Vitalware, LLC
Owned by Health Catalyst, Inc.
South Jordan, Utah

System and Organization Controls Report
Relevant to Mid-Revenue Cycle Software-as-a-Service System

SOC 3® Report

June 1, 2021 to May 31, 2022

WIPFLI

SOC 3® is a registered trademark of the American Institute of Certified Public Accountants.

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.

Vitalware, LLC

SOC 3 Report

June 1, 2021 to May 31, 2022

Table of Contents

Section 1
Vitalware, LLC's Assertion

Vitalware LLC's Assertion

We are responsible for designing, implementing, operating, and maintaining effective controls within Vitalware LLC's ("Vitalware") Mid-Revenue Cycle Software-as-a-Service System (the "system") throughout the period June 1, 2021 to May 31, 2022, to provide reasonable assurance that Vitalware'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, 2021 to May 31, 2022, to provide reasonable assurance that Vitalware'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*). Vitalware'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.

We assert that the controls within the system were effective throughout the period June 1, 2021 to May 31, 2022, to provide reasonable assurance that Vitalware'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 Vitalware, LLC
South Jordan, Utah

Scope
We have examined Vitalware, LLC's (Vitalware) accompanying assertion titled "Vitalware, LLC's Assertion" (the "assertion") that the controls within Vitalware's Mid-Revenue Cycle Software-as-a-Service System (the "system") were effective throughout the period June 1, 2021 to May 31, 2022, to provide reasonable assurance that Vitalware'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*).

Service Organization's Responsibilities
Vitalware 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 Vitalware's service commitments and system requirements were achieved. Vitalware has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, Vitalware 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 Vitalware'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 Vitalware'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.

WIPFLI

Independent Service Auditor's Report (Continued)

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 Vitalware's Mid-Revenue Cycle Software-as-a-Service System were effective throughout the period June 1, 2021 to May 31, 2022, to provide reasonable assurance that Vitalware'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
July 11, 2022

Attachment A – Description of the Boundaries of Vitalware LLC's Mid-Revenue Cycle Software-as-a-Service System

Attachment A – Description of the Boundaries of Vitalware's Mid-Revenue Cycle Software-as-a-Service System

Services Provided

Vitalware, LLC ("Vitalware by Health Catalyst" or "Vitalware") provides mid-revenue cycle management solutions, data and consulting services, and expert consulting for health systems, hospitals, physicians, and healthcare revenue cycle solutions providers. The organization's mid-revenue cycle solutions scale supports hospitals of all sizes. It also drives positive financial outcomes that protect reimbursement and reputation with an accurate chargemaster and help financial professionals discover and capture missing revenue.

The organization was acquired by Health Catalyst, Inc. in 2020 and remains a dedicated business unit under the organizational structure that makes up the larger enterprise. The combined people, process, and technology were evaluated and assessed under the scope as hereto explained.

The systems supporting the services are all housed in the United States. Systems are physically housed in TierPoint colocation facilities in Seattle and Dallas. Additional support and development staff are in Uruguay.

Client access to systems is facilitated through Internet Protocol Security (IPsec) virtual private network (VPN) tunnels, IP-whitelisted File Transfer Protocol (FTP), Hypertext Transfer Protocol (HTTP), and generally available web-based applications. Clients sign agreements for services, including a Master Services Agreement (MSA), Business Associates Agreements (BAA), and an order form outlining general and specific delivery requirements. Agreements outline general security, confidentiality, and compliance commitments. Client service and account management teams work with clients during the onboarding process to define appropriate services to provide specifications for data inflows and outflows from the system. In addition, Vitalware has professional services that are available in some business lines to provide additional onboarding and ongoing services to assist clients in implementing and operating the systems provided.

Descriptions of the various service applications and support services are described in more detail in the following sections.

VitalKnowledge™

VitalKnowledge provides clients with a single source for advanced coding, regulatory, and reimbursement resources. VitalKnowledge maintains reference information related to revenue management. Vitalware provides users, including compliance, revenue cycle, and coding teams, with timely, automatic updates on comprehensive and current regulatory and financial information that is critical to achieving accurate, compliant coding and reimbursement.

VitalCDM™

VitalCDM was designed to improve visibility into clients' chargemasters for healthcare-related services and supplies and increase staff productivity. It includes functionality for daily workflow and reporting with corporate standardization and provides detailed insights into issues to decrease compliance risk, increase efficiency, and help ensure appropriate reimbursement.

Confidential and proprietary to Vitalware, LLC and Wipfli LLP
Not to be reproduced without permission

Attachment A – Description of the Boundaries of Vitalware's Mid-Revenue Cycle Software-as-a-Service System

Services Provided (Continued)

Charge Capture

Charge Capture was designed to address pre- and post-billing reviews to identify errors and provide improvement opportunities.

Price Transparency

Price Transparency publishes regulatory required pricing information based on the organization's standard charges.

Components of the System Used to Provide the Services

Infrastructure

Vitalware maintains a network diagram that showcases the organization's technical infrastructure and critical network infrastructure. The network diagram is reviewed, updated, and approved by the IT staff annually or when changes are made. Sensitive systems are isolated from other systems using virtual local area networks (VLANs) and firewalls that segment VLANs.

The organization's Information Security Management System (ISMS) Policy addresses how Vitalware maintains an inventory of systems automatically by system management software.

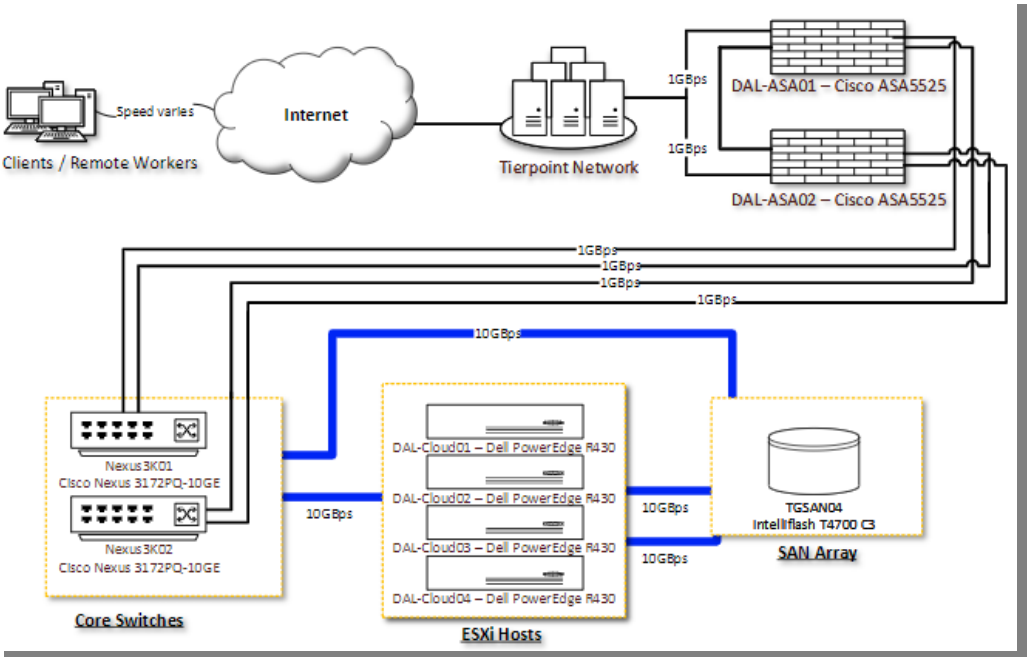


Figure 1: Vitalware's Dallas Network Architecture Diagram

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

Infrastructure (Continued)

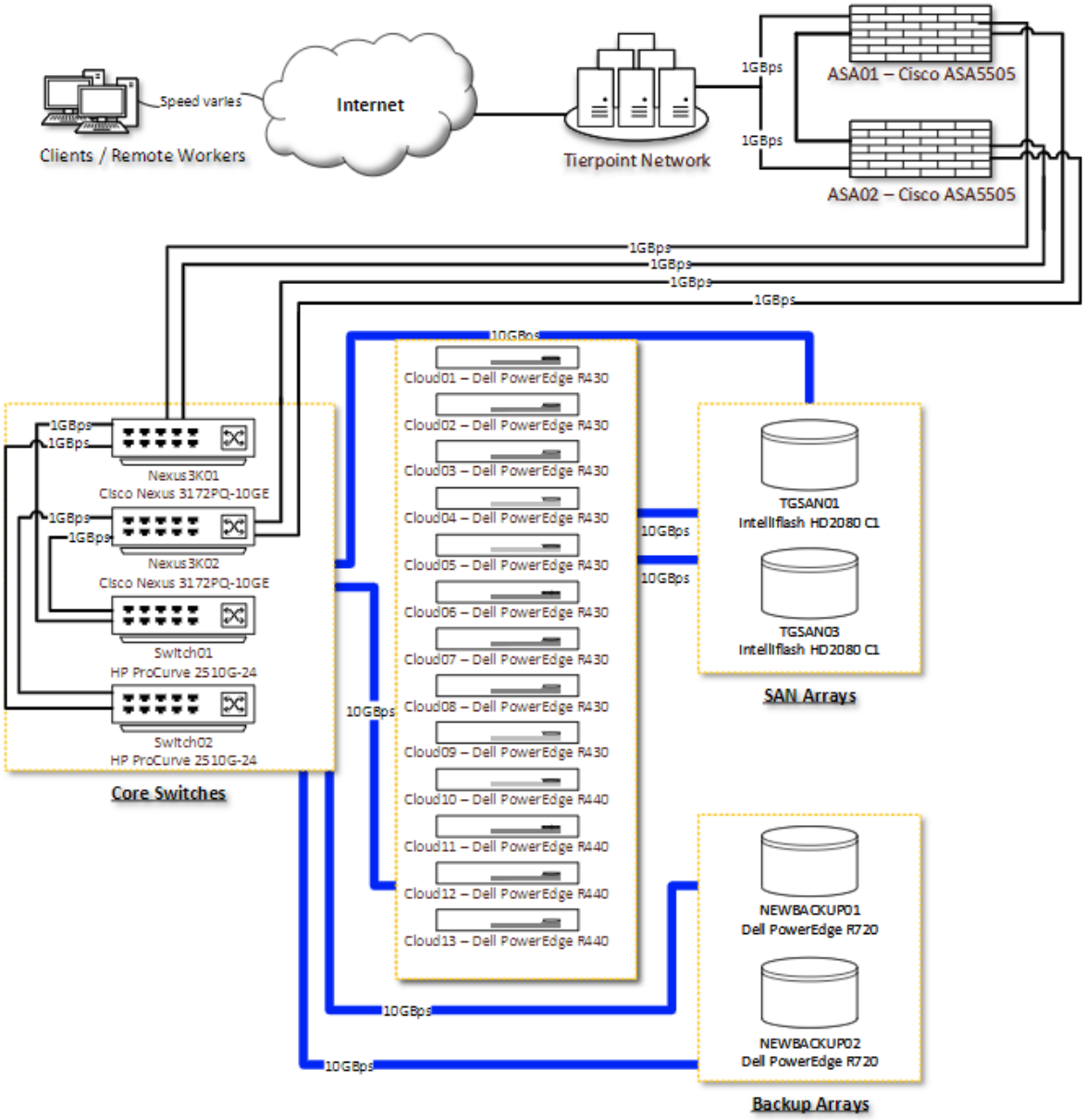


Figure 2: Vitalware's Seattle Network Architecture Diagram

Attachment A – Description of the Boundaries of Vitalware's Mid-Revenue Cycle Software-as-a-Service System

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

Software

Vitalware maintains a complete inventory of the software used to support the operation of its technical infrastructure and day-to-day operations activities. The inventory records the name, version, vendor, and function and is maintained manually with information available from workstation management software and production environment configuration management. Vitalware's software service providers include the following:

- ADAudit Plus
- App Orchard
- Axure RP Pro
- Azure DevOps Artifacts
- Azure DevOps Dashboards
- Azure DevOps Environments
- Azure DevOps Pipelines
- Azure DevOps Repositories
- Azure DevOps Retrospectives
- Azure DevOps Wiki
- Azure KeyVault
- Azure Application Insights
- Azure Storage Accounts
- ColdFusion
- Confluence
- CrowdStrike
- EF Plan Enterprise
- Elasticsearch
- Ext JS Premium Maintenance and Support
- Flare
- GitLab
- Insight
- Jira Service Desk
- Jira Software
- Kendo UI
- Kibana
- Mashery
- MongoDB
- MS Visual Studio
- MS Visual StudioCode
- Netwrix
- NextGen Connect
- Octopus Deploy
- Pingdom
- Postman Pro
- Salesforce
- Slack
- Smartsheet
- Sophos
- SQL Compare Professional/SQLData Compare
- SQL Server
- TeamCity
- TestRail
- TrackVia
- TruCode
- Ubuntu 20.04
- Udemy EnterprisePlan
- Veeam
- VMware
- Windows Server 2019
- ZixMail
- Zoom

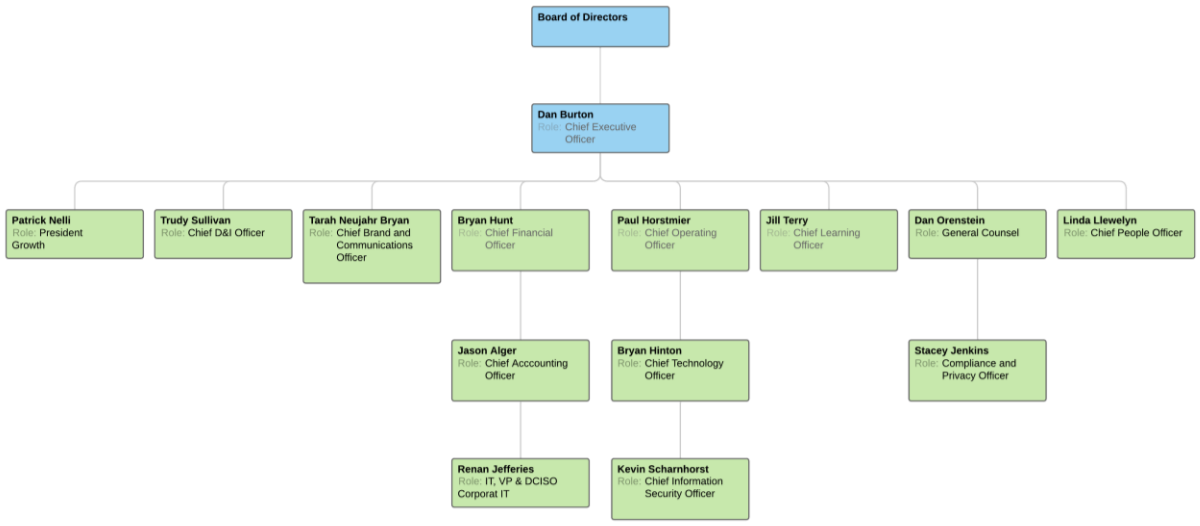
People

Vitalware maintains an organizational chart that shows divisions operating under executive leadership, with executive leadership reporting to the Chief Executive Officer (CEO). Vitalware's organizational chart addresses the organization's traditional hierarchy structure and the relationship between executive management and information security oversight through the Chief Information Security Officer (CISO). The organization is built on a framework of senior executive leadership, executive leadership, management, departments, and employees.

Confidential and proprietary to Vitalware, LLC and Wipfli LLP
Not to be reproduced without permission

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

People (Continued)



Vitalware's operation team reports to the same division as the Data Operating System team, and all other service teams report to different divisional leadership based on the alignment of the service with the organization's strategic vision. The Security team, led by the CISO, oversees the security and compliance efforts for all product lines.

Vitalware acts as a financial services business unit of Health Catalyst, Inc. Health Catalyst, Inc. is publicly traded (symbol: HCAT), and its board of directors consists of appointed members who are responsible for the direction of the organization and have final decision-making authority. Members of the Board of Directors are kept informed about information security controls and issues.

Data

The organization identifies and classifies data captured by Vitalware as either confidential, internal, or public. Vitalware's data is primarily healthcare related and includes electronic protected health information (ePHI), and client activities related to its data include the following:

- Data entry and uploading
- Data analytics
- Data exchange with client-side systems
- Data reporting and extracts, including application programming interface and secure file transfer delivery

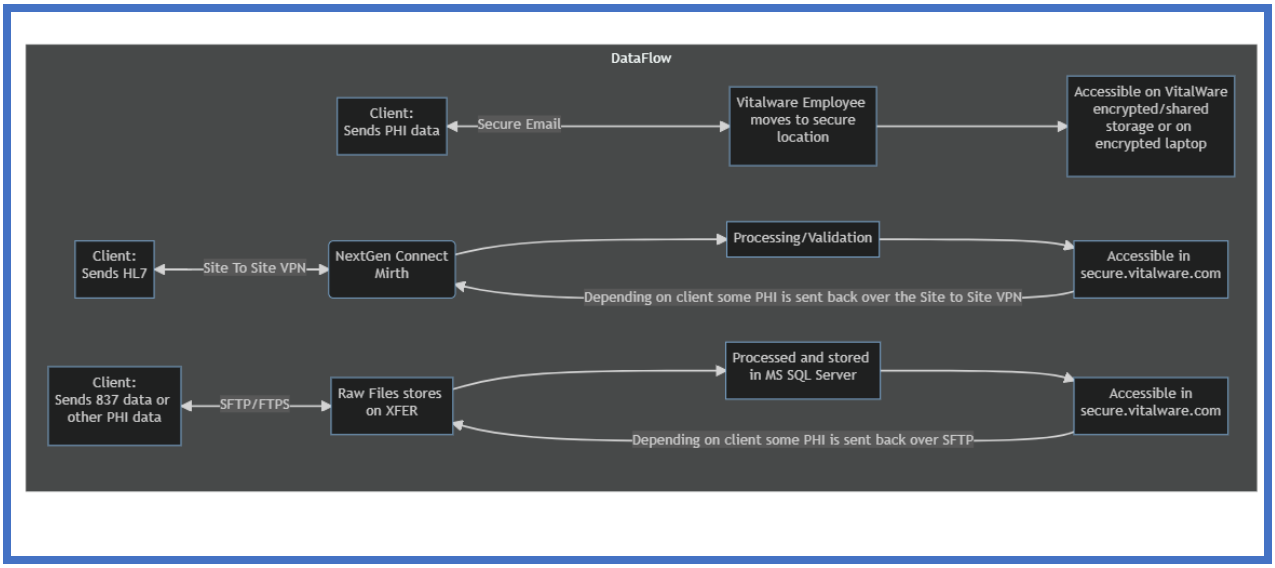
The organization identifies data flows and handles data in compliance with Vitalware's data classification policies and general best practices.

Confidential and proprietary to Vitalware, LLC and Wipfli LLP
Not to be reproduced without permission

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

Data (Continued)

Vitalware's Data Flow Diagram shows how data enters and leaves the control of the organization and includes Health Level Seven (HL7) exchange files, other data files via Secure Shell (SSH) FTP, and data inbound via secure email. Data processing results in data outputs of file exchanges and user interfaces in Vitalware's web applications.



The organization classifies data to determine data-handling parameters, including retention and storage requirements. In addition, Vitalware stores, processes, and transmits data related to protected health information (PHI) and is subject to HIPAA compliance as a Business Associate. Client commitments are documented in contracts and addressed by implementing appropriate data security and retention controls.

The organization maintains encryption for sensitive data across public and untrusted networks. Encryption is the primary means of data integrity protection in transit. Vitalware's data transmission is limited to HTTPS, Secure Shell Protocol (SSH), and VPN. Data access methods use only encrypted protocols. The organization implements encryption strengths of Advanced Encryption Standard (AES) 128 for transmission and AES 256 for storage.

Confidential and proprietary to Vitalware, LLC and Wipfli LLP
Not to be reproduced without permission

Attachment A – Description of the Boundaries of Vitalware LLC's Mid-Revenue Cycle Software-as-a-Service 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

Vitalware by Health Catalyst uses subservice organizations to perform a range of functions. The following describes the subservice organizations used by Health Catalyst:

Subservice Organization	Function
TierPoint	Colocation facilities

Complementary User Entity Control Considerations

Vitalware 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 Vitalware 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 Vitalware'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 Vitalware.
User organizations practice removal of user accounts for any users who have been terminated and were previously involved in material functions or activities associated with Vitalware's services.

Complementary User Entity Control Considerations (Continued)

Complementary User Entity Controls
Transactions for user organizations relating to Vitalware's services are appropriately authorized, and transactions are secure, timely, and complete.
For user organizations sending data to Vitalware, data is protected by appropriate methods to ensure confidentiality, privacy, integrity, availability, and nonrepudiation.
User organizations implement controls requiring additional approval procedures forcritical transactions relating to Vitalware's services.
User organizations report to Vitalware in a timely manner any material changes to their overall control environment that may adversely affect services being performed by Vitalware.
User organizations notify Vitalware in a timely manner of any changes to personnel directly involved with services performed by Vitalware. These personnel may be involved in financial, technical, or ancillary administrative functions directly associated with services provided by Vitalware.
User organizations adhere to the terms and conditions stated in their contracts with Vitalware.
User organizations develop and, if necessary, implementing a business continuity and disaster recovery plan (BCDRP) that will aid in the continuation of services provided by Vitalware.

Complementary Subservice Organization Controls

Vitalware's controls related to the Mid-Revenue Software-as-a-Service System cover only a portion of overall internal control for each user entity of Vitalware. It is not feasible for the trust services criteria related to Mid-Revenue Software-as-a-Service System to be achieved solely by Vitalware. Therefore, each user entity's internal control must be evaluated in conjunction with Vitalware'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
Security and availability incidents are provided to guide users in identifying and reporting failures, incidents, concerns, and other complaints.
Logical access controls have been implemented at the data center through firewalls, network security and monitoring tool security.
Video surveillance cameras are used to monitor data center facilities.
Badge usage in the company's facility is tracked for audit purposes.
Visitors are required to sign in on a log at the front desk upon entry to the building.
Entrances and restricted areas are monitored by security cameras, and footage is retained for at least 90 amount of days.

Confidential and proprietary to Vitalware, LLC and Wipfli LLP
Not to be reproduced without permission

Complementary Subservice Organization Controls (Continued)

Complementary Subservice Organization Controls
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.

Attachment B – Service Commitments and System Requirements of Vitalware LLC's Mid-Revenue Cycle Software-as-a-Service System

Attachment B – Service Commitments and System Requirements of Vitalware LLC's Mid-Revenue Cycle Software-as-a-Service System

Vitalware designs its processes and procedures related to the Mid-Revenue Cycle Software-as-a-Service System to meet its objectives for the successful delivery of the Mid-Revenue Cycle Software-as-a-Service System. Those objectives are based on the service commitments Vitalware makes to user entities, the laws and regulations that govern the provision of mid-revenue cycle management services, and the financial, operational, and compliance requirements Vitalware has established for the services. The mid-revenue cycle software-as-a-service system of Vitalware is subject to the security and privacy requirements of the Health Insurance Portability and Accountability Act (HIPAA), as well as state privacy security laws and regulations in the jurisdictions in which Vitalware 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 Mid-Revenue Cycle Software-as-a-Service 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 client data both at rest and in transit.

Vitalware 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 which Vitalware's procedures and system design documentation align with and contracts with clients are bound to. 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 Mid-Revenue Cycle Software-as-a-Service System.

Regulatory Commitments

Due to the type of data Vitalware collects, stores, processes, and transmits, the organization is primarily impacted by HIPAA and strives to maintain security control programs commensurate with those accepted by the healthcare industry. A combination of control design and implementation, compliance and security oversight, contractual safeguards, and technologies are used to support compliance with HIPAA and industry standards. Reviews of the organization's regulatory compliance is completed through HITRUST certification and annual compliance reviews.

Contractual Commitments

Vitalware commits to reasonable efforts for availability and uptime, using contractual materials to define its service commitments to clients. Contractual materials are tailored to individual client needs but generally include sections on software licensing and details on selected consultation services.

SLAs vary by client contract, but the organization promises clients an average of 99.5% uptime outside scheduled maintenance, commits service levels for uptime, and monitors service delivery. Vitalware employees engage constantly and operate a small call center to support after-hours calls and alert staff of outages. The organization's colocation centers provide a reliable physical environment for the servers to operate.

Attachment B – Service Commitments and System Requirements of Vitalware's Mid-Revenue Cycle Software-as-a-Service System

System Design

Vitalware designs its Mid-Revenue Cycle Software-as-a-Service System to meet its regulatory and contractual commitments. These commitments are based on the services that Vitalware provides to its clients, the laws and regulations that govern the provision of those services, and the financial, operational, and compliance requirements that Vitalware has established for its services. Vitalware establishes operational requirements in its system design that support the achievement of its regulatory and contractual commitments. These requirements are communicated in Vitalware's system policies and procedures, system design documentation, and contracts with clients.