions. Healthfinch (now Embedded) and MeasureAble are a part of Health Catalyst's Population Health offering, which includes seven other products. The Vitalware business unit folds up under Health Catalyst's financial services business unit. KPI Ninja provides products similar to HCI that serve the health information exchange market within healthcare.

Attachment A – Description of the Boundaries of Health Catalyst, Inc.'s Data Operating System (DOS), Interoperability Platform, Analytics, and Decision Support System

Services Provided (Continued)

The organization has a single third party that was acquired by Health Catalyst which is provided access to specific clients' data. Health Catalyst DOS clients are configured to send data to MeasureAble, the third party that is provided access to client data. The MeasureAble service processes provided data and generates measures relevant to the data to allow for appropriate decision making and reporting. MeasureAble 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).

Components of the System Used to Provide the Services

Infrastructure and Software

Health Catalyst leverages Microsoft Azure for cloud-based infrastructure and services and Flexential's colocation facilities for HCI-hosted clients. 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.

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.

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.

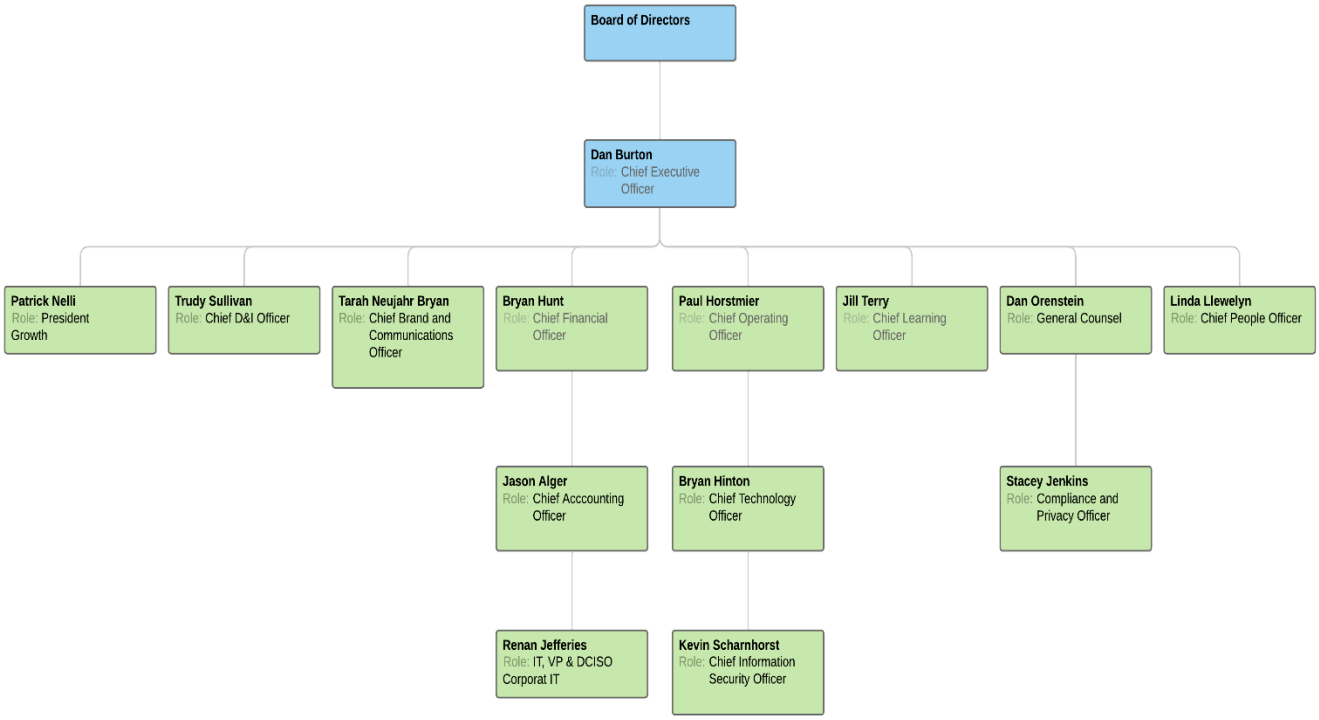
The organization maintains its software inventory through workstation management services that include Active Directory and production environments that use automatically updated deployment automation.

Attachment A – Description of the Boundaries of Health Catalyst, Inc.'s Data Operating System (DOS), Interoperability Platform, Analytics, and Decision Support System

Components of the System Used to Provide the Services (Continued)

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 company 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 all 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.

Attachment A – Description of the Boundaries of Health Catalyst, Inc.'s Data Operating System (DOS), Interoperability Platform, Analytics, and Decision Support System

Components of the System Used to Provide the Services (Continued)

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

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 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.

Attachment A – Description of the Boundaries of Health Catalyst, Inc.'s Data Operating System (DOS), Interoperability Platform, Analytics, and Decision Support System

Components of the System Used to Provide the Services (Continued)

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

Subservice Organizations

The Analytics and Interoperability platforms use subservice organizations to perform a range of functions. The following describes the subservice organizations used by the Analytics and Interoperability platforms:

Subservice Organization	Function
Microsoft Azure	Cloud-based infrastructure and services
Flexential	Colocation facilities
Cognizant	Staff augmentation services

Attachment A – Description of the Boundaries of Health Catalyst, Inc.'s Data Operating System (DOS), Interoperability Platform, Analytics, and Decision Support System

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. 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 transactions are secure, timely, 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 the authorization of disclosing personal information to Health Catalyst.
User organizations are responsible for reporting any identified security, availability, confidentiality and privacy incidents.

Attachment A – Description of the Boundaries of Health Catalyst, Inc.'s Data Operating System (DOS), Interoperability Platform, Analytics, and Decision Support System

Complementary Subservice Organization Controls

Health Catalyst's controls related to the Data Operating System (DOS), Interoperability Platform, Analytics, and Decision Support 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 Data Operating System (DOS), Interoperability Platform, Analytics, and Decision Support 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 organization(s) as described below.

Complementary Subservice Organization Controls
Subservice organizations are responsible for notifying Health Catalyst of security, availability, confidentiality and privacy incidents.
Logical access controls have been implemented at the data center 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 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 Health Catalyst, Inc.’s Data Operating System (DOS), Interoperability Platform, Analytics, and Decision Support System

Attachment B – Service Commitments and System Requirements of Health Catalyst, Inc.'s Data Operating System (DOS), Interoperability Platform, Analytics, and Decision Support System

Health Catalyst designs its processes and procedures related to its DOS, Interoperability Platform, Analytics, and Decision Support System to meet its objectives for the successful delivery of custom data analytics, decision support, and interoperability services solutions. Those objectives are based on the service commitments Health Catalyst makes to user entities, the laws and regulations that govern the provision of custom data analytics, decision support, and interoperability services solutions, 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. Availability commitments to user entities are not documented in the client agreements.

- Security commitments include principles within the fundamental designs of the custom data analytics, decision support, and interoperability services solutions 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 client data both at rest and in transit.

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 custom data analytics, decision support, and interoperability services solutions.

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.

Attachment B – Service Commitments and System Requirements of Health Catalyst, Inc.'s Data Operating System (DOS), Interoperability Platform, Analytics, and Decision Support System

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 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. 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.

Privacy Policy and Procedures

This privacy policy sets out how Health Catalyst uses and protects any information provided to Health Catalyst. Health Catalyst is committed to ensuring that privacy is protected. Information provided to Health Catalyst, for which users can be identified by, will be used in accordance with this privacy statement. Health Catalyst may change this policy from time to time by updating webpage that houses the policy. Users should check the webpage from time to time to ensure that you are happy with any changes. This policy is effective from 14th of December 2012.

Health Catalyst may collect the following information:

- Name and job title.
- Contact information including email address.
- Company and position in the company.
- Other information relevant to customer surveys.

Privacy Policy and Procedures (Continued)

Health Catalyst requires this information to understand user needs and to provide a better service, and in particular for the following reasons:

- Internal record keeping.
- Use the information to improve products and services.
- Health Catalyst may periodically send promotional emails about new products, special offers or other information which using the email address which users have provided.
- From time to time, Health Catalyst may also use user information to contact individuals for market research purposes. Contact could be through email, phone, fax or mail. Additionally, Health Catalyst may use the information to customize the website according to user's interests.

Security

Health Catalyst is committed to ensuring that user information is secure. In order to prevent unauthorized access or disclosure, physical, electronic and managerial procedures have been put in place to safeguard and secure the information collected online.

How Cookies are Used

A cookie is a small file which asks permission to be placed on a user's computer's hard drive. Once the user agrees, the file is added and the cookie helps analyze web traffic or lets users know when they visit a particular site. Cookies allow web applications to respond to users as an individual. The web application can tailor its operations to user needs, likes and dislikes by gathering and remembering information about their preferences. Health Catalyst use traffic log cookies to identify which pages are being used. This helps Health Catalyst analyze data about webpage traffic and improve the website in order to tailor it to customer needs. Health Catalyst only use this information for statistical analysis purposes and then the data is removed from the system. Overall, cookies help Health Catalyst provide users with a better website, by enabling Health Catalyst to monitor which pages users find useful or not useful. A cookie in no way gives Health Catalyst access to user's computers or any information about the user, other than the data users choose to share with Health Catalyst. Users can choose to accept or decline cookies. Most web browsers automatically accept cookies, but users can usually modify browser setting to decline cookies if preferred. This may prevent users from taking full advantage of the website. Health Catalyst also use Google Analytics, including its remarketing and cross-device functionality.

Links to Other Websites

Health Catalyst's website may contain links to other websites of interest. However, once users have used these links to leave the Health Catalyst site, users should note that Health Catalyst does not have any control over other websites. Therefore, Health Catalyst cannot be responsible for the protection and privacy of any information which users provide whilst visiting such sites and such sites are not governed by this privacy statement. Users should exercise caution and look at the privacy statement applicable to the website in question.

Privacy Policy and Procedures (Continued)

Controlling Your Personal Information

Users may choose to restrict the collection or use of personal information in the following ways:

- Whenever users are asked to fill in a form on the website, they should look for the box that users can click to indicate that they do not want the information to be used by anybody for direct marketing purposes.
- If users have previously agreed to Health Catalyst using their personal information for direct marketing purposes, users may change their mind at any time by writing to Health Catalyst.

Health Catalyst will not sell, distribute, or lease personal information to third parties unless Health Catalyst has user permission or are required by law to do so. Health Catalyst may use personal information to send users promotional information about third parties which Health Catalyst think users may find interesting if users wish this to happen. Users may request details of personal information which Health Catalyst hold about users under the Data Protection Act 1998.