Chase Data Corp
Type 1 SOC 2 with HIPAA/HITECH
2021

REPORT ON CHASE DATA CORP'S DESCRIPTION OF ITS SYSTEM AND ON THE SUITABILITY OF THE DESIGN OF ITS CONTROLS RELEVANT TO SECURITY WITH HIPAA/HITECH REQUIREMENTS

Pursuant to Reporting on System and Organization Controls 2 (SOC 2)
Type 1 examination performed under AT-C 105 and AT-C 205

May 31, 2021

Table of Contents

SECTION 1

ASSERTION OF CHASE DATA CORP MANAGEMENT

ASSERTION OF CHASE DATA CORP MANAGEMENT

June 15, 2021

We have prepared the accompanying description of Chase Data Corp's ('Chase Data' or 'the Company') Call Center Software Services System titled "Chase Data Corp's Description of Its Call Center Software Services System as of May 31, 2021" (description) based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (AICPA, *Description Criteria*), (description criteria). The description is intended to provide report users with information about the Call Center Software Services System that may be useful when assessing the risks arising from interactions with Chase Data's system, particularly information about system controls that Chase Data has designed, implemented, and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to Security (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*) and essential elements of the Health Insurance Portability and Accountability Act Security Rule of 2003 ("HIPAA") and the Health Information Technology for Economic and Clinical Health Act ("HITECH"), enacted as part of the American Recovery and Reinvestment Act of 2009.

Chase Data uses Google Cloud and OVHcloud ('Google Cloud' and 'OVH' or 'subservice organizations') to provide data center hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Chase Data, to achieve Chase Data's service commitments and system requirements based on the applicable trust services criteria and HIPAA/HITECH requirements. The description presents Chase Data's controls, the applicable trust services criteria and HIPAA/HITECH requirements, and the types of complementary subservice organization controls assumed in the design of Chase Data'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 are necessary, along with controls at Chase Data, to achieve Chase Data's service commitments and system requirements based on the applicable trust services criteria and HIPAA/HITECH requirements. The description presents Chase Data's controls, the applicable trust services criteria and HIPAA/HITECH requirements, and the complementary user entity controls assumed in the design of Chase Data's controls.

We confirm, to the best of our knowledge and belief, that:

a. the description presents Chase Data's Call Center Software Services System that was designed and implemented as of May 31, 2021, in accordance with the description criteria.
b. the controls stated in the description were suitably designed as of May 31, 2021, to provide reasonable assurance that Chase Data's service commitments and system requirements would be achieved based on the applicable trust services criteria and HIPAA/HITECH requirements, if its controls operated effectively as of that date, and if the subservice organization and user entities applied the complementary controls assumed in the design of Chase Data's controls as of that date.

Ahmed A. Macklai
Chief Executive Officer
Chase Data Corp

SECTION 2

INDEPENDENT SERVICE AUDITOR'S REPORT

INDEPENDENT SERVICE AUDITOR'S REPORT

To: Chase Data Corp

Scope

We have examined Chase Data's accompanying description of its Call Center Software Services System titled "Chase Data Corp's Description of Its Call Center Software Services System as of May 31, 2021" (description) based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (AICPA, *Description Criteria*), (description criteria) and the suitability of the design of controls stated in the description as of May 31, 2021, to provide reasonable assurance that Chase Data's service commitments and system requirements were achieved based on the trust services criteria relevant to Security (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*). We have also examined the suitability of the design of controls to meet essential elements of the Health Insurance Portability and Accountability Act Security Rule of 2003 ("HIPAA") and the Health Information Technology for Economic and Clinical Health Act ("HITECH"), enacted as part of the American Recovery and Reinvestment Act of 2009.

Chase Data uses Google Cloud and OVH to provide data center hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Chase Data, to achieve Chase Data's service commitments and system requirements based on the applicable trust services criteria and HIPAA/HITECH requirements. The description presents Chase Data's controls, the applicable trust services criteria and HIPAA/HITECH requirements, and the types of complementary subservice organization controls assumed in the design of Chase Data's controls. The description does not disclose the actual controls at the subservice organizations. Our examination did not include the services provided by 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 controls at Chase Data, to achieve Chase Data's service commitments and system requirements based on the applicable trust services criteria and HIPAA/HITECH requirements. The description presents Chase Data's controls, the applicable trust services criteria and HIPAA/HITECH requirements, and the complementary user entity controls assumed in the design of Chase Data's controls. Our examination did not include such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such controls.

Service Organization's Responsibilities

Chase Data 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 Chase Data's service commitments and system requirements were achieved. Chase Data has provided the accompanying assertion titled "Assertion of Chase Data Corp Management" (assertion) about the description and the suitability of the design of controls stated therein. Chase Data is also responsible for preparing the description and assertion, including the completeness, accuracy, and method of presentation of the description and assertion; providing the services covered by the description; selecting the applicable trust services criteria and HIPAA/HITECH requirements and stating the related controls in the description; and identifying the risks that threaten the achievement of the service organization's service commitments and system requirements.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the description and on the suitability of design of controls stated in the description based on our examination. 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, in all material respects, the description is presented in accordance with the description criteria and the controls stated therein were suitably designed to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria and HIPAA/HITECH requirements. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

An examination of the description of a service organization's system and the suitability of the design of controls involves the following:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements
- Assessing the risks that the description is not presented in accordance with the description criteria and that controls were not suitably designed
- Performing procedures to obtain evidence about whether the description is presented in accordance with the description criteria
- Performing procedures to obtain evidence about whether controls stated in the description were suitably designed to provide reasonable assurance that the service organization achieved its service commitments and system requirements based the applicable trust services criteria and HIPAA/HITECH requirements
- Evaluating the overall presentation of the description

Our examination also included performing such other procedures as we considered necessary in the circumstances.

Inherent Limitations

The description is prepared to meet the common needs of a broad range of report users and may not, therefore, include every aspect of the system that individual report users may consider important to meet their informational needs.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. The projection to the future of any conclusions about the suitability of the design 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.

Other Matter

We did not perform any procedures regarding the operating effectiveness of controls stated in the description and, accordingly, do not express an opinion thereon.

Opinion

In our opinion, in all material respects:

a. the description presents Chase Data's Call Center Software Services System that was designed and implemented as of May 31, 2021, in accordance with the description criteria.
b. the controls stated in the description were suitably designed as of May 31, 2021, to provide reasonable assurance that Chase Data's service commitments and system requirements would be achieved based on the applicable trust services criteria and HIPAA/HITECH requirements, if its controls operated effectively as of that date and if the subservice organization and user entities applied the complementary controls assumed in the design of Chase Data's controls as of that date.

Restricted Use

This report is intended solely for the information and use of Chase Data, user entities of Chase Data's Call Center Software Services System as of May 31, 2021, business partners of Chase Data subject to risks arising from interactions with the Call Center Software Services System, practitioners providing services to such user entities and business partners, prospective user entities and business partners, and regulators 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
- 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 and HIPAA/HITECH requirements
- 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 is not intended to be, and should not be, used by anyone other than these specified parties.

A-LIGN ASSURANCE

Tampa, Florida
June 15, 2021

SECTION 3

CHASE DATA CORP'S DESCRIPTION OF ITS CALL CENTER SOFTWARE SERVICES SYSTEM AS OF MAY 31, 2021

OVERVIEW OF OPERATIONS

Company Background

Chase Data was founded in 1996. The company born out of a necessity to deliver powerful predictive dialing software that runs securely on Windows desktop computers. This organization is based in Plantation, Florida.

Chase Data makes software that helps call centers succeed. Chase Data's call center software platform empowers thousands of call centers around the world from startups and entrepreneurs to large publicly traded companies connect one conversation at a time with the people they serve.

Description of Services Provided

Chase Data's core application, Contact Center as a Service (CCaaS), is a multiuser, transaction-based application suite that enables the processing and delivery of high volume, interpersonal telephonic/voice services for call centers. The CCaaS software enables the following features:

- Enabling high volume outbound calling to call center business units, business to consumer organizations, Business Processing Outsourcers (BPOs), and governments entities
- Enabling the efficient routing of inbound calls to call center agents
- Providing full chain of custody tracking on telephone calls received and initiated (ex. Total talk time, agent handling call, dispositions, etc.)
- Managing secure integration of voice services with back office, legacy, proprietary web-based and third-party software in application
- Managing post call processes (ex. Scheduled call backs, etc.)
- Providing operational, management, and ad hoc reports
- Providing data reporting in a variety of formats

Principal Service Commitments and System Requirements

Chase Data designs its processes and procedures to meet its objectives for the services that are provided to clients. Those objectives are based on the service commitments that Chase Data makes to user entities, and the financial, operational, and compliance requirements that Chase Data has established for the services.

Commitments to user entities are documented and communicated in Service Level Agreements (SLAs) and other customer agreements, as well as in the description of the service offering provided online. Security commitments are standardized and include, but are not limited to, the following:

Security principles are designed to permit system users to access the information they need based on their role in the system while restricting them from accessing information not needed for their role. The employees use secure Chase Data provided workstations for providing the required support. Use of encryption technologies to protect customer data both at rest and in transit are built into the system.

Chase Data establishes operational requirements that support the achievement of security commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in Chase Data system policies and procedures, and contracts with customers. Information security policies define an organization-wide approach to how systems and data are protected. These include policies around how the service is designed and developed, how the system is operated, how the internal business systems and networks are managed and how 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 in the operation of servicing the clients.

Components of the System

Infrastructure

Primary infrastructure used to support Chase Data's Call Center Software Services System includes the following:

Primary Infrastructure		
Hardware	**Type**	**Purpose**
Desktop Computer	Dell and HP	Office workstations
Firewall	Cisco Meraki MX67	Network security appliance used at the office

Software

Primary software used to provide Chase Data's Call Center Software Services System includes the following:

Primary Software		
Software	**Operating System**	**Purpose**
Google Suite (G-Suite)	Web Based	E-mails, document storage, monitoring
Zoho Desk	Web Based	Ticketing System for new hires/incidents etc.
Google Drive	Web Based	Repository for policies and procedures.
HubSpot	Web Based	For tracking Sales cycle
Microsoft Office Package	Windows	For performing day to day operations
JumpCloud	Web Based	SSO, cloud LDAP, SaaS RADIUS, GPO-like policies

People

Chase Data has a staff of approximately 17 employees organized in the following functional areas:

- Corporate. Executives, senior client services staff, and company administrative support staff, such as finance, human resources, and Internal Operations. These individuals use different tools like salesforce etc. to conduct business at an overall corporate level
- Operations/Support. Staff that provide the direct day-to-day services to the clients are stationed at the Chase Data facilities to fulfill the contractual obligations and delivery technical support to clients
- Software Development. Staff that develop, test and deploy Chase Data software

Data

Data is defined as information within databases residing in Chase Data's system infrastructure and used to drive Chase Data's software. This data is stored in encrypted databases which are backed up routinely. The data would include standard CDR (Call Data Records) detailing time/date stamped call attempts, machine response codes, user selected disposition codes, time/date/agents, and assigned call back schedules.

Processes, Policies and Procedures

Formal IT policies and procedures exist that describe physical security, logical access, computer operations, change control, and data communication standards. Teams are expected to adhere to the Chase Data policies and procedures that define how services should be delivered. These are located on the Company's Confluence pages and can be accessed by any Chase Data team member.

Physical Security

The in-scope system and supporting infrastructure is hosted by Google Cloud and OVH. As such, Google Cloud and OVH are responsible for the physical security controls for the in-scope system.

Logical Access

Upon hire, employees are assigned to a position in the Automatic Data Processing Human Resources (ADP HR) management system. Two days prior to the employees' start date, an employee user IDs to be created and access to be granted. The G-Suite admin creates a Chase Data e-mail id and grants the Google Drive access policies page access. On a frequent basis, access is reviewed, and termination or access rule changes are performed.

Chase Data Sysadmin assigns a workstation to an employee where a user account is created, and the user is restricted from installing any software and if there is a need for a software it has to be installed by the Sysadmin after determining the software need and in compliance with Chase Data policies.

Assets are tracked using an asset inventory tracker. The Sysadmin is responsible for installing any additional software.

Computer Operations - Backups

Data is stored at the Google Cloud and OVH facilities and backups are handled by Chase Data and no special backup requirements are needed. The backups stored by Google Cloud and OVH are the backups of Chase Data's databases and those backups are encrypted. Database data is composed of call data records used by their system. Chase Data does not store or handle "customer data" defined as locally accessible data sources on the customers' workstations, servers, or proprietary local network accessed data sources at the customer's location.

Computer Operations - Availability

Incident response policies and procedures are in place to guide personnel in reporting and responding to information technology incidents. Procedures exist to identify, report, and act upon system security breaches and other incidents. Incident response procedures are in place to identify and respond to incidents on the network.

Chase Data has implemented a patch management process to ensure infrastructure systems are patched in accordance with vendor recommended operating system patches. Chase Data Sysadmin review proposed operating system patches to determine whether the patches need to be applied. Chase Data Sysadmin is responsible for determining the risk of applying or not applying patches based upon the security and availability impact of those systems. Sysadmin raises a Change request and follow thru the approval process, and once approved notify affected parties and validate that patches have been installed, and if applicable that reboots have been completed.

Change Control

Chase Data maintains policies and procedures to guide personnel in documenting and implementing application and infrastructure changes. Change control procedures include change request and initiation processes, documentation requirements, and required approval procedures.

The Favro system is utilized to document the change control procedures for changes in the application and implementation of new changes. Testing results are documented and maintained with the associated change request. Development and testing are performed in an environment that is logically separated from the production environment (If possible). Management approves changes prior to migration to the production environment and documents those approvals within the ticketing system.

Chase Data has implemented a patch management process to ensure infrastructure systems are patched in accordance with vendor recommended operating system patches. Chase Data Sysadmin review proposed operating system patches to determine whether the patches are applied. Chase Data Sysadmin is responsible for determining the risk of applying or not applying patches based upon the security and availability impact of those systems. Sysadmin raises a Change request and follow thru the approval process, and once approved notify affected parties and validate that patches have been installed, and if applicable that reboots have been completed.

Data Communications

Authorized employees may access the Internet using wired Local Area Network (LAN) technology. There are no Wi-Fi networks present.

Firewall systems are in place to filter unauthorized inbound network traffic from the Internet and deny any type of network connection that is not explicitly authorized. Network address translation (NAT) functionality is utilized to manage internal IP addresses. Administrative access to the firewall is restricted to authorized employees.

Redundancy is built into the system infrastructure supporting the Google Cloud and OVH data center services to help ensure that there is no single point of failure that includes firewalls, routers, and servers. In the event that a primary system fails, the redundant hardware is configured to take its place.

Penetration testing is conducted to measure the security posture of a target system or environment. Chase Data uses an accepted industry standard penetration testing methodology specified by OpenVAS standards. Chase Data's approach begins with a vulnerability analysis of the target system to determine what vulnerabilities exist on the system that can be exploited via a penetration test, simulating a disgruntled/disaffected insider or an attacker that has obtained internal access to the network. Once vulnerabilities are identified, the third-party vendor attempts to exploit the vulnerabilities to determine whether unauthorized access or other malicious activity is possible. Penetration testing includes network and application layer testing as well as testing of controls and processes around the networks and applications.

Vulnerability scanning is performed by a third-party vendor on a weekly basis in accordance with Chase Data's anti-virus, malware, and vulnerability scanning policy. The third-party vendor uses industry standard scanning technologies and a formal methodology specified by OpenVAS. These technologies are customized to test the organization's infrastructure and software in an efficient manner while minimizing the potential risks

Boundaries of the System

The scope of this report includes the Chase Data's Call Center Software Services System performed in the Plantation, Florida facility.

This report does not include the data center hosting services provided by Google Cloud and OVH at the respective facilities.

RELEVANT ASPECTS OF THE CONTROL ENVIRONMENT, RISK ASSESSMENT PROCESS, INFORMATION AND COMMUNICATION, AND MONITORING

Control Environment

Integrity and Ethical Values

The effectiveness of controls cannot rise above the integrity and ethical values of the people who create, administer, and monitor them. Integrity and ethical values are essential elements of Chase Data's control environment, affecting the design, administration, and monitoring of other components. Integrity and ethical behavior are the product of Chase Data's ethical and behavioral standards, how they are communicated, and how they are reinforced in practices. They include management's actions to remove or reduce incentives and temptations that might prompt personnel to engage in dishonest, illegal, or unethical acts. They also include the communication of entity values and behavioral standards to personnel through policy statements and codes of conduct, as well as by example.

Specific control activities that the service organization has implemented in this area are described below:

- Formally, documented organizational policy statements and codes of conduct communicate entity values and behavioral standards to personnel:
    - Chase Data Staff Orientation, Training, and Competency Policy
    - Chase Data Acceptable Use Policy
    - Chase Data Code of Business Conduct and Ethics
    - Chase Data Employee Handbook and Acknowledgement of Handbook
    - Chase Data HHS Investigations Policy
- Policies and procedures require employees sign an acknowledgment form indicating they have been given access to the employee manual and understand their responsibility for adhering to the policies and procedures contained within the manual
- Acknowledgement of Chase Data Employee Handbook
- A confidentiality statement agreeing not to disclose proprietary or confidential information, including client information, to unauthorized parties is a component of the employee handbook
- Background checks are performed for employees as a component of the hiring process

Commitment to Competence

Chase Data's management defines competence as the knowledge and skills necessary to accomplish tasks that define employees' roles and responsibilities. Management's commitment to competence includes management's consideration of the competence levels for jobs and how those levels translate into the requisite skills and knowledge.

Specific control activities that the service organization has implemented in this area are described below:

- Management has considered the competence levels for jobs and translated required skills and knowledge levels into written position requirements
- Possible candidates are interviewed against the requirements to ensure that a competent resource is identified to fulfill the requirement
- Training and ongoing training are provided to maintain the skill level of personnel in certain positions

Management's Philosophy and Operating Style

Chase Data's management philosophy and operating style encompass a broad range of characteristics. Such characteristics include management's approach to taking and monitoring business risks, and management's attitudes toward business growth, information processing, accounting functions, and personnel.

Specific control activities that the service organization has implemented in this area are described below:

- Management is briefed on regulatory and industry changes affecting the services provided
- Executive management meetings are held to discuss initiatives and issues that affect the business as a whole

Organizational Structure and Assignment of Authority and Responsibility

Chase Data's organizational structure provides the framework within which its activities for achieving entity-wide objectives are planned, executed, controlled, and monitored. Management believes establishing a relevant organizational structure includes considering key areas of authority and responsibility. An organizational structure has been developed to suit its needs. This organizational structure is based, in part, on its size and the nature of its activities.

Chase Data's assignment of authority and responsibility activities include factors such as how authority and responsibility for operating activities are assigned and how reporting relationships and authorization hierarchies are established. It also includes policies relating to appropriate business practices, knowledge, and experience of key personnel, and resources provided for carrying out duties. In addition, it includes policies and communications directed at ensuring personnel understand the entity's objectives, know how their individual actions interrelate and contribute to those objectives, and recognize how and for what they will be held accountable.

Specific control activities that the service organization has implemented in this area are described below:

- Organizational charts are in place to communicate key areas of authority and responsibility
- Organizational charts are communicated to employees and updated as needed

Human Resources Policies and Practices

Chase Data's success is founded on sound business ethics, reinforced with a high level of efficiency, integrity, and ethical standards. The result of this success is evidenced by its proven track record for hiring and retaining top quality personnel who ensures the service organization is operating at maximum efficiency. Chase Data's human resources policies and practices relate to employee hiring, orientation, training, evaluation, counseling, promotion, compensation, and disciplinary activities.

Specific control activities that the service organization has implemented in this area are described below:

- New employees are required to sign acknowledgement forms for the employee handbook and a confidentiality agreement following new hire orientation on their first day of employment
- Goal setting and evaluations for each employee are performed on an annual basis
- Employee termination procedures are in place to guide the termination process and are documented in a termination checklist

Risk Assessment Process

Chase Data risk assessment process identifies and manages risks that could potentially affect Chase Data's ability to provide reliable services to user organizations. This ongoing process requires that management identify significant risks inherent in products or services as they oversee their areas of responsibility. Chase Data identifies the underlying sources of risk, measures the impact to organization, establishes acceptable risk tolerance levels, and implements appropriate measures to monitor and manage the risks.

This process has identified risks resulting from the nature of the services provided by Chase Data, and management has implemented measures designed to manage these risks. Risks identified in this process include the following:

- Operational risk - changes in the environment, accounting, staff, or management personnel
- Strategic risk - new technologies, changing business models, and shifts within the industry

- Compliance - legal and regulatory changes
- Fraud risk - monitor the effectiveness of anti-fraud processes controls in place, and if the culture of honesty and ethics are being practiced by employees

Chase Data's risk manager is responsible for identifying risks to the entity and monitoring the operation of the firm's internal controls. The approach is intended to align the entity's strategy more closely with its key stakeholders, assist the organizational units with managing uncertainty more effectively, minimize threats to the business, and maximize its opportunities in the rapidly changing market environment. Chase Data attempts to actively identify and mitigate significant risks through the implementation of initiatives and communication with senior management.

Integration with Risk Assessment

The environment in which the system operates; the commitments, agreements, and responsibilities of Chase Data's operations; as well as the nature of the components of the system result in risks that the criteria will not be met. Chase Data addresses these risks through the implementation of suitably designed controls to provide reasonable assurance that the criteria are met. Because each system and the environment in which it operates are unique, the combination of risks to meeting the criteria and the controls necessary to address the risks will be unique. As part of the design and operation of the system, Chase Data's management identifies the specific risks that the criteria will not be met and the controls necessary to address those risks.

Information and Communications Systems

Information and communication are an integral component of Chase Data's internal control system. It is the process of identifying, capturing, and exchanging information in the form and time frame necessary to conduct, manage, and control the entity's operations. This process encompasses the primary classes of transactions of the organization, including the dependence on, and complexity of, information technology. At Chase Data, information is identified, captured, processed, and reported by information systems, as well as through conversations with clients, vendors, regulators, and employees.

Monthly meetings are held to discuss operational efficiencies within the applicable functional areas and to disseminate new policies, procedures, controls, and other strategic initiatives within the organization. Additionally, company-wide annual retreats are held in Fort Lauderdale to provide staff with updates on the firm and key issues affecting the organization and its employees. Senior executives lead the company meetings with information gathered from internal systems, as well as conversations with internal and external colleagues. General updates to entity-wide security policies and procedures are routinely communicated to the appropriate Chase Data personnel via e-mail messages.

Monitoring Controls

Management monitors controls to ensure that they are operating as intended and that controls are modified as conditions change. Chase Data's management performs monitoring activities to assess the quality of internal control over time. Necessary corrective actions are taken as required to correct deviations from company policies and procedures. Employee activity and adherence to company policies and procedures is also monitored. This process is accomplished through ongoing monitoring activities, separate evaluations, or a combination of the two.

On-Going Monitoring

Chase Data's management conducts quality assurance monitoring on a regular basis and additional training is provided based upon results of monitoring procedures. Monitoring activities are used to initiate corrective action through department meetings, internal conference calls, and informal notifications.

Management's close involvement in Chase Data's operations helps to identify significant variances from expectations regarding internal controls. Upper management evaluates the facts and circumstances related to any suspected control breakdown. A decision for addressing any control's weakness is made based on whether the incident was isolated or requires a change in the company's procedures or personnel. The goal of this process is to ensure legal compliance and to maximize the performance of Chase Data's personnel.

Reporting Deficiencies

An internal tracking tool is utilized to document and track the results of on-going monitoring procedures. Escalation procedures are maintained for responding and notifying management of any identified risks. Risks receiving a high rating are responded to immediately. Corrective actions, if necessary, are documented and tracked within the internal tracking tool. Annual risk meetings are held for management to review reported deficiencies and corrective actions.

HIPAA/HITECH REQUIREMENTS AND RELATED CONTROLS

Organizational Structure and Assignment of Authority and Responsibility

Chase Data's organizational structure provides the framework within which its activities for achieving enterprise-wide objectives are planned, executed, controlled, and monitored. Management believes establishing a relevant organizational structure includes considering key areas of authority and responsibility. An organizational structure has been developed to suit its needs. This organizational structure is based, in part, on its size and the nature of its activities.

Chase Data's assignment of authority and responsibility activities include factors such as how authority and responsibility is assigned and how reporting relationships and authority hierarchies are established. It also includes policies relating to appropriate business practices, knowledge, and experience of key personnel, and resources provided for carrying out duties. In addition, it includes policies and communications to ensure personnel understand the company's objectives, how their individual actions contribute to those objectives, and what they will be held accountable for. Organizational charts are in place to communicate key areas of authority and responsibility. These charts are communicated to employees and updated as needed.

Risk Assessment Process

Chase Data's risk assessment process identifies and manages risks that could potentially affect the health and safety of personnel and Chase Data's ability to provide reliable services to user organizations. This ongoing process requires that management identify significant risks inherent in products or services as they oversee their areas of responsibility. Chase Data identifies the underlying sources of risk, measures the impact to organization, establishes acceptable tolerance levels, and implements appropriate measures to monitor and manage the risks.

This process has identified risks resulting from the nature of the services provided by Chase Data, and management has implemented various measures designed to manage these risks. Risks identified in this process include the following:

- Operational risk - changes in the environment, staff, or management personnel
- Strategic risk - new technologies, changing business models, and shifts within the industry
- Compliance - legal and regulatory changes

Chase Data has established an organizational business unit that is responsible for identifying risks to the company and monitoring the operation of the firm's internal controls. The approach is intended to align the company's strategy more closely with its key stakeholders, assist the organizational units with managing uncertainty more effectively, minimize threats to the business, and maximize its opportunities in the rapidly changing market environment. Chase Data actively identifies and mitigates significant risks through the implementation of initiatives and continuous communication with other leadership committees and senior management.

Integration with Risk Assessment

The environment in which the system operates; the commitments, agreements, and responsibilities of Chase Data's services; as well as the nature of the components of the system result in risks that the criteria may not be met. Chase Data addresses these risks through the implementation of suitably designed controls to provide reasonable assurance that the criteria are met. Because each system and the environment in which it operates are unique, the combination of risks to meeting the criteria and the controls necessary to address the risks will be unique. As part of the design and operation of the system, Chase Data's management identifies the specific risks that the criteria will not be met and the controls necessary to address those risks.

Periodic Assessments

Chase Data has a risk assessment process in place to identify and manage the risks that could affect the Company's ability to provide services to its user entities. The risk assessment procedure defines the responsibility, methodologies and processes used by Chase Data to assess the risks while providing services and develop mitigation strategies to address those risks. This process requires the Company to identify risk based on management's internal knowledge of its operations. The following risk factors are discussed among the executive management at periodic intervals:

- Risk Assessment: The risk assessment is performed by management personnel
- Health Information Security Risks: Health information security risks are assessed by management personnel

Policies and Procedures

Health information security policies and procedures have been implemented regarding the protection of information assets. The policies and procedures act as a guide for Chase Data personnel. These policies and procedures define guidelines for the health information security program related to scope of services, which includes implementing and managing logical access security and controls, including the following:

- Health information security policy
- Asset management
- Data classification
- Business continuity
- Incident management

These policies are reviewed and approved by management on at least an annual basis.

Security Awareness Training

Chase Data employees receive security awareness training including health information security as part of the onboarding process. This training is reinforced by security awareness communications on current issues which are distributed periodically. Additionally, employees are also required to participate in security awareness training on a quarterly basis.

Remediation and Continuous Improvement

Areas of non-compliance in Chase Data's internal control system surface from many sources, including the Company's ongoing monitoring procedures, separate evaluations of the internal control system, and external parties. Management has developed protocols to help ensure findings, if identified, of internal control non-compliant items should be reported not only to the individual responsible for the function or activity involved, who is in the position to take corrective action. This process enables that individual to provide needed support or oversight for taking corrective action, and to communicate with others in the organization whose activities may be affected. Management evaluates the specific facts and circumstances related to areas of non-compliance in internal control procedures and make the decision for addressing any non-compliant items based on whether the incident was isolated or requires a change in the Company's procedures or personnel.

Incident Response

Chase Data maintains a documented incident response plan including breach notification requirements as mandated by HITECH. The procedures include, but are not limited to, the identification, response, escalation, and remediation of security breaches and other incidents. A formal breach notification process is utilized to document and track resolution of incidents noted. The incident response procedures are tested during the normal course of business and are updated as needed.

Changes to the System Since the Last Review

No significant changes have occurred to the services provided to user entities since the organization's last review.

Incidents Since the Last Review

No significant incidents have occurred to the services provided to user entities since the organization's last review.

Trust Services Criteria and HIPAA/HITECH Requirements Not Applicable to the System

The following Trust Services Criteria and HIPAA/HITECH requirements are not applicable to the system:

Trust Services Criteria and HIPAA/HITECH Requirements Not Applicable to the System		
Category / Safeguard	**Criteria / Requirement**	**Reason**
Administrative Safeguards	164.308(a)(4)(ii)(A); 164.308 (b)(1)	The entity is not a health care clearinghouse.
		The entity is not a covered entity.
Organizational Safeguards	164.314(a)(2)(ii); 164.314(b)(1); 164.314(b)(2)	The entity is not a government entity.
		The entity is not a plan sponsor.

Trust Services Criteria and HIPAA/HITECH Requirements Not Applicable to the System		
Category / Safeguard	**Criteria / Requirement**	**Reason**
Breach Notification	164.404(a); 164.404 (2); 164.404(b); 164.404(c)(1); 164.404(c)(2); 164.404(d)(1)(i); 164.404(d)(1)(ii); 164.404(d)(2); 164.404(d)(2)(i); 164.404(d)(2)(ii); 164.404(d)(3); 164.406; 164.408(a); 164.408(b); 164.408(c)	The entity is a business associate; its responsibilities for breach notification are limited to its covered entity customers.

Subservice Organizations

This report does not include the data center hosting services provided by Google Cloud and OVH at the respective facilities.

Subservice Description of Services

Google Cloud and OVH are internet infrastructure providers that powers the applications. Google Cloud and OVH's hybrid infrastructure delivers performance without compromise, blending virtual and bare-metal cloud, hosting and colocation services across a global network of data centers, optimized from the application to the end user and backed by reliable customer support and uptime.

Complementary Subservice Organization Controls

Chase Data's services are designed with the assumption that certain controls will be implemented by subservice organizations. Such controls are called complementary subservice organization controls. It is not feasible for all of the trust services criteria and HIPAA/HITECH requirements related to Chase Data's services to be solely achieved by Chase Data control procedures. Accordingly, subservice organizations, in conjunction with the services, should establish their own internal controls or procedures to complement those of Chase Data.

The following subservice organization controls should be implemented by Google Cloud to provide additional assurance that the trust services criteria and HIPAA/HITECH requirements described within this report are met:

Subservice Organization - Google Cloud		
Category / Safeguard	**Criteria / Requirement**	**Control**
Common Criteria/Security; Physical Safeguards	CC6.4; 164.310(a)(1); 164.310(a)(2)(ii); 164.310(a)(2)(iii); 164.310(a)(2)(iv)	Only authorized employees, contractors, security guards, and customers are granted physical access to the data center.
		Physical access to the data center is revoked upon termination of employees, contractors, and security guards.
		Physical access to the data center is revoked upon notification by customers to the NOC for customer employee terminations.
		Colocation security personnel perform a quarterly audit to validate the appropriateness of all employee, contractor, and security guard physical access to the data centers. Third-party service vendors are contacted periodically to verify the appropriateness of contractor physical access to data centers.
		Colocation security personnel perform a quarterly audit to validate the appropriateness of all customers' physical access to the data centers.
		In order to gain physical access to data centers, employees and customers must be validated via a combination of key card and/or biometric technology.
		Customer equipment is segregated via locked cages or locked cabinets to ensure that customers can only access their own equipment. Lock mechanisms are combination, badge reader, or physical key.

The following subservice organization controls should be implemented by OVH to provide additional assurance that the trust services criteria and HIPAA/HITECH requirements described within this report are met:

Subservice Organization - OVHcloud		
Category / Safeguard	**Criteria / Requirement**	**Control**
Common Criteria/Security; Physical Safeguards	CC6.4; 164.310(a)(1); 164.310(a)(2)(ii); 164.310(a)(2)(iii); 164.310(a)(2)(iv)	Only authorized employees, contractors, security guards, and customers are granted physical access to the data center.
		Physical access to the data center is revoked upon termination of employees, contractors, and security guards.

Subservice Organization - OVHcloud		
Category / Safeguard	**Criteria / Requirement**	**Control**
		Physical access to the data center is revoked upon notification by customers to the NOC for customer employee terminations.
		colocation security personnel perform a quarterly audit to validate the appropriateness of all employee, contractor, and security guard physical access to the data centers. Third-party service vendors are contacted periodically to verify the appropriateness of contractor physical access to data centers.
		colocation security personnel perform a quarterly audit to validate the appropriateness of all customers' physical access to the data centers.
		In order to gain physical access to data centers, employees and customers must be validated via a combination of key card and/or biometric technology.
		Customer equipment is segregated via locked cages or locked cabinets to ensure that customers can only access their own equipment. Lock mechanisms are combination, badge reader, or physical key.

Chase Data management, along with the subservice organizations, define the scope and responsibility of the controls necessary to meet all the relevant trust services criteria through written contracts, such as service level agreements. In addition, Chase Data performs monitoring of the subservice organization controls, including the following procedures:

- Reviewing and reconciling output reports
- Reviewing attestation reports over services provided by vendors and subservice organizations

COMPLEMENTARY USER ENTITY CONTROLS

Chase Data's services are designed with the assumption that certain controls will be implemented by user entities. Such controls are called complementary user entity controls. It is not feasible for all of the Trust Services Criteria and HIPAA/HITECH requirements related to Chase Data's services to be solely achieved by Chase Data control procedures. Accordingly, user entities, in conjunction with the services, should establish their own internal controls or procedures to complement those of Chase Data's.

The following complementary user entity controls should be implemented by user entities to provide additional assurance that the Trust Services Criteria and HIPAA/HITECH requirements described within this report are met. As these items represent only a part of the control considerations that might be pertinent at the user entities' locations, user entities' auditors should exercise judgment in selecting and reviewing these complementary user entity controls.

1. User entities are responsible for understanding and complying with their contractual obligations to Chase Data.
2. User entities are responsible for maintaining their own system of record.
3. User entities are responsible for ensuring the supervision, management, and control of the use of Chase Data services by their personnel.
4. User entities are responsible for immediately notifying Chase Data of any actual or suspected information security breaches, including compromised user accounts, including those used for integrations and secure file transfers.

TRUST SERVICES CATEGORIES

In-Scope Trust Services Categories

Common Criteria (to the Security Category)
Security refers to the protection of i. information during its collection or creation, use, processing, transmission, and storage and ii. systems that use electronic information to process, transmit or transfer, and store information to enable the entity to meet its objectives. Controls over security prevent or detect the breakdown and circumvention of segregation of duties, system failure, incorrect processing, theft or other unauthorized removal of information or system resources, misuse of software, and improper access to or use of, alteration, destruction, or disclosure of information.

HEALTH INFORMATION SECURITY PROGRAM

Chase Data has developed a health information security management program to meet the information security and compliance requirements related to Call Center Software Services System and its customer base. The program incorporates the elements of the HIPAA and the HITECH. The description below is a summary of safeguards that Chase Data has implemented to adhere to the applicable components of HIPAA Final Security Rule and the breach notification requirements of HITECH.

Administrative Safeguards - Policies and procedures designed to show how Chase Data complies with the act:

- Management has adopted a written set of health information security policies and designated the information security officer to be responsible for developing and implementing the required policies and procedures.
- Procedures address access authorization, establishment, modification, and termination.
- Documented incident response policies for reporting security incidents are in place to guide employees in identifying, reporting, of security incidents.
- Business continuity plans are documented to enable continuation of critical business processes in the event of an emergency.
- Privileged administrative access to systems is restricted to authorized individuals.
- Automated backup systems are in place to perform scheduled replication of production data and systems at pre-defined intervals.
- Antivirus software is utilized to detect and eliminate data or files that contain certain virus signatures on certain production servers.

Physical Safeguards - Controlling physical access to protected data:

- Access procedures are in place restrict access and terminate access to protected data.
- Inventory listings are utilized to track and monitor hardware and removable media.
- Data destruction procedures are in place to guide the secure disposal of data and media.

Technical Safeguards - Controlling access to computer systems and enabling covered entities to protect communications containing Protected Health Information (PHI) transmitted electronically over open networks from being intercepted by anyone other than the intended recipient:

- Access to in-scope systems are restricted to authorized personnel based on a valid user account and password.
- Systems are configured to enforce pre-determined thresholds to lock user sessions due to invalid login attempts.
- Security monitoring applications and manual reviews are utilized to monitor and analyze the in-scope systems for possible or actual security breaches.

Organizational Safeguards - Adherence to policies and procedures in regard to PHI documentation availability, as well as documentation retention:

- Documented policies address the confidentiality threshold of PHI documents and the length of time they should be retained before being destroyed.
- Contractual responsibilities by subparts of an organization are written and maintained in contracts.
- Separation of duties is existent in order to protect to confidentiality, availability, and integrity of PHI.
- Ensure that only appropriate parties gain access to PHI internally and external to the organization.

Breach Notification - A business associate shall, following the discovery of a breach of unsecured protected health information, notify the covered entity of such breach:

- Documented policies and procedures are in place to guide personnel in notifying the covered entity upon discovery of a breach.
- Documented policies and procedures are in place to guide personnel in responding to discovery of a breach.
- Documented policies and procedures require disclosure of the unsecured protected health information and include, to the extent possible, the identification of each individual and a description of the event.
- Documented policies and procedures are in place to guide personnel in the exception processes of delaying and documenting notifications.
- Documented policies and procedures are in place to guide personnel in documentation of administrative requirements for demonstrating that notifications were made as required.

CONTROL ACTIVITIES SPECIFIED BY THE SERVICE ORGANIZATION

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
CC1.0	**Control Environment**	
Control Point	**Criteria**	**Control Activity Specified by the Service Organization**
CC1.1	COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.	Core values are communicated from executive management to personnel through policies, directives, guidelines, the code of conduct and the employee handbook. An employee handbook and code of conduct are documented to communicate workforce conduct standards and enforcement procedures. Upon hire, personnel are required to acknowledge the employee handbook and code of conduct. Upon hire, personnel are required to complete a background check. Personnel are required to acknowledge the employee handbook and code of conduct on an annual basis. Performance and conduct evaluations are performed for personnel on an annual basis. Sanction policies, which include probation, suspension and termination, are in place for employee misconduct. An anonymous hotline is in place to allow employees, third-parties, and customers to report unethical behavior in a confidential manner.
CC1.2	COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	Executive management roles and responsibilities are documented and reviewed annually. Executive management evaluates the skills and expertise of its members annually. Executive management maintains independence from those that operate the key controls within the environment. Executive management meets monthly with operational management to assess the effectiveness and performance of internal controls within the environment. Operational management assigns responsibility for and monitors the effectiveness and performance of internal controls implemented within the environment.
CC1.3	COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	A documented organizational chart is in place that defines organizational structures, lines of reporting, and areas of authority. Executive management reviews the organizational chart annually and makes updates to the organizational structure and lines of reporting, if necessary.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
CC1.0	**Control Environment**	
Control Point	**Criteria**	**Control Activity Specified by the Service Organization**
		Roles and responsibilities are defined in written job descriptions and communicated to personnel through the entity's Google Drive.
		Executive management reviews job descriptions annually and makes updates, if necessary.
		Upon hire, personnel are required to acknowledge the employee handbook which requires adherence to the personnel's job role and responsibilities.
		Executive management has established proper segregations of duties for key job functions and roles within the organization.
CC1.4	COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	Policies and procedures are in place that outline the performance evaluation process as well as the competency and training requirements for personnel.
		Performance and conduct evaluations are performed for personnel on an annual basis.
		The entity evaluates the competencies and experience of candidates prior to hiring, and of personnel transferring job roles or responsibilities.
		Job requirements are documented in the job descriptions and candidates' abilities to meet these requirements are evaluated as part of the hiring or transfer process.
		The entity has a recruiting department that is responsible for attracting individuals with competencies and experience that align with the entity's goals and objectives.
		Employees are required to attend continued training annually that relates to their job role and responsibilities.
		Executive management uses an outside vendor to assist with its continued training of employees.
		Upon hire, personnel are required to complete a background check.
CC1.5	COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	A documented organizational chart is in place that defines organizational structures, lines of reporting, and areas of authority.
		Roles and responsibilities are defined in written job descriptions and communicated to personnel through the entity's Google Drive.
		Upon hire, personnel are required to acknowledge the employee handbook which requires adherence to the personnel's job role and responsibilities.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
CC1.0	**Control Environment**	
Control Point	**Criteria**	**Control Activity Specified by the Service Organization**
		Personnel are required to acknowledge the employee handbook and code of conduct on an annual basis. Policies and procedures are in place that outline the performance evaluation process as well as the competency and training requirements for personnel. Performance and conduct evaluations are performed for personnel on an annual basis. Sanction policies, which include probation, suspension and termination, are in place for employee misconduct.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
CC2.0	**Information and Communication**	
Control Point	**Criteria**	**Control Activity Specified by the Service Organization**
CC2.1	COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	Organizational and information security policies and procedures are documented for supporting the functioning of controls and processes and made available to its personnel through the entity's ADP Portal and Google Drive. Data flow diagrams are documented and maintained by management to identify the relevant internal and external information sources of the system. Data that entered into the system, processed by the system and output from the system is protected from unauthorized access.
CC2.2	COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	Roles and responsibilities are defined in written job descriptions and communicated to personnel through the entity's Google Drive. The entity's policies and procedures, code of conduct and employee handbook are made available to employees through the entity's ADP Portal. Upon hire, employees are required to read and acknowledge the information security policies and procedures and complete information security and awareness training. Current employees are required to read and acknowledge the information security policies and procedures and complete information security and awareness training on an annual basis. Upon hire, personnel are required to acknowledge the employee handbook and code of conduct. Personnel are required to acknowledge the employee handbook and code of conduct on an annual basis. Employees are required to attend security awareness training quarterly. Management tracks and monitors compliance with information security and awareness training requirements.
CC2.3	COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.	The entity's third-party agreement delineates the boundaries of the system and describes relevant system components. The entity's third-party agreement communicates the system commitments and requirements of third-parties. The system commitments and requirements of external users are provided to external users prior to allowing them access to the system.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
CC2.0	**Information and Communication**	
Control Point	**Criteria**	**Control Activity Specified by the Service Organization**
		The entity's third-party agreement outlines and communicates the terms, conditions and responsibilities of third-parties. Customer commitments, requirements and responsibilities are outlined and communicated through service agreements. Documented escalation procedures for reporting failures incidents, concerns and other complaints are in place and shared with external parties.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
CC3.0	**Risk Assessment**	
Control Point	**Criteria**	**Control Activity Specified by the Service Organization**
CC3.1	COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	The entity establishes organizational strategies and objectives that are used to determine entity structure and performance metrics. Executive management identifies and assesses risks that could prevent the entity's objectives from being achieved. Responsible parties are defined and assigned to coordinate and monitor compliance and audit activities. Budgets align with the entity's strategies and objectives. Entity strategies, objectives and budgets are assessed on a monthly basis. The entity undergoes compliance audits at least annually to show compliance to relevant laws, regulations and standards.
CC3.2	COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.	Documented policies and procedures are in place to guide personnel when performing a risk assessment. Management has defined a formal risk assessment process that specifies the process for identifying internal and external threats and vulnerabilities, evaluating and addressing risks and defining specified risk tolerances. A formal risk assessment is performed on at least an annual basis to identify internal and external threats and vulnerabilities that could impair system commitments and requirements. The entity's risk assessment process includes: • Identifying the relevant information assets that are critical to business operations • Prioritizing the criticality of those relevant information assets • Identifying and assessing the impact of the threats to those information assets • Identifying and assessing the impact of the vulnerabilities associated with the identified threats • Assessing the likelihood of identified threats and vulnerabilities • Determining the risks associated with the information assets • Addressing the associated risks • Identified for each identified vulnerability Identified risks are rated using a risk evaluation process and ratings are approved by management.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
CC3.0	**Risk Assessment**	
Control Point	**Criteria**	**Control Activity Specified by the Service Organization**
		Risks identified as a part of the risk assessment process are addressed using one of the following strategies: • Avoid the risk • Mitigate the risk • Transfer the risk • Accept the risk Management develops risk mitigation strategies to address risks identified during the risk assessment process. For gaps and vulnerabilities identified from the risk assessment, remediation efforts, including the implementation of controls, are assigned to process owners based on roles and responsibilities.
CC3.3	COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.	On an annual basis, management identifies and assesses the types of fraud that could impact their business and operations. As part of management's assessment of fraud risks, management considers key fraud factors such as incentives, pressures, opportunity for unauthorized access or use of data, and employee morale and attitude.
CC3.4	COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.	Changes to the business structure and operations are considered and evaluated as part of the annual comprehensive risk assessment. Changes in key management and personnel are considered and evaluated as part of the annual comprehensive risk assessment. Changes to the entity's systems, applications, technologies, and tools are considered and evaluated as part of the annual comprehensive risk assessment.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
CC4.0	**Monitoring Activities**	
Control Point	**Criteria**	**Control Activity Specified by the Service Organization**
CC4.1	COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.	Monitoring software is used to identify and evaluate ongoing system performance, capacity, security threats, changing resource utilization needs and unusual system activity. Management reviews policies, procedures and other control documents for accuracy and applicability on an annual basis. On an annual basis, management reviews the controls implemented within the environment for operational effectiveness and identifies potential control gaps and weaknesses. Control self-assessments that include, but are not limited to, logical access reviews, and backup restoration tests are performed on at least an annual basis. Vulnerability scans are performed annually on the environment to identify control gaps and vulnerabilities. Evaluations of policies, controls, systems, tools, applications, and third-parties for effectiveness and compliance is required at least annually. A third-party performs a penetration test annually to identify and exploit vulnerabilities identified within the environment. Performance and conduct evaluations are performed for personnel on an annual basis. Management obtains and reviews attestation reports of third-parties to evaluate the effectiveness of controls within the vendor or third-party's environment. A formal risk assessment is performed on at least an annual basis to identify internal and external threats and vulnerabilities that could impair system commitments and requirements.
CC4.2	COSO Principle 17: The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.	Vulnerabilities, deviations and control gaps identified from the compliance, control and risk assessments are communicated to those parties responsible for taking corrective actions. Vulnerabilities, deviations and control gaps identified from the compliance, control and risk assessments are documented, investigated, and addressed. Vulnerabilities, deviations and control gaps identified from the compliance, control and risk assessments are addressed by those parties responsible for taking corrective actions.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
CC4.0	**Monitoring Activities**	
Control Point	**Criteria**	**Control Activity Specified by the Service Organization**
		Management tracks whether vulnerabilities, deviations and control gaps identified as part of the evaluations performed are addressed in a timely manner.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
CC5.0	**Control Activities**	
Control Point	**Criteria**	**Control Activity Specified by the Service Organization**
CC5.1	COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	Controls within the environment are modified and implemented to mitigate vulnerabilities, deviations and control gaps identified as part of the various evaluations performed. Performance of the internal controls implemented within the environment are assigned to appropriate process owners and operational personnel based on roles and responsibilities. Management has documented the relevant controls in place for each key business or operational process. Management has incorporated a variety of controls into their environment that include manual, automated, preventive, detective, and corrective controls. Management develops risk mitigation strategies, including the implementation of controls, to address risks identified during the risk assessment process. Business continuity and disaster recovery plans are developed and updated on an annual basis. Business continuity and disaster recovery plans are tested on an annual basis.
CC5.2	COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.	Organizational and information security policies and procedures are documented for supporting the functioning of controls and processes and made available to its personnel through the entity's ADP Portal and Google Drive. Management has established controls around the entity's technology infrastructure to address the risks of incomplete, inaccurate, and unavailable technology processing. The internal controls implemented around the entity's technology infrastructure include, but are not limited to: • Restricting access rights to authorized users • Limiting services to what is required for business operations • Authentication of access • Protecting the entity's assets from external threats
CC5.3	COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	Organizational and information security policies and procedures are documented for supporting the functioning of controls and processes and made available to its personnel through the entity's ADP Portal and Google Drive.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
CC5.0	**Control Activities**	
Control Point	**Criteria**	**Control Activity Specified by the Service Organization**
		The organizational and information security policies and procedures detail the day-to-day activities to be performed by personnel. Management has implemented controls that are built into the organizational and information security policies and procedures. Process owners and key management are assigned ownership to each key internal control implemented within the entity's environment. Roles and responsibilities are defined in written job descriptions and communicated to personnel through the entity's Google Drive. Performance of the internal controls implemented within the environment are assigned to appropriate process owners and operational personnel based on roles and responsibilities.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
CC6.0	**Logical and Physical Access**	
Control Point	**Criteria**	**Control Activity Specified by the Service Organization**
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	An inventory of system assets and components is maintained to classify and manage the information assets. Privileged access to sensitive resources is restricted to authorized personnel. Documented policies and procedures are in place regarding system settings, access, and security monitoring.
	Network	
		Network user access is restricted via role-based security privileges defined within the access control system. Network administrative access is restricted to user accounts accessible by the following personnel: • CTO • VP of Tech Services & Support Networks are configured to enforce password requirements that include: • Password history • Password age • Password length • Complexity Network users are authenticated via individually assigned user accounts and passwords. Network account lockout settings are in place that include: • Account lockout duration • Account lockout threshold • Account lockout counter reset Network audit logging settings are in place that include: • Account logon events • Account management • Directory service access • Logon events • Object access • Policy change • Privilege use • Process tracking • System events • Security system extension • System integrity • IPsec driver • Other system events • Security state change

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
CC6.0	**Logical and Physical Access**	
Control Point	**Criteria**	**Control Activity Specified by the Service Organization**
		Network audit logs are maintained and reviewed as needed.
	Operating System	
		Operating system user access is restricted via role-based security privileges defined within the access control system. Operating system administrative access is restricted to user accounts accessible by the following personnel: • CTO • VP of Tech Services & Support Operating systems are configured to enforce password requirements that include: • Password history • Password age • Password length • Complexity Operating system users are authenticated via individually assigned user accounts and passwords. Operating system account lockout settings are in place that include: • Account lockout duration • Account lockout threshold • Account lockout counter reset Operating system audit logging settings are in place that include: • Account logon events • Account management • Directory service access • Logon events • Object access • Policy change • Privilege use • Process tracking • System events • Security system extension • System integrity • IPsec driver • Other system events • Security state change Operating system audit logs are maintained and reviewed as needed.
	Database	
		Database user access is restricted via role-based security privileges defined within the access control system.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
CC6.0	**Logical and Physical Access**	
Control Point	**Criteria**	**Control Activity Specified by the Service Organization**
		Database administrative access is restricted to user accounts accessible by the following personnel: • President/CEO • CTO Databases are configured to enforce password requirements that include: • Password history • Password age • Password length • Complexity Database users are authenticated via individually assigned user accounts and passwords. Database account lockout settings are in place that include: • Account lockout duration • Account lockout threshold • Account lockout counter reset Database audit logging settings are in place that include: • Application role change password • Audit change • Backup restore • Broker login • Database change • Database logout • Database ownership change • Database permission change • Database principal change • Database principal impersonation • Database role member change • Failed database authentication • Failed login • Logout • Successful database authentication • Successful login • User change password Database audit logs are maintained and reviewed as needed.
	Application	
		Application user access is restricted via role-based security privileges defined within the access control system.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
CC6.0	**Logical and Physical Access**	
Control Point	**Criteria**	**Control Activity Specified by the Service Organization**
		Application administrative access is restricted to user accounts accessible by the following personnel: • CTO • VP of Tech Services & Support • Senior Product Specialist The application is configured to enforce password requirements that include: • Password age • Password length • Complexity Application users are authenticated via individually assigned user accounts and passwords. Application account lockout settings are in place that include: • Account lockout trigger Application audit policy settings are in place that include: • Account logon events • Account activity • Account logoff events • Account management • System events Application audit logs are maintained and reviewed as needed. Data coming into the environment is secured and monitored through the use of firewalls and an IDS and IPS. Server certificate-based authentication is used as part of the TLS encryption with a trusted certificate authority. Stored passwords are encrypted. Critical data is stored in encrypted format using software supporting the AES. Encryption keys are protected during storage and use. The entity restricts access to its environment using the following mechanisms: • Port restrictions (via firewall rule settings) • Access protocol restrictions (via firewall rule settings) • User identification • Digital certifications

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
CC6.0	**Logical and Physical Access**	
Control Point	**Criteria**	**Control Activity Specified by the Service Organization**
		Logical access to systems is approved and granted to an employee as a component of the hiring process.
		Logical access to systems is revoked as a component of the termination process.
CC6.2	Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.	Documented policies and procedures are in place regarding system settings, access, and security monitoring.
		Logical access to systems is approved and granted to an employee as a component of the hiring process.
		Logical access to systems is revoked as a component of the termination process.
		Logical access reviews are completed on an annual basis.
		Privileged access to sensitive resources is restricted to authorized personnel.
CC6.3	The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.	Documented policies and procedures are in place regarding system settings, access, and security monitoring.
		Logical access to systems is approved and granted to an employee as a component of the hiring process.
		Logical access to systems is revoked as a component of the termination process.
		Privileged access to sensitive resources is restricted to authorized personnel.
		Control self-assessments that include physical and logical access reviews are performed on at least an annual basis.
CC6.4	The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.	The controls related to this criterion are the responsibility of the subservice organization. Refer to the Subservice Organizations section above for controls managed by the subservice organization.
CC6.5	The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.	Policies and procedures are in place to guide personnel in purging data off of machines prior to sending them to Google Cloud/OVH to destroy.
		The entity purges servers and hardware when they are no longer rendered applicable for business purposes.
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	Network address translation (NAT) functionality is utilized to manage internal IP addresses.
		Server certificate-based authentication is used as part of the TLS encryption with a trusted certificate authority.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
CC6.0	**Logical and Physical Access**	
Control Point	**Criteria**	**Control Activity Specified by the Service Organization**
		A firewall is in place to filter unauthorized inbound network traffic from the internet. The firewall system is configured to deny any type of network connection that is not explicitly authorized by a firewall system rule. An IDS and an IPS are utilized to analyze network events and report possible or actual network security breaches. Antivirus software is installed on workstations to detect and prevent the transmission of data or files that contain certain virus signatures recognized by the antivirus software. The antivirus software provider pushes updates to the installed antivirus software as new updates/signatures are available. The antivirus software is configured to scan workstations on a daily basis. Critical data is stored in encrypted format using software supporting the AES. Use of removable media is prohibited by policy except when authorized for a valid business case by management.
CC6.7	The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.	Backup media is rotated off-site by a third-party vendor at least weekly. The ability to recall backed up data is restricted to authorized personnel. The entity secures its environment using a multi-layered defense approach that includes firewalls, and IDS and an IPS. Server certificate-based authentication is used as part of the TLS encryption with a trusted certificate authority. A firewall is in place to filter unauthorized inbound network traffic from the internet. The firewall system is configured to deny any type of network connection that is not explicitly authorized by a firewall system rule. NAT functionality is utilized to manage internal IP addresses. An IDS and IPS are utilized to analyze network events and report possible or actual network security breaches. Critical data is stored in encrypted format using software supporting the AES. Backup media is stored in an encrypted format.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
CC6.0	**Logical and Physical Access**	
Control Point	**Criteria**	**Control Activity Specified by the Service Organization**
CC6.8	The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.	Use of removable media is prohibited by policy except when authorized for a valid business case by management. The ability to install applications and software is restricted to authorized personnel. The ability to migrate changes into the production environment is restricted to authorized and appropriate users. File integrity monitoring (FIM) software is in place to ensure only authorized changes are deployed into the production environment. The FIM software is configured to notify key IT personnel via e-mail alert when a change to the production application code files is detected. Documented change control policies and procedures are in place to guide personnel in the change management process. Antivirus software is installed on workstations to detect and prevent the transmission of data or files that contain certain virus signatures recognized by the antivirus software. The antivirus software provider pushes updates to the installed antivirus software as new updates/signatures are available. The antivirus software is configured to scan workstations on a daily basis. Information assets, software, hardware, tools, and applications introduced into the environment are scanned for vulnerabilities and malware prior to implementation into the environment.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
CC7.0	**System Operations**	
Control Point	**Criteria**	**Control Activity Specified by the Service Organization**
CC7.1	To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.	Management has defined configuration standards in the information security policies and procedures. Monitoring software is used to identify and evaluate ongoing system performance, capacity, security threats, changing resource utilization needs and unusual system activity. The monitoring software is configured to alert IT personnel, support groups and executives when thresholds have been exceeded. An IDS and IPS are utilized to analyze network events and report possible or actual network security breaches. FIM software is in place to ensure only authorized changes are deployed into the production environment. The FIM software is configured to notify key IT personnel via e-mail alert when a change to the production application code files is detected. Use of removable media is prohibited by policy except when authorized for a valid business case by management. A firewall is in place to filter unauthorized inbound network traffic from the internet. The firewall system is configured to deny any type of network connection that is not explicitly authorized by a firewall system rule. Policies and procedures are in place regarding detection, logging, and monitoring of unknown or unauthorized components into the environment. Internal and external vulnerability scans are performed on at least an annual basis and remedial actions are taken where necessary.
CC7.2	The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.	Documented incident response and escalation procedures for reporting security incidents are in place to guide users in identifying, reporting and mitigating failures, incidents, concerns, and other complaints. Policies and procedures are in place regarding detection, logging, and monitoring of unknown or unauthorized components into the environment. The monitoring software is configured to alert IT personnel, support groups and executives when thresholds have been exceeded.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
CC7.0	**System Operations**	
Control Point	**Criteria**	**Control Activity Specified by the Service Organization**
		Monitoring software is used to identify and evaluate ongoing system performance, capacity, security threats, changing resource utilization needs and unusual system activity. An IDS and IPS are utilized to analyze network events and report possible or actual network security breaches. FIM software is in place to ensure only authorized changes are deployed into the production environment. The FIM software is configured to notify key IT personnel via e-mail alert when a change to the production application code files is detected. A firewall is in place to filter unauthorized inbound network traffic from the internet. The firewall system is configured to deny any type of network connection that is not explicitly authorized by a firewall system rule. Antivirus software is installed on workstations to detect and prevent the transmission of data or files that contain certain virus signatures recognized by the antivirus software. The antivirus software provider pushes updates to the installed antivirus software as new updates/signatures are available. The antivirus software is configured to scan workstations on a daily basis. Use of removable media is prohibited by policy except when authorized for a valid business case by management.
CC7.3	The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.	Documented incident response and escalation procedures for reporting security incidents are in place to guide users in identifying, reporting and mitigating failures, incidents, concerns, and other complaints. The incident response and escalation procedures are reviewed at least annually for effectiveness. The incident response policies and procedures define the classification of incidents based on its threat level. Resolution of incidents are documented within the ticket and communicated to affected users. Incidents are documented and tracked in a standardized ticketing system and updated to reflect the planned incident and problem resolution.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
CC7.0	**System Operations**	
Control Point	**Criteria**	**Control Activity Specified by the Service Organization**
		Incidents resulting in the unauthorized use or disclosure of personal information are communicated to the affected users.
		Identified incidents are analyzed, classified and prioritized based on threat level to determine the appropriate response strategy, including step by step procedures.
CC7.4	The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.	Roles and responsibilities for the implementation and execution of the incident response program are defined and documented.
		Documented incident response and escalation procedures for reporting security incidents are in place to guide users in identifying, reporting and mitigating failures, incidents, concerns, and other complaints.
		Incidents are documented and tracked in a standardized ticketing system and updated to reflect the planned incident and problem resolution.
		Documented incident response procedures are in place to guide personnel in addressing the threats posed by security incidents.
		Resolution of incidents are documented within the ticket and communicated to affected users.
		Remediation actions taken for security incidents are documented within the ticket and communicated to affected users.
		Identified incidents are analyzed, classified and prioritized based on threat level to determine the appropriate response strategy, including step by step procedures.
		The incident response and escalation procedures are reviewed at least annually for effectiveness.
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	Data backup and restore procedures are in place to guide personnel in performing backup activities.
		Control self-assessments that include, but are not limited to, logical access reviews, and backup restoration tests are performed on at least an annual basis.
		On an annual basis, preventative and detective controls are evaluated and changed as necessary.
		A business continuity and disaster recovery plan is documented to identify and reduce risks, limit the consequences of damaging incidents, and ensure the timely resumption of essential operations.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
CC7.0	**System Operations**	
Control Point	**Criteria**	**Control Activity Specified by the Service Organization**
		The disaster recovery plan is tested on an annual basis.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
CC8.0	**Change Management**	
Control Point	**Criteria**	**Control Activity Specified by the Service Organization**
CC8.1	The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	Documented change control policies and procedures are in place to guide personnel in the change management process. The change management process has defined the following roles and assignments: • Authorization of change requests • Change tests • Code review • Push change to production System changes are communicated to both affected internal and external users. Access to implement changes in the production environment is restricted to authorized IT personnel. System changes are authorized and approved by management prior to implementation. Prior code is held in the source code repository for rollback capability in the event that a system change does not function as designed. Development and test environments are physically and logically separated from the production environment. System change requests are documented and tracked in a ticketing system. FIM software is utilized to help detect unauthorized changes within the production environment. System changes are tested prior to implementation. Types of testing performed depend on the nature of the change. Information security policies and procedures document the baseline requirements for configuration of IT systems and tools. Documented change control policies and procedures are in place to guide personnel in the change management process.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
CC9.0	**Risk Mitigation**	
Control Point	**Criteria**	**Control Activity Specified by the Service Organization**
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	Documented policies and procedures are in place to guide personnel in performing risk mitigation activities. Management has defined a formal risk assessment process that specifies the process for identifying internal and external threats and vulnerabilities, evaluating and addressing risks and defining specified risk tolerances. A formal risk assessment is performed on at least an annual basis to identify internal and external threats and vulnerabilities that could impair system commitments and requirements. Identified risks are rated using a risk evaluation process and ratings are approved by management. Management develops risk mitigation strategies to address risks identified during the risk assessment process.
CC9.2	The entity assesses and manages risks associated with vendors and business partners.	Management has defined a third-party vendor risk management process that specifies the process for evaluating third-party risks based on identified threats and the specified tolerances. Management develops third-party risk mitigation strategies to address risks identified during the risk assessment process. Identified third-party risks are rated using a risk evaluation process and ratings are approved by management. The entity's third-party agreement outlines and communicates the terms, conditions and responsibilities of third-parties. Management obtains and reviews attestation reports of vendors and third-parties to evaluate the effectiveness of controls within the vendor or third-party's environment.

ADMINISTRATIVE SAFEGUARDS		
Ref	**Regulation**	**Control Activity Specified by the Service Organization**
164.308 (a)(1)(i)	**Security management process:** Implement policies and procedures to prevent, detect, contain and correct security violations.	Documented incident response and escalation procedures for reporting security incidents are in place to guide users in identifying, reporting and mitigating failures, incidents, concerns, and other complaints. Policies and procedures are in place regarding preventing, detecting, containing, and correcting security violations. Monitoring software is used to identify and evaluate ongoing system performance, capacity, security threats, changing resource utilization needs and unusual system activity. The monitoring software is configured to alert IT personnel, support groups and executives when thresholds have been exceeded. An IDS and IPS are utilized to analyze network events and report possible or actual network security breaches. FIM software is in place to ensure only authorized changes are deployed into the production environment. The FIM software is configured to notify key IT personnel via e-mail alert when a change to the production application code files is detected. Antivirus software is installed on workstations to detect and prevent the transmission of data or files that contain certain virus signatures recognized by the antivirus software. Internal and external vulnerability scans are performed on at least an annual basis and remedial actions are taken where necessary.
	Network	
		Network account lockout settings are in place that include: • Account lockout duration • Account lockout threshold • Account lockout counter reset

ADMINISTRATIVE SAFEGUARDS		
Ref	**Regulation**	**Control Activity Specified by the Service Organization**
		Network audit logging settings are in place that include: • Account logon events • Account management • Directory service access • Logon events • Object access • Policy change • Privilege use • Process tracking • System events • Security system extension • System integrity • IPsec driver • Other system events • Security state change Network audit logs are maintained and reviewed as needed.
	Operating System	
		Operating system user access is restricted via role-based security privileges defined within the access control system. Operating system administrative access is restricted to user accounts accessible by the following personnel: • CTO • VP of Tech Services & Support Operating systems are configured to enforce password requirements that include: • Password history • Password age • Password length • Complexity Operating system users are authenticated via individually assigned user accounts and passwords. Operating system account lockout settings are in place that include: • Account lockout duration • Account lockout threshold • Account lockout counter reset

ADMINISTRATIVE SAFEGUARDS		
Ref	**Regulation**	**Control Activity Specified by the Service Organization**
		Operating system audit logging settings are in place that include: • Account logon events • Account management • Directory service access • Logon events • Object access • Policy change • Privilege use • Process tracking • System events • Security system extension • System integrity • IPsec driver • Other system events • Security state change Operating system audit logs are maintained and reviewed as needed.
	Database	
		Database account lockout settings are in place that include: • Account lockout duration • Account lockout threshold • Account lockout counter reset Database audit logging settings are in place that include: • Application role change password • Audit change • Backup restore • Broker login • Database change • Database logout • Database ownership change • Database permission change • Database principal change • Database principal impersonation • Database role member change • Failed database authentication • Failed login • Logout • Successful database authentication • Successful login • User change password Database audit logs are maintained and reviewed as needed.
	Application	
		Application account lockout settings are in place that include: • Account lockout trigger

ADMINISTRATIVE SAFEGUARDS		
Ref	**Regulation**	**Control Activity Specified by the Service Organization**
164.308 (a)(1)(ii)(A)	**Risk analysis:** Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity or business associate.	Application audit policy settings are in place that include: • Account logon events • Account activity • Account logoff events • Account management • System events Application audit logs are maintained and reviewed as needed. Documented policies and procedures are in place to guide personnel when performing a risk assessment. Management has defined a formal risk assessment process that specifies the process for identifying internal and external threats and vulnerabilities, evaluating and addressing risks and defining specified risk tolerances. A formal risk assessment is performed on at least an annual basis to identify internal and external threats and vulnerabilities that could impair system commitments and requirements. The entity's risk assessment process includes: • Identifying the relevant information assets that are critical to business operations • Prioritizing the criticality of those relevant information assets • Identifying and assessing the impact of the threats to those information assets • Identifying and assessing the impact of the vulnerabilities associated with the identified threats • Assessing the likelihood of identified threats and vulnerabilities • Determining the risks associated with the information assets • Addressing the associated risks • Identified for each identified vulnerability

ADMINISTRATIVE SAFEGUARDS		
Ref	**Regulation**	**Control Activity Specified by the Service Organization**
164.308 (a)(1)(ii)(B)	**Risk management:** Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with § 164.306(a). Factors identified in §164.306 include: • The size, complexity, capability of the covered entity • The covered entity's technical infrastructure • The costs of security measures • The probability and criticality of potential risks to ePHI	The entity's risk assessment process includes: • Identifying the relevant information assets that are critical to business operations • Prioritizing the criticality of those relevant information assets • Identifying and assessing the impact of the threats to those information assets • Identifying and assessing the impact of the vulnerabilities associated with the identified threats • Assessing the likelihood of identified threats and vulnerabilities • Determining the risks associated with the information assets • Addressing the associated risks • Identified for each identified vulnerability Risks identified as a part of the risk assessment process are addressed using one of the following strategies: • Avoid the risk • Mitigate the risk • Transfer the risk • Accept the risk Management develops risk mitigation strategies to address risks identified during the risk assessment process. An IDS and IPS are utilized to analyze network events and report possible or actual network security breaches. FIM software is in place to ensure only authorized changes are deployed into the production environment. The FIM software is configured to notify key IT personnel via e-mail alert when a change to the production application code files is detected. Antivirus software is installed on workstations to detect and prevent the transmission of data or files that contain certain virus signatures recognized by the antivirus software. Internal and external vulnerability scans are performed on at least an annual basis and remedial actions are taken where necessary. A firewall is in place to filter unauthorized inbound network traffic from the internet. The firewall system is configured to deny any type of network connection that is not explicitly authorized by a firewall system rule.

ADMINISTRATIVE SAFEGUARDS		
Ref	**Regulation**	**Control Activity Specified by the Service Organization**
164.308 (a)(1)(ii)(C)	**Sanction policy:** Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity or business associate.	Sanction policies, which include warnings, suspension termination, and layoffs are in place for employee misconduct.
164.308 (a)(1)(ii)(D)	**Information system activity review:** Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.	Documented policies and procedures are in place regarding system settings, authentication, access, and security monitoring.
	Network	
		Network audit logging settings are in place that include: • Account logon events • Account management • Directory service access • Logon events • Object access • Policy change • Privilege use • Process tracking • System events • Security system extension • System integrity • IPsec driver • Other system events • Security state change Network audit logs are maintained and reviewed as needed.
	Operating System	
		Operating system audit logging settings are in place that include: • Account logon events • Account management • Directory service access • Logon events • Object access • Policy change • Privilege use • Process tracking • System events • Security system extension • System integrity • IPsec driver • Other system events • Security state change Operating system audit logs are maintained and reviewed as needed.

ADMINISTRATIVE SAFEGUARDS		
Ref	**Regulation**	**Control Activity Specified by the Service Organization**
	Database	
		Database audit logging settings are in place that include: • Application role change password • Audit change • Backup restore • Broker login • Database change • Database logout • Database ownership change • Database permission change • Database principal change • Database principal impersonation • Database role member change • Failed database authentication • Failed login • Logout • Successful database authentication • Successful login • User change password Database audit logs are maintained and reviewed as needed.
	Application	
		Application audit policy settings are in place that include: • Account logon events • Account activity • Account logoff events • Account management • System events Application audit logs are maintained and reviewed as needed.
164.308 (a)(2)	**Assigned security responsibility:** Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the covered entity or business associate.	Responsibility for the development, implementation, and regular maintenance of the policies and procedures that govern the security of protected ePHI is formally documented and assigned to the privacy or HIPAA officer.
164.308 (a)(3)(i)	**Workforce security:** Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, as provided under the Information Access Management standard and to prevent those who do not have appropriate access from obtaining access to ePHI. Policies and procedures should include Authorization and/or Supervision procedures, Workforce Clearance Procedure, and Termination Procedures.	An inventory of system assets and components is maintained to classify and manage the information assets.

ADMINISTRATIVE SAFEGUARDS		
Ref	**Regulation**	**Control Activity Specified by the Service Organization**
		Privileged access to sensitive resources is restricted to authorized personnel. Documented policies and procedures are in place regarding system settings, access, and security monitoring. The entity restricts access to its environment using the following mechanisms: • Port restrictions (via firewall rule settings) • Access protocol restrictions (via firewall rule settings) • User identification • Digital certifications
164.308 (a)(3)(ii)(A)	**Authorization and/or supervision:** Implement procedures for the authorization and/or supervision of workforce members who work with electronic protected health information or in locations where it might be accessed.	Logical access to systems is approved and granted to an employee as a component of the hiring process. An inventory of system assets and components is maintained to classify and manage the information assets. Privileged access to sensitive resources is restricted to authorized personnel. Logical access to systems is revoked as a component of the termination process.
164.308 (a)(3)(ii)(B)	**Workforce clearance procedure:** Implement procedures to determine that the access of a workforce member to electronic protected health information is appropriate.	Privileged access to sensitive resources is restricted to authorized personnel. The entity restricts access to its environment using the following mechanisms: • Port restrictions (via firewall rule settings) • Access protocol restrictions (via firewall rule settings) • User identification • Digital certifications
164.308 (a)(3)(ii)(C)	**Termination procedures:** Implement procedures for terminating access to electronic protected health information when the employment of, or other arrangement with, a workforce member ends or as required by determinations made as specified in paragraph (a)(3)(ii)(B) [the Workforce Clearance Procedure] of this section.	Logical access to systems is revoked as a component of the termination process. Privileged access to sensitive resources is restricted to authorized personnel.
164.308 (a)(4)(i)	**Information access management:** Implement policies and procedures for authorizing access to electronic protected health information that are consistent with the applicable requirements of the Privacy Rule. Policies and procedures should include: Isolating Health Care Clearinghouse Functions, Access Authorization and Access Establishment and Modification.	Procedures that specify the proper functions, processes, and appropriate environments of information systems that access ePHI are in place. Logical access to systems is approved and granted to an employee as a component of the hiring process.

ADMINISTRATIVE SAFEGUARDS		
Ref	**Regulation**	**Control Activity Specified by the Service Organization**
164.308 (a)(4)(ii)(A)	**Isolating healthcare clearinghouse functions:** If a health care clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the electronic protected health information of the clearinghouse from unauthorized access by the larger organization.	Not Applicable. The entity is not a healthcare clearinghouse.
164.308 (a)(4)(ii)(B)	**Access authorization:** Implement policies and procedures for granting access to ePHI, for example, through access to a workstation, transaction, program, process, or other mechanism.	Logical access to systems is approved and granted to an employee as a component of the hiring process. Privileged access to sensitive resources is restricted to authorized personnel.
164.308 (a)(4)(ii)(C)	**Access establishment and modification:** Implement policies and procedures that, based upon the covered entity's or the business associate's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process.	Documented policies and procedures are in place regarding system settings, access, and security monitoring. Privileged access to sensitive resources is restricted to authorized personnel. Logical access to systems is approved and granted to an employee as a component of the hiring process. Logical access to systems is revoked as a component of the termination process.
164.308 (a)(5)(i)	**Security awareness and training:** Implement a security awareness and training program for all members of the workforce (including management). Component of the Security Awareness and Training program should include Security Reminders, Protection Malicious Software, Log-in Monitoring and Password Management.	Executive management uses an outside vendor to assist with its continued training of employees. Employees are required to attend continued training quarterly that relates to their job role and responsibilities. Upon hire, employees are required to read and acknowledge the information security policies and procedures and complete information security and awareness training. Current employees are required to read and acknowledge the information security policies and procedures and complete information security and awareness training on an annual basis.
164.308 (a)(5)(ii)(A)	**Security reminders:** Periodic security updates.	Users are made aware of security updates and updates to security policies.
164.308 (a)(5)(ii)(B)	**Protection from malicious software:** Procedures for guarding against, detecting, and reporting malicious software.	Policies and procedures are formally documented regarding preventing, detecting, and reporting the presence of malicious software. Antivirus software is installed on workstations to detect and prevent the transmission of data or files that contain certain virus signatures recognized by the antivirus software.
164.308 (a)(5)(ii)(C)	**Log-in monitoring:** Procedures for monitoring log-in attempts and reporting discrepancies.	Documented policies and procedures are in place regarding system settings, authentication, access, and security monitoring.

ADMINISTRATIVE SAFEGUARDS		
Ref	**Regulation**	**Control Activity Specified by the Service Organization**
	Network	
		Network audit logging settings are in place that include: • Account logon events • Account management • Directory service access • Logon events • Object access • Policy change • Privilege use • Process tracking • System events • Security system extension • System integrity • IPsec driver • Other system events • Security state change Network audit logs are maintained and reviewed as needed.
	Operating System	
		Operating system audit logging settings are in place that include: • Account logon events • Account management • Directory service access • Logon events • Object access • Policy change • Privilege use • Process tracking • System events • Security system extension • System integrity • IPsec driver • Other system events • Security state change Operating system audit logs are maintained and reviewed as needed.

ADMINISTRATIVE SAFEGUARDS		
Ref	**Regulation**	**Control Activity Specified by the Service Organization**
	Database	
		Database audit logging settings are in place that include: • Application role change password • Audit change • Backup restore • Broker login • Database change • Database logout • Database ownership change • Database permission change • Database principal change • Database principal impersonation • Database role member change • Failed database authentication • Failed login • Logout • Successful database authentication • Successful login • User change password Database audit logs are maintained and reviewed as needed.
	Application	
		Application account lockout settings are in place that include: • Account lockout trigger Application audit policy settings are in place that include: • Account logon events • Account activity • Account logoff events • Account management • System events Application audit logs are maintained and reviewed as needed.
164.308 (a)(5)(ii)(D)	**Password management:** Procedures for creating, changing, and safeguarding passwords.	Policies are in place to guide personnel in creating, changing, and safeguarding passwords.
	Network	
		Networks are configured to enforce password requirements that include: • Password history • Password age • Password length • Complexity

ADMINISTRATIVE SAFEGUARDS		
Ref	**Regulation**	**Control Activity Specified by the Service Organization**
	Operating System	
		Operating systems are configured to enforce password requirements that include: • Password history • Password age • Password length • Complexity
	Database	
		Databases are configured to enforce password requirements that include: • Password history • Password age • Password length • Complexity
	Application	
		The application is configured to enforce password requirements that include: • Password age • Password length • Complexity
164.308 (a)(6)(i)	**Security incident procedures:** Implement policies and procedures to address security incidents. Policies and procedures should include response reporting.	Documented incident response and escalation procedures for reporting security incidents are in place to guide users in identifying, reporting and mitigating failures, incidents, concerns, and other complaints. Incidents are documented and tracked in a standardized ticketing system and updated to reflect the planned incident and problem resolution.
164.308 (a)(6)(ii)	**Response and reporting:** Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity or business associate; and document security incidents and their outcomes.	Documented incident response and escalation procedures for reporting security incidents are in place to guide users in identifying, reporting and mitigating failures, incidents, concerns, and other complaints. Identified incidents are analyzed, classified and prioritized based on threat level to determine the appropriate response strategy, including step by step procedures. Incidents are documented and tracked in a standardized ticketing system and updated to reflect the planned incident and problem resolution. Resolution of incidents are documented within the ticket and communicated to affected users.

ADMINISTRATIVE SAFEGUARDS		
Ref	**Regulation**	**Control Activity Specified by the Service Organization**
164.308 (a)(7)(i)	**Contingency plan:** Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain ePHI.	A documented disaster recovery plan is in place to guide personnel in the event of an emergency. The disaster recovery plan is tested on an annual basis.
164.308 (a)(7)(ii)(A)	**Data backup plan:** Establish and implement procedures to create and maintain retrievable exact copies of ePHI.	Data backup policies and procedures are formally documented. Incremental backups of certain application and database components are performed on a daily basis.
164.308 (a)(7)(ii)(B)	**Disaster recovery plan:** Establish (and implement as needed) procedures to restore any loss of data.	A documented disaster recovery plan is in place to guide personnel in the event of an emergency. The disaster recovery plan is tested on an annual basis. Data backup restoration tests are performed on an annual basis.
164.308 (a)(7)(ii)(C)	**Emergency Mode Operation Plan:** Establish and implement procedures to enable continuation of critical business processes for protection of the security of ePHI while operating in emergency mode.	A documented disaster recovery plan is in place to guide personnel in the event of an emergency. The disaster recovery plan is tested on an annual basis.
164.308 (a)(7)(ii)(D)	**Testing and revision procedures:** Implement procedures for periodic testing and revision of contingency plans.	A documented disaster recovery plan is in place to guide personnel in the event of an emergency. The disaster recovery plan is tested on an annual basis. Data backup restoration tests are performed on an annual basis.
164.308 (a)(7)(ii)(E)	**Applications and data criticality analysis:** Assess the relative criticality of specific applications and data in support of another contingency plan component.	A documented disaster recovery plan is in place to guide personnel in the event of an emergency. The disaster recovery plan is tested on an annual basis. Data backup restoration tests are performed on an annual basis.
164.308 (a)(8)	**Evaluation:** Perform a periodic technical and nontechnical evaluation based initially upon the standards implemented under this rule and subsequently, in response to environmental or operations changes affecting the security of ePHI, that establishes the extent to which an entity's security policies and procedures meet the requirement.	A documented disaster recovery plan is in place to guide personnel in the event of an emergency. The disaster recovery plan is tested on an annual basis. Internal and external vulnerability scans are performed on at least an annual basis and remedial actions are taken where necessary.

ADMINISTRATIVE SAFEGUARDS		
Ref	**Regulation**	**Control Activity Specified by the Service Organization**
164.308 (b)(1)	**Business associate contracts and other arrangements:** A covered entity, in accordance with 164.306 [The Security Standards: General Rules], may permit a business associate to create, receive, maintain, or transmit ePHI on the covered entity's behalf only if the covered entity obtains satisfactory assurances, in accordance with 164.314 [the Organization Requirements] that the business associate will appropriately safeguard the information.	Not Applicable. The entity is not a covered entity.
164.308 (b)(2)	A business associate may permit a business that is a subcontractor to create, receive, maintain, or transmit ePHI on its behalf only if the business associate obtains satisfactory assurances, in accordance with §164.314(a), that the subcontractor will appropriately safeguard the information.	The entity maintains business associate agreements with businesses that create, receive maintain, or transmit ePHI.
164.308 (b)(3)	**Written contract or other arrangement:** Document the satisfactory assurances required by paragraph (b)(1) or (b2) above of this section through a written or other arrangement with the business associate that meets the applicable requirements of 164.314(a) [the Organizational Requirements].	The entity maintains business associate agreements with businesses that create, receive maintain, or transmit ePHI.
164.308 (b)(4)	**Arrangement:** Document the satisfactory assurances required by paragraph (b)(1) [the Business Associates Contracts and Other Arrangements] of this section through a written or other arrangement with the business associate that meets the applicable requirements of 164.314(a).	The entity maintains business associate agreements with businesses that create, receive maintain, or transmit ePHI.

PHYSICAL SAFEGUARDS		
Ref	**Regulation**	**Control Activity Specified by the Service Organization**
164.310 (a)(1)	**Facility access controls:** Implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.	The controls related to this regulation are the responsibility of the subservice organization. Refer to the Subservice Organizations section above for controls managed by the subservice organization.
164.310 (a)(2)(i)	**Contingency operations:** Establish (and implement as needed) procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency.	A documented disaster recovery plan is in place to guide personnel in the event of an emergency. The disaster recovery plan is tested on an annual basis. Data backup restoration tests are performed on an annual basis.
164.310 (a)(2)(ii)	**Facility security plan:** Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.	The controls related to this regulation are the responsibility of the subservice organization. Refer to the Subservice Organizations section above for controls managed by the subservice organization.
164.310 (a)(2)(iii)	**Access control and validation procedures:** Implement procedures to control and validate a person's access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision.	Documented policies and procedures are in place regarding system settings, access, and security monitoring. Additional controls related to this regulation are the responsibility of the subservice organization. Refer to the Subservice Organizations section above for controls managed by the subservice organization.
164.310 (a)(2)(iv)	**Maintenance records:** Implement policies and procedures to document repairs and modifications to the physical components of a facility which are related to security (for example, hardware, walls, doors, and locks).	Policies and procedures are in place to guide personnel in purging data off of machines prior to sending them to Google Cloud/OVH to destroy. An inventory of system assets and components is maintained to classify and manage the information assets. The entity purges servers and hardware when they are no longer rendered applicable for business purposes. Additional controls related to this regulation are the responsibility of the subservice organization. Refer to the Subservice Organizations section above for controls managed by the subservice organization.
164.310 (b)	**Workstation use:** Implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access ePHI.	Procedures that specify the proper functions, processes, and appropriate environments of information systems that access ePHI are in place.
164.310 (c)	**Workstation security:** Covered entities should implement physical safeguards for all workstations that access ePHI, to restrict access to authorized users.	Procedures that specify the proper functions, processes, and appropriate environments of information systems that access ePHI are in place.

PHYSICAL SAFEGUARDS		
Ref	**Regulation**	**Control Activity Specified by the Service Organization**
164.310 (d)(1)	**Device and media control:** Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain ePHI into and out of a facility, and the movement of these items within the facility.	Policies and procedures are in place to guide personnel in purging data off of machines prior to sending them to Google Cloud/OVH to destroy. An inventory of system assets and components is maintained to classify and manage the information assets. The entity purges servers and hardware when they are no longer rendered applicable for business purposes.
164.310 (d)(2)(i)	**Disposal:** Implement policies and procedures to address the final disposition of ePHI, and/or the hardware or electronic media on which it is stored.	Policies and procedures are in place to guide personnel in purging data off of machines prior to sending them to Google Cloud/OVH to destroy. An inventory of system assets and components is maintained to classify and manage the information assets. The entity purges servers and hardware when they are no longer rendered applicable for business purposes.
164.310 (d)(2)(ii)	**Media re-use:** Implement procedures for removal of ePHI from electronic media before the media are made available for re-use. Ensure that ePHI previously stored on electronic media cannot be accessed and reused. Identify removable media and their use. Ensure that ePHI is removed from reusable media before they are used to record new information.	Policies and procedures are in place to guide personnel in purging data off of machines prior to sending them to Google Cloud/OVH to destroy. An inventory of system assets and components is maintained to classify and manage the information assets. The entity purges servers and hardware when they are no longer rendered applicable for business purposes.
164.310 (d)(2)(iii)	**Accountability:** Maintain a record of the movements of hardware and electronic media and any person responsible therefore.	Policies and procedures are in place to guide personnel in purging data off of machines prior to sending them to Google Cloud/OVH to destroy. An inventory of system assets and components is maintained to classify and manage the information assets.
164.310 (d)(2)(iv)	**Data backup and storage:** Create a retrievable, exact copy of ePHI, when needed, before movement of equipment.	Data backup policies and procedures are formally documented. Data backup restoration tests are performed on an annual basis.

TECHNICAL SAFEGUARDS		
Ref	**Regulation**	**Control Activity Specified by the Service Organization**
164.312 (a)(1)	**Access control:** Implement technical policies and procedures for electronic information systems that maintain ePHI to allow access only to those persons or software programs that have been granted access rights as specified in §164.308(a)(4) [Information Access Management].	Documented policies and procedures are in place regarding system settings, authentication, access, and security monitoring. Privileged access to sensitive resources is restricted to authorized personnel. Logical access to systems is approved and granted to an employee as a component of the hiring process. Logical access to systems is revoked as a component of the termination process.
	Network	
		Networks are configured to enforce password requirements that include: • Password history • Password age • Password length • Complexity Network administrative access is restricted to user accounts accessible by the following personnel: • CTO • VP of Tech Services & Support
	Operating System	
		Operating system user access is restricted via role-based security privileges defined within the access control system. Operating system administrative access is restricted to user accounts accessible by the following personnel: • CTO • VP of Tech Services & Support Operating systems are configured to enforce password requirements that include: • Password history • Password age • Password length • Complexity
	Database	
		Databases are configured to enforce password requirements that include: • Password history • Password age • Password length • Complexity

TECHNICAL SAFEGUARDS		
Ref	**Regulation**	**Control Activity Specified by the Service Organization**
		Database administrative access is restricted to user accounts accessible by the following personnel: • President/CEO • CTO
	Application	
164.312 (a)(2)(i)	**Unique user identification:** Assign a unique name and/or number for identifying and tracking user identity. Ensure that system activity can be traced to a specific user. Ensure that the necessary data is available in the system logs to support audit and other related business functions.	The application is configured to enforce password requirements that include: • Password age • Password length • Complexity Application administrative access is restricted to user accounts accessible by the following personnel: • CTO • VP of Tech Services & Support • Senior Product Specialist Documented policies and procedures are in place regarding system settings, authentication, access, and security monitoring.
	Network	
		Network administrative access is restricted to user accounts accessible by the following personnel: • CTO • VP of Tech Services & Support Networks are configured to enforce password requirements that include: • Password history • Password age • Password length • Complexity Network account lockout settings are in place that include: • Account lockout duration • Account lockout threshold • Account lockout counter reset

TECHNICAL SAFEGUARDS		
Ref	**Regulation**	**Control Activity Specified by the Service Organization**
		Network audit logging settings are in place that include: • Account logon events • Account management • Directory service access • Logon events • Object access • Policy change • Privilege use • Process tracking • System events • Security system extension • System integrity • IPsec driver • Other system events • Security state change Network audit logs are maintained and reviewed as needed.
	Operating System	
		Operating system administrative access is restricted to user accounts accessible by the following personnel: • CTO • VP of Tech Services & Support Operating systems are configured to enforce password requirements that include: • Password history • Password age • Password length • Complexity Operating system account lockout settings are in place that include: • Account lockout duration • Account lockout threshold • Account lockout counter reset

TECHNICAL SAFEGUARDS		
Ref	**Regulation**	**Control Activity Specified by the Service Organization**
		Operating system audit logging settings are in place that include: • Account logon events • Account management • Directory service access • Logon events • Object access • Policy change • Privilege use • Process tracking • System events • Security system extension • System integrity • IPsec driver • Other system events • Security state change Operating system audit logs are maintained and reviewed as needed.
	Database	
		Database administrative access is restricted to user accounts accessible by the following personnel: • President/CEO • CTO Databases are configured to enforce password requirements that include: • Password history • Password age • Password length • Complexity Database account lockout settings are in place that include: • Account lockout duration • Account lockout threshold • Account lockout counter reset

TECHNICAL SAFEGUARDS		
Ref	**Regulation**	**Control Activity Specified by the Service Organization**
		Database audit logging settings are in place that include: • Application role change password • Audit change • Backup restore • Broker login • Database change • Database logout • Database ownership change • Database permission change • Database principal change • Database principal impersonation • Database role member change • Failed database authentication • Failed login • Logout • Successful database authentication • Successful login • User change password Database audit logs are maintained and reviewed as needed.
	Application	
		Application administrative access is restricted to user accounts accessible by the following personnel: • CTO • VP of Tech Services & Support • Senior Product Specialist The application is configured to enforce password requirements that include: • Password age • Password length • Complexity Application account lockout settings are in place that include: • Account lockout trigger Application audit policy settings are in place that include: • Account logon events • Account activity • Account logoff events • Account management • System events Application audit logs are maintained and reviewed as needed.

TECHNICAL SAFEGUARDS		
Ref	**Regulation**	**Control Activity Specified by the Service Organization**
164.312 (a)(2)(ii)	**Emergency access procedure:** Establish (and implement as needed) procedures for obtaining necessary ePHI during an emergency.	A documented disaster recovery plan is in place to guide personnel in the event of an emergency. The disaster recovery plan is tested on an annual basis.
164.312 (a)(2)(iii)	**Automatic logoff:** Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.	Workstations are configured to terminate inactive sessions after five minutes of inactivity. Users are required to re-validate with a username and password to gain control of the workstation.
164.312 (a)(2)(iv)	**Encryption and decryption:** Implement a mechanism to encrypt and decrypt ePHI.	Server certificate-based authentication is used as part of the TLS encryption with a trusted certificate authority.
164.312 (b)	**Audit controls:** Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use ePHI.	Documented policies and procedures are in place regarding system settings, authentication, access, and security monitoring. FIM software is in place to ensure only authorized changes are deployed into the production environment. The FIM software is configured to notify key IT personnel via e-mail alert when a change to the production application code files is detected.
	Network	
		Network audit logging settings are in place that include: • Account logon events • Account management • Directory service access • Logon events • Object access • Policy change • Privilege use • Process tracking • System events • Security system extension • System integrity • IPsec driver • Other system events • Security state change Network audit logs are maintained and reviewed as needed.

TECHNICAL SAFEGUARDS		
Ref	**Regulation**	**Control Activity Specified by the Service Organization**
	Operating System	
		Operating system audit logging settings are in place that include: • Account logon events • Account management • Directory service access • Logon events • Object access • Policy change • Privilege use • Process tracking • System events • Security system extension • System integrity • IPsec driver • Other system events • Security state change Operating system audit logs are maintained and reviewed as needed.
	Database	
		Database audit logging settings are in place that include: • Application role change password • Audit change • Backup restore • Broker login • Database change • Database logout • Database ownership change • Database permission change • Database principal change • Database principal impersonation • Database role member change • Failed database authentication • Failed login • Logout • Successful database authentication • Successful login • User change password Database audit logs are maintained and reviewed as needed.
	Application	
		Application audit policy settings are in place that include: • Account logon events • Account activity • Account logoff events • Account management • System events

TECHNICAL SAFEGUARDS		
Ref	**Regulation**	**Control Activity Specified by the Service Organization**
		Application audit logs are maintained and reviewed as needed.
164.312 (c)(1)	**Integrity:** Implement policies and procedures to protect ePHI from improper alteration or destruction.	Server certificate-based authentication is used as part of the TLS encryption with a trusted certificate authority. FIM software is in place to ensure only authorized changes are deployed into the production environment. The FIM software is configured to notify key IT personnel via e-mail alert when a change to the production application code files is detected.
164.312 (c)(2)	**Mechanisms to authenticate ePHI:** Implement electronic mechanisms to corroborate that ePHI has not been altered or destroyed in an unauthorized manner.	Server certificate-based authentication is used as part of the TLS encryption with a trusted certificate authority. FIM software is in place to ensure only authorized changes are deployed into the production environment. The FIM software is configured to notify key IT personnel via e-mail alert when a change to the production application code files is detected.
164.312 (d)	**Person or entity authentication:** Implement procedures to verify that a person or entity seeking access to ePHI is the one claimed.	Documented policies and procedures are in place regarding system settings, authentication, access, and security monitoring.
	Network	
		Networks are configured to enforce password requirements that include: • Password history • Password age • Password length • Complexity
	Operating System	
		Operating systems are configured to enforce password requirements that include: • Password history • Password age • Password length • Complexity
	Database	
		Databases are configured to enforce password requirements that include: • Password history • Password age • Password length • Complexity

TECHNICAL SAFEGUARDS		
Ref	**Regulation**	**Control Activity Specified by the Service Organization**
	Application	
		The application is configured to enforce password requirements that include: • Password age • Password length • Complexity
164.312 (e)(1)	**Transmission security:** Implement technical security measures to guard against unauthorized access to ePHI that is being transmitted over an electronic communications network.	Server certificate-based authentication is used as part of the TLS encryption with a trusted certificate authority. A firewall is in place to filter unauthorized inbound network traffic from the internet. The firewall system is configured to deny any type of network connection that is not explicitly authorized by a firewall system rule.
164.312 (e)(2)(i)	**Integrity controls:** Implement security measures to ensure that electronically transmitted ePHI is not improperly modified without detection until disposed of.	Server certificate-based authentication is used as part of the TLS encryption with a trusted certificate authority. A firewall is in place to filter unauthorized inbound network traffic from the internet. The firewall system is configured to deny any type of network connection that is not explicitly authorized by a firewall system rule.
164.312 (e)(2)(ii)	**Encryption:** Implement a mechanism to encrypt ePHI whenever deemed appropriate.	Server certificate-based authentication is used as part of the TLS encryption with a trusted certificate authority. Critical data is stored in encrypted format using software supporting the AES.

ORGANIZATIONAL REQUIREMENTS		
Ref	**Regulation**	**Control Activity Specified by the Service Organization**
164.314 (a)(1)	**Business associate contracts or other arrangements:** A covered entity is not in compliance with the standards in § 164.502(e) if the covered entity knew of a pattern of an activity or practice of the business associate that constituted a material breach or violation of the business associate's obligation under the contract or other arrangement, unless the covered entity took reasonable steps to cure the breach or end the violation, as applicable, and, if such steps were unsuccessful - (A) Terminated the contract or arrangement, if feasible; or (B) If termination is not feasible, reported the problem to the Secretary."	The entity maintains business associate agreements with businesses that create, receive maintain, or transmit ePHI. The business associate agreements communicate: • The boundaries of the system • System commitments and requirements • Terms, conditions and responsibilities between the involved parties
164.314 (a)(2)(i)	**Business Associate Contracts:** A business associate contract must provide that the business associate will: "Implement safeguards that protect the confidentiality, integrity, and availability of the electronic protected health…; Report to the covered entity any security incident of which it becomes aware; Authorize termination of the contract, if the covered entity determines that the business associate has violated a material term of the contract."	The entity maintains business associate agreements with businesses that create, receive maintain, or transmit ePHI. The business associate agreements communicate: • The boundaries of the system • System commitments and requirements • Terms, conditions and responsibilities between the involved parties
164.314 (a)(2)(ii)	**Other Arrangement:** The Other Arrangements implementation specifications provide that when a covered entity and its business associate are both government entities, the covered entity may comply with the standard in either of two alternative ways: (1) if it enters into a memorandum of understanding (MOU) with the business associate and the MOU contains terms which accomplish the objectives of the Business Associate Contracts section of the Security Rule; or (2) if other law (including regulations adopted by the covered entity or its business associate) contain requirements applicable to the business associate that accomplish the objectives of the business associate contract.	Not Applicable. The entity is not a government entity.
164.314 (b)(1)	**Requirements for Group Health Plans:** Except when the only ePHI disclosed to a plan sponsor is disclosed pursuant to §164.504(f)(1)(ii) or (iii), or as authorized under §164.508, a group health plan must ensure that its plan documents provide that the plan sponsor will reasonably and appropriately safeguard ePHI created, received, maintained, or transmitted to or by the plan sponsor on behalf of the group health plan.	Not Applicable. The entity is not a plan sponsor.

ORGANIZATIONAL REQUIREMENTS		
Ref	**Regulation**	**Control Activity Specified by the Service Organization**
164.314 (b)(2)	**Implementation Specifications:** The plan documents of the group health plan must be amended to incorporate provisions to require the plan sponsor to— (i) Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the ePHI that it creates, receives, maintains, or transmits on behalf of the group health plan; (ii) Ensure that the adequate separation required by §164.504(f)(2)(iii) is supported by reasonable and appropriate security measures; (iii) Ensure that any agent, including a subcontractor, to whom it provides this information agrees to implement reasonable and appropriate security measures to protect the information; and (iv) Report to the group health plan any security incident of which it becomes aware.	Not Applicable. The entity is not a plan sponsor.
164.316 (a)	**Policies and Procedures:** Implement reasonable and appropriate policies and procedures to comply with the standards, implementation specifications, or other requirements of this subpart, taking into account those factors specified in 164.306(b)(2)(i), (ii), (iii), and (iv) [the Security Standards: General Rules, Flexibility of Approach]. This standard is not to be construed to permit or excuse an action that violates any other standard. A covered entity or business associate may change its policies and procedures at any time, provided that the changes are documented and are implemented in accordance with this subpart.	The entity creates and implements appropriate policies and procedures as required by applicable legislations, regulators, and customers. Policies and procedures are reviewed annually and updated, if necessary, and distributed, or otherwise made available to personnel.
164.316 (b)(1)	**Documentation:** Maintain the policies and procedures implemented to comply with this subpart in written (which may be electronic) form; and (ii) if an action, activity or assessment is required by this subpart to be documented, maintain a written (which may be electronic) record of the action, activity, or assessment.	Policies and procedures are appropriately retained for a minimum of six (6) years from the date it was created or when it was last in effect, whichever is later. Policies and procedures are reviewed annually and updated, if necessary, and distributed, or otherwise made available to personnel. Policies and procedures are created and maintained in written and electronic form.
164.316 (b)(1)(ii)	**Documentation:** if an action, activity or assessment is required by this subpart to be documented, maintain a written (which may be electronic) record of the action, activity, or assessment.	HIPAA related incidents and events are documented in a ticketing system.

ORGANIZATIONAL REQUIREMENTS		
Ref	**Regulation**	**Control Activity Specified by the Service Organization**
164.316 (b)(2)(i)	**Time Limit:** Retain the documentation required by paragraph (b) (1) of this section for 6 years for the date of its creation or the date when it last was in effect, whichever is later.	Policies and procedures are appropriately retained for a minimum of six (6) years from the date it was created or when it was last in effect, whichever is later.
164.316 (b)(2)(ii)	**Availability:** Make documentation available to those persons responsible for implementing the procedures to which the documentation pertains.	Policies and procedures are reviewed annually and updated, if necessary, and distributed, or otherwise made available to personnel.
164.316 (b)(2)(iii)	**Updates:** Review documentation periodically, and update as needed, in response to environmental or operational changes affecting the security of the ePHI.	Policies and procedures are reviewed annually and updated, if necessary, and distributed, or otherwise made available to personnel.

BREACH NOTIFICATION		
Ref	**Regulation**	**Control Activity Specified by the Service Organization**
164.402	Breach means the acquisition, access, use, or disclosure of protected health information in a manner not permitted under subpart E of this part which compromises the security or privacy of the protected health information. (1)(i) For purposes of this definition, compromises the security or privacy of the protected health information means poses a significant risk of financial, reputational, or other harm to the individual. (ii) A use or disclosure of protected health information that does not include the identifiers listed at §164.514(e)(2), date of birth, and zip code does not compromise the security or privacy of the protected health information.	Breach notification letters or e-mails are developed and prepared to be used during a breach of ePHI.
164.404 (a)	A covered entity shall, following the discovery of a breach of unsecured protected health information, notify each individual whose unsecured protected health information has been, or is reasonably believed by the covered entity to have been, accessed, acquired, used or disclosed as a result of such breach.	Not Applicable. The entity is a business associate; its responsibilities for breach notification are limited to its covered entity customers.
164.404 (2)	For purposes of paragraph (a)(1) of this section, §§ 164.406(a), and 164.408(a), a breach shall be treated as discovered by a covered entity as of the first day on which such breach is known to the covered entity, or, by exercising reasonable diligence would have been known to the covered entity. A covered entity shall be deemed to have knowledge of a breach if such breach is known, or by exercising reasonable diligence would have been known, to any person, other than the person committing the breach, who is a workforce member or agent of the covered entity (determined in accordance with the federal common law of agency).	Not Applicable. The entity is a business associate; its responsibilities for breach notification are limited to its covered entity customers.
164.404 (b)	Except as provided in §164.412, a covered entity shall provide the notification required by paragraph (a) of this section without unreasonable delay and in no case later than 60 days after discovery of a breach.	Not Applicable. The entity is a business associate; its responsibilities for breach notification are limited to its covered entity customers.

BREACH NOTIFICATION		
Ref	**Regulation**	**Control Activity Specified by the Service Organization**
164.404 (c)(1)	Elements of the notification required by paragraph (a) of this section shall include to the extent possible: (A) a brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known; (B) a description of the types of unsecured protected health information that were involved in the breach (Such as whether full name, social security number, date of birth, home address, account number, diagnosis, disability code, or other types of information were involved); (C) any steps the individual should take to protect themselves from potential harm resulting from the breach; (D) a brief description of what the covered entity is doing to investigation the breach, to mitigate harm to individuals, and to protect against further breaches; and (E) contact procedures for individuals to ask questions or learn additional information which should include a toll-free number, an e-mail address, website, or postal address.	Not Applicable. The entity is a business associate; its responsibilities for breach notification are limited to its covered entity customers.
164.404 (c)(2)	The notification required by paragraph (a) of this section shall be written in plain language.	Not Applicable. The entity is a business associate; its responsibilities for breach notification are limited to its covered entity customers.
164.404 (d)(1)(i)	The notification required by paragraph (a) shall be provided in the following form: Written notification by first-class mail to the individual at the last known address of the individual or, if the individual agrees to electronic notice and such agreement has not been withdrawn, by electronic mail. The notification may be provided in one or more mailings as more information becomes available.	Not Applicable. The entity is a business associate; its responsibilities for breach notification are limited to its covered entity customers.
164.404 (d)(1)(ii)	The notification required by paragraph (a) shall be provided in the following form: If the covered entity knows the individual is deceased and has the address of the next of kin or personal representative of the individual (as specified under §164.502(g)(4) of subpart E), written notification by first-class mail to either the next of kin or personal representative of the individual. The notification may be provided in one or more mailings as information is available.	Not Applicable. The entity is a business associate; its responsibilities for breach notification are limited to its covered entity customers.

BREACH NOTIFICATION		
Ref	**Regulation**	**Control Activity Specified by the Service Organization**
164.404 (d)(2)	**Substitute notice**. In the case where there is insufficient or out-of-date contact information that precludes written notification to the individual under this paragraph (d)(1)(i) of this section, a substitute form of notice reasonable calculated to reach the individual shall be provided. Substitute notice need not be provided in the case in which there is insufficient or out-of-date contact information that precludes written notification to the next of kin or personal representative of the individual under paragraph (d)(1)(ii).	Not Applicable. The entity is a business associate; its responsibilities for breach notification are limited to its covered entity customers.
164.404 (d)(2)(i)	In the case where there is insufficient or out-of-date contact information for fewer than 10 individuals, then substitute notice may be provided by an alternative form of written notice, telephone or other means.	Not Applicable. The entity is a business associate; its responsibilities for breach notification are limited to its covered entity customers.
164.404 (d)(2)(ii)	In the case in which there is insufficient or out-of-date contact information for 10 or more individuals, then such substitute notice shall: (A) be in the form of either a conspicuous posting for a period of 90 days on the home page of the web site of the covered entity involved, or conspicuous notice in a major print or broadcast media in geographic areas where the individuals affected by the breach likely reside; and (B) include a toll-free number that remains active for at least 90 days where an individual can learn whether the individual's secured protected health information may be included in the breach.	Not Applicable. The entity is a business associate; its responsibilities for breach notification are limited to its covered entity customers.
164.404 (d)(3)	In any case deemed by the covered entity to require urgency because of possible imminent misuse of unsecured protected health information, the covered entity may provide information to individuals by telephone or other means, as appropriate, in addition to notice provided under paragraph (d)(1) of this section.	Not Applicable. The entity is a business associate; its responsibilities for breach notification are limited to its covered entity customers.
164.406	§164.406(a) For a breach of unsecured protected health information involving more than 500 residents of a State or jurisdiction, a covered entity shall, following the discovery of the breach, notify prominent media outlets serving the State or jurisdiction. (b) Except as provided in §164.412, a covered entity shall provide the notification required by paragraph (a) of this section without unreasonable delay and in no case later than 60 calendar days after discovery of a breach. (c) The content of the notification required by paragraph (a) shall meet the requirements of §164.404(c).	Not Applicable. The entity is a business associate; its responsibilities for breach notification are limited to its covered entity customers.

BREACH NOTIFICATION		
Ref	**Regulation**	**Control Activity Specified by the Service Organization**
164.408 (a)	A covered entity shall, following the discovery of a breach of unsecured protected health information as provided in §164.404(a)(2), notify the Secretary.	Not Applicable. The entity is a business associate; its responsibilities for breach notification are limited to its covered entity customers.
164.408 (b)	For breaches of unsecured protected health information involving 500 or more individuals, a covered entity shall, expect as provided in §164.412, provide the notification required by paragraph (a) contemporaneously with the notice required by §164.404(a) and in the manner specified on the HHS web site.	Not Applicable. The entity is a business associate; its responsibilities for breach notification are limited to its covered entity customers.
164.408 (c)	For breaches of unsecured protected health information involving less than 500 individuals, a covered entity shall maintain a log or other documentation of such breaches and, not later than 60 days after the end of each calendar year, provide the notification required by paragraph (a) of this section for breaches occurring during the preceding calendar year, in a manner specified on the HHS web site.	Not Applicable. The entity is a business associate; its responsibilities for breach notification are limited to its covered entity customers.
164.410 (a)(1)	A business associate shall, following the discovery of a breach of unsecured protected health information, notify the covered entity of such breach.	Breach notification letters or e-mails are developed and prepared to be used during a breach of ePHI.
164.410 (a)(2)	(2) For the purposes of paragraph (1) of this section, a breach shall be treated as discovered by a business associate as of the first day on which such breach is known to the business associate or, by exercising reasonable diligence, would have been known to the business associate. A business associate shall be deemed to have knowledge of a breach if the breach is known, or by exercising reasonable diligence would have been known, to any person, other than the person committing the breach, who is an employee, officer, or other agent of the business associate (determined in accordance with the federal common law of agency).	The entity acknowledges responsibility for notifying affected parties in the event of a breach of unsecured protected health information.
164.410 (b)	Except as provided in §164.412, a business associate shall provide the notification required by paragraph (a) of this section without unreasonable delay and in no case later than 60 calendar days after the discovery of a breach.	The entity notifies affected parties of a breach of ePHI no later than sixty (60) calendar days after the discovery of the breach.
164.410 (c)(1)	The notification required by paragraph (a) of this section shall include, to the extent possible, the identification of each individual whose unsecured protected health information has been, or is reasonably believed by the business associate to have been accessed, acquired, used or disclosure during the breach.	The identification of each individual who's unsecured ePHI has been accessed during the breach is disclosed during notification procedures.

BREACH NOTIFICATION		
Ref	**Regulation**	**Control Activity Specified by the Service Organization**
164.410 (c)(2)	A business associate shall provide the covered entity with any other information that the covered entity is required to include in the notification to the individual under §164.404(c) at the time of the notification required by paragraph (a) of this section or promptly thereafter as information becomes available.	Management provides the covered entity with any information that the covered entity is required to include in the notification to the individual at the time of the breach and as soon as it is available.
164.412	If a law enforcement official states to a covered entity or business associate that a notification, notice or posting required under this subpart would impede a criminal investigation or cause damage to national security, a covered entity or business associate shall: (a) If the statement is in writing and specifies the time for which a delay is required, delay such notification, notice, or posting for the time period specified by the official; or (b) If the statement is made orally, document the statement, including the identity of the official making the statement, and delay the notification, notice, or posting temporarily and no longer than 30 days from the date of the oral statement, unless a written statement as described in paragraph (a) of this section is submitted during that time.	The entity refrains from, or delays notifying HHS personnel, the covered entity, or other required persons following the discovery of a breach of unsecured protected health information when required by law.
164.414	**Administrative requirements and burden of proof**: (a) covered entity is required to comply with the administrative requirements of § 164.530(b), (d), (e), (g), (h), (i), and (j) with respect to the requirements of this subpart. (b) In the event of a use or disclosure in violation of subpart E, the covered entity or business associate; as applicable, shall have the burden of demonstrating that all notifications were made as required by this subpart or that the use or disclosures did not constitute a breach as defined at §164.402. See §164.530 for definition of breach.	The entity acknowledges responsibility for notifying affected parties in the event of a breach of unsecured protected health information.

SECTION 4

INFORMATION PROVIDED BY THE SERVICE AUDITOR

GUIDANCE REGARDING INFORMATION PROVIDED BY THE SERVICE AUDITOR

A-LIGN ASSURANCE's examination of the controls of Chase Data was limited to the Trust Services Criteria and HIPAA/HITECH requirements, related criteria and control activities specified by the management of Chase Data and did not encompass all aspects of Chase Data' operations or operations at user entities. Our examination was performed in accordance with American Institute of Certified Public Accountants (AICPA) AT-C 105 and AT-C 205.

Our examination of the control activities was performed using the following testing methods:

TEST	DESCRIPTION
Inquiry	The service auditor made inquiries of service organization personnel. Inquiries were made to obtain information and representations from the client to determine that the client's knowledge of the control and corroborate policy or procedure information.
Observation	The service auditor observed application of the control activities by client personnel.
Inspection	The service auditor inspected among other items, source documents, reports, system configurations to determine performance of the specified control activity and in some instances the timeliness of the performance of control activities.
Re-performance	The service auditor independently executed procedures or controls that were originally performed by the service organization as part of the entity's internal control.

In determining whether the report meets the user auditor's objectives, the user auditor should perform the following procedures:

- Understand the aspects of the service organization's controls that may affect the service commitments and system requirements based on the applicable trust services criteria;
- Understand the aspects of the service organization's controls that may affect the HIPAA/HITECH requirements;
- Understand the infrastructure, software, procedures and data that are designed, implemented and operated by the service organization;
- Understand the flow of ePHI through the service organization;
- Determine whether the criteria are relevant to the user entity's assertions;
- Determine whether the service organization's controls are suitably designed to provide reasonable assurance that its service commitments and system were achieved based on the applicable trust services criteria; and
- Determine whether the service organization's controls are suitably designed to meet the health information security program of the user entity's and determine whether they have been implemented.