A-LIGN

Profisee Group Inc.

Type 1 SOC 2 with HIPAA/HITECH

2022

Profisee

A-LIGN.COM

REPORT ON PROFISEE GROUP INC.'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

August 9, 2022

Table of Contents

SECTION 1

ASSERTION OF PROFISEE GROUP INC. MANAGEMENT

ASSERTION OF PROFISEE GROUP INC. MANAGEMENT

September 5, 2022

We have prepared the accompanying description of Profisee Group Inc.'s ('Profisee' or 'the Company') Database and File Management Software Services System titled "Profisee Group Inc.'s Description of Its Database and File Management Software Services System as of August 9, 2022" (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 Database and File Management Software Services System that may be useful when assessing the risks arising from interactions with Profisee's system, particularly information about system controls that Profisee 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.

Profisee uses Microsoft Azure ('Azure' or 'subservice organization') to provide cloud computing services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Profisee, to achieve Profisee's service commitments and system requirements based on the applicable trust services criteria and HIPAA/HITECH requirements. The description presents Profisee's controls, the applicable trust services criteria and HIPAA/HITECH requirements, and the types of complementary subservice organization controls assumed in the design of Profisee's controls. The description does not disclose the actual controls at the subservice organization.

The description indicates that complementary user entity controls that are suitably designed are necessary, along with controls at Profisee to achieve Profisee's service commitments and system requirements based on the applicable trust services criteria and HIPAA/HITECH requirements. The description presents Profisee's controls, the applicable trust services criteria and HIPAA/HITECH requirements, and the complementary user entity controls assumed in the design of Profisee's controls.

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

a. the description presents Profisee's Database and File Management Software Services System that was designed and implemented as of August 9, 2022, in accordance with the description criteria.
b. the controls stated in the description were suitably designed as of August 9, 2022, to provide reasonable assurance that Profisee'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 Profisee's controls as of that date.

Nick Powell
CFO
Profisee Group Inc.

SECTION 2

INDEPENDENT SERVICE AUDITOR’S REPORT

INDEPENDENT SERVICE AUDITOR’S REPORT

To: Profisee Group Inc.

Scope

We have examined Profisee’s accompanying description of its Database and File Management Software Services System titled "Profisee Group Inc.’s Description of Its Database and File Management Software Services System as of August 9, 2022” (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 August 9, 2022, to provide reasonable assurance that Profisee’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.

Profisee uses Azure to provide cloud computing services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Profisee, to achieve Profisee’s service commitments and system requirements based on the applicable trust services criteria and HIPAA/HITECH requirements. The description presents Profisee’s controls, the applicable trust services criteria and HIPAA/HITECH requirements, and the types of complementary subservice organization controls assumed in the design of Profisee’s controls. The description does not disclose the actual controls at the subservice organization. Our examination did not include the services provided by the subservice organization, 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 Profisee, to achieve Profisee’s service commitments and system requirements based on the applicable trust services criteria and HIPAA/HITECH requirements. The description presents Profisee’s controls, the applicable trust services criteria and HIPAA/HITECH requirements, and the complementary user entity controls assumed in the design of Profisee’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.

The information included in section 5, "Other Information Provided by The Service Organization” that is not covered by the service auditor’s report, is presented by Profisee management to provide additional information and is not a part of the description. Information about Profisee’s management’s response to testing exceptions has not been subjected to the procedures applied in the examination of the description, the suitability of the design of controls, and the operating effectiveness of the controls to achieve Profisee’s service commitments and system requirements based on the applicable trust services criteria and HIPAA/HITECH requirements.

Service Organization’s Responsibilities

Profisee 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 Profisee’s service commitments and system requirements were achieved. Profisee has provided the accompanying assertion titled "Assertion of Profisee Group Inc. Management" (assertion) about the description and the suitability of the design of controls stated therein. Profisee 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.

Independence and Ethical Responsibilities

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the examination engagement.

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 Profisee’s Database and File Management Software Services System that was designed and implemented as of August 9, 2022, in accordance with the description criteria.
b. the controls stated in the description were suitably designed as of August 9, 2022, to provide reasonable assurance that Profisee’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 Profisee’s controls as of that date.

Restricted Use

This report is intended solely for the information and use of Profisee, user entities of Profisee’s Database and File Management Software Services System as of August 9, 2022, business partners of Profisee subject to risks arising from interactions with the Database and File Management 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
September 5, 2022

SECTION 3

PROFISEE GROUP INC.'S DESCRIPTION OF ITS DATABASE AND FILE MANAGEMENT SOFTWARE SERVICES SYSTEM AS OF AUGUST 9, 2022

OVERVIEW OF OPERATIONS

Company Background

Microsoft developed and released SQL Server Master Data Services (MDS) after acquiring Stratature in 2006. Principals at Stratature then created a new company - Profisee - to help more companies leverage enterprise master data management (MDM). As Microsoft developed its Azure ecosystem of cloud computer, storage, and analytics tools, it ceased development in MDS - and asked Profisee to embrace Azure and move off MDS as a code base in 2017. Profisee continues to elevate the MDM market with a commitment to being fast to deploy and easy to maintain allowing customers to solve their data problems quickly.

Profisee is a Microsoft Gold partner and is levered by firms in Financial Services, Telecommunications, Legal Services, Advertising, Manufacturing, Healthcare, Retail, Educational institutions.

Description of Services Provided

Profisee provides Database and File Management Software services and the Profisee Application to allow for companies to query databases and systems that may otherwise be unable to integrate, update records across these systems and validate data with reputable sources. Profisee additionally allows for data science to evaluate inputs from these systems and data analytics to be applied across unintegrated systems and sources.

Principal Service Commitments and System Requirements

Profisee designs its systems and approach to the product to require as little interaction without outside systems as possible, reducing system exposure and protecting information systems as best as possible. Profisee’s traditional deployment in PaaS and IaaS deployments require no interaction with Profisee Corporate systems to operate, no data is collected or processed by Profisee Corporate with this approach extending to our new SaaS offering where applicable.

Profisee strives to be able to provide the best Master Data Management service with the least interaction from Profisee where possible, this includes limiting exposure of any information to unapproved users, meeting compliance requirements, following government regulatory standards, and establishing repeatable process where customers retain control and access to data without requiring approval for new access to be approved.

Profisee has committed to Service Level Agreements (SLA) with SaaS customers, where security commitments, availability of the platform and access control are used to design a service that is able to grow and expand while maintaining agreed upon SLAs.

Profisee has also integrated Terraform, Infrastructure as Code, to be able to ensure environments are deployed uniformly for each customer and reduce the likelihood of misconfigurations to be introduced, reducing the need of effort to ensure proper deployment and allow for the allocation of resources to be dedicated to design more secure environments.

Components of the System

Infrastructure

Primary infrastructure used to provide the service includes the following:

Primary Infrastructure		
Hardware	**Type**	**Purpose**
Web Application Firewall	Azure	Provide filtering services for SaaS deployment
Jumpbox Virtual Machines (VM)	Azure	Control access to the SaaS environment
Kubernetes Services	Azure	Host and process requests for SaaS customers
SQL Servers	Azure	Host data for SaaS customers

Software

Primary software used to provide the service includes the following:

Primary Software		
Software	**Operating System**	**Purpose**
Failover Region Pairs	Azure	Provide High Availability and recovery environments
Backup	Azure	Provide Long term recovery for customers
Defender	Azure	Preform Anti-virus scans, remediation activity and security monitoring services across Azure native systems where the Profisee SaaS solution is hosted
Azure Active Directory (AD)	Azure	Provides authentication and Single Sign-On (SSO) services for the SaaS solution. Profisee utilizes Azure AD for our users to authenticate, and customers integrate their Azure AD for SSO access to the Profisee SaaS solution

People

Profisee has approximately 110 employees organized in the following functional areas:

- Corporate - Executive team members are responsible for the delivery of various functions such as the development of the platform, sale of the products and review overall objectives and goals that the company has set
- Operations - SaaS Operations teams is made of up individuals who are tasked with the operation, delivery, and monitoring of the SaaS solution. These team members support, troubleshoot and respond to tickets raised by customers. Information Technology (IT) Operations team is responsible for the operation, maintenance and administration of any device, IT service, hardware, software or network service
- Sales - Sales team is responsible for providing demonstration of the product, working with prospective customers, answers questions and any other activity during the sales process

- Professional Services - Professional Services members are responsible for providing troubleshooting, aiding in the deployment of Profisee and resolving issues a customers may have in Traditional Deployments and SaaS deployments. These activities are conducted in either an “Over the Shoulder” manner where the customer is responsible for conducting the activity under the supervision of a Professional Services team member or with the guiding principle of Least Privilege where access to information or systems is granted on a need basis
- Marketing - Marketing is responsible for the development of marketing material, slogans, tag lines and other related documents. Marketing also conducts research and education activities designed to better position Profisee in the MDM marketplace and ensure potential customers understand the value of the services provided

Data

Data that is uploaded to the Profisee SaaS solution is at the discretion of the customer who retains ultimate access and authority of data that is stored. Profisee does not access or view customer data and enables Row Level Security is a default behavior to prevent unauthorized access. Profisee SaaS processes and stores any data that a customer uploads, data destruction is provided through Azure controls with confirmation able to be provided.

Because Profisee does not have insight into customer data, all data is treated with equal protection, all systems are covered by the same security controls, encryption at rest and in transit is enforced through all portions of the environment, and access must be approved by a customer and is controlled through a customer’s Azure AD to ensure access control is provided.

Processes, Policies and Procedures

Physical Security

The in-scope system and supporting infrastructure is hosted by Azure. As such, Azure is responsible for the physical security controls for the in-scope system. Access is controlled through Azure VM Jump boxes to provide access control that are controlled through the same protections as all Azure systems with the availability agnostic to where an employee may be connecting from.

Logical Access

Profisee uses role-based access control, administered through Azure Active Directory, Azure AD Groups and Azure Roles to provide levels of access and control that can be granularly administered. Additionally logical access is controlled through the use of Jump Boxes and Virtual Private Network (VPN) isolation that is controlled through both logical access and AD group restrictions.

Profisee controls access through approved users requiring requesting access from appropriate parties, approval and requests be relevant to their job function. Customer access is controlled through customer’s own processes and able to be determined by customer’s unique controls and requirements.

Access records are recorded and logged in a central Security information and event management (SIEM) solution with controls to monitor for access modification activity, complex password requirements for access with a minimum character length of 12 characters, lockout events triggered after 5 failures that require manual investigation to unlock and time outs set for 5 minutes of inactivity.

All access is also required to satisfy Microsoft Azure AD Multi-factor Authentication (MFA) requests, with access revoked at the time of termination through the disabling and removal of the user AD account.

Customer access is controlled through a thick client connection to a customer’s tenant in the Profisee SaaS solution, with Azure AD SSO used to approve authentication, using the customer’s Azure AD. Traffic is encrypted with Transport Layer Security (TLS) 1.2 in transit and Application Programming Interface (API) access is limited to approved processes and sources.

Profisee reviews access on an annual basis for Profisee Employees to ensure only approved users and access for those users.

Computer Operations - Backups

Profisee utilizes Replication zones across region pairs in the region that is relevant, in the US this is East US and Central US. Profisee also offers up to 89 days of backups through the Azure Backup process in addition to the full replication from East US to Central US, or other region pairs.

Should a failover event need triggered, Profisee is able to manually trigger a fail over, and during annual testing we average 15 minutes for a full fail over, with partial operational functions within minutes.

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.

Profisee centrally logs security relevant information with Log Analytics and Azure Sentinel to provide monitoring of events, review logs and manage incidents.

Infrastructure is designed to run on Kubernetes which enables scalability as part of the design, which is also built on Azure Cloud allowing for scalability of the platform and resources. Profisee utilizes Azure to enable industry leading services that allow for infrastructure that is easy to patch, manage, increase capacity, backup strategy, storage and controls that are native. Profisee closely monitors open-source software and utilizes static code analysis for minor releases with an Application Penetration Assessment prior to any major releases.

Change Control

Profisee Change Control is currently tracked through Azure DevOps, with User Acceptance Testing (UAT) results are documented and maintained results that are required prior to promotion to Production. Changes to the Production environment require communication with any affected customer, backout plans, and approved service windows. Profisee conducts updates of the Profisee Platform as versions are released with any patching that can be automated through Azure systems being enabled.

Data Communications

Profisee utilizes Azure network controls including Application Firewall, Firewall, Azure VPN and will integrate Azure Intrusion Detection and Prevention System (IPDS) in the next major release. Firewalls control Network Address Translation functionality to manage network exposure, with access to the firewalls restricted to approved users, policies applied by and controlled through Terraform to ensure uniformity between environments.

Profisee utilizes full redundancy provided through Azure to prevent any issue that would prevent operation at one data center from preventing service from ceasing and allowing for failover to happen, for example from East US to Central US.

Profisee has engaged Evolve Security to provide a number of services, including Internal and External vulnerability scanning, Pentest/Red team engagements and Application Pentest Assessment activities. Upon disclosure vulnerabilities are reviewed by Profisee, identified for priority and patched or remediated within time frame requirements based on severity. Malicious activity impact has been discussed and planned for, limiting all access to customer data from all employees, preventing unauthorized access or disclosure.

Approved users must access systems through Azure Jump Boxes, which require authentication, MFA requests and be an approved user of the jump box. Identity Access Control is then used to limit a user's access from the jump box to approved systems, following the least privilege access to grant access to the least required systems.

Boundaries of the System

The scope of this report includes the Database and File Management Software services performed in the Alpharetta, Georgia facilities.

This report does not include the cloud computing services provided by Azure.

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

Control Environment

Integrity and Ethical Values

Profisee's commitment to providing ethical administration of the SaaS solution have led to the design, functions and access controls of the Profisee Solution. As part of the employee on-boarding process Profisee's commitment to ethical behavior is a required training meeting that covers both the employee handbook as well as the Growth Mindset which is discussed during ongoing communications, employee celebrations and lessons learned activities where the Growth Mindset is used to frame lessons learned.

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
- 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
- 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

As part of the evaluation of employees and creation of the role descriptions competencies, certifications, and specific skills are identified and assessed for. Profisee also evaluates employees for alignment with the Growth Mindset as part of the evaluation phase.

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

- Management has considered the competence levels for particular jobs and translated required skills and knowledge levels into written position requirements
- Training is provided to maintain the skill level of personnel in certain positions

Management's Philosophy and Operating Style

Profisee'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 information processing, accounting functions, and personnel. This can be most seen in Profisee collecting and accessing no customer data or selling information to third-parties in any manner.

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

- Management is periodically briefed on regulatory and industry changes affecting the services provided with specific design decisions such as hosting in region to provide regulatory compliance
- Executive management meetings are held to discuss major initiatives and issues that affect the business as a whole

Organizational Structure and Assignment of Authority and Responsibility

Profisee'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.

Relevant responsibilities and activities are assigned to individuals and teams best able to achieve the stated goals of the organization. These goals and strategies are laid out for all employees during an annual meeting that all employees are invited to attend.

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 and accessible through the Human Resources (HR) portal

Human Resources Policies and Practices

Profisee'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. Profisee'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
- 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
- To make the termination process, Profisee implements SSO and Identity based authentication in all possible solutions

Risk Assessment Process

Profisee's risk assessment process identifies and manages risks that could potentially affect Profisee'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. Profisee 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 Profisee, 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

Profisee reviews, updates and identifies emerging threats on an annual basis, tracking these organizational risks with a central risk register, taking into consideration the likelihood of this risk occurring, the impact of the risk to the organization and system or information impacted by the risk. This report is used to plan for remediation efforts, plan for new controls and implement new and emerging technologies to reduce these risks.

Information and Communications Systems

Profisee establishes standard communication channels, stakeholders and other relevant operational systems to communicate with customers and notify of changes, events, or receive feedback and suggestions.

Internal communications are provided at annual Town Halls, sprint reviews and other meetings to cover goals, strategy accomplishments and lessons learned with internal employees. E-mail communications are also sent to companywide mailing lists providing updates, information and requests to all employees at an ad-hoc basis.

Monitoring Controls

Management monitors controls to ensure that they are operating as intended and that controls are modified as conditions change. Profisee's management performs monitoring activities to continuously 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. Certification and renewal activities are used to monitor specific systems and controls are functioning, with feedback collected and used to strengthen existing controls, create new controls and resolve any gaps that are identified during engagements.

Management's close involvement in Profisee'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.

Reporting Deficiencies

Management's close involvement in Profisee'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.

HIPAA/HITECH REQUIREMENTS AND RELATED CONTROLS

Periodic Assessments

Profisee 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 Profisee 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 including the Chief Executive Officer (CEO), Chief Operating Officer (COO), Vice President of Information Services, Vice President of Operations, Vice President of Compliance, Vice President of Sales and the Director of Client Services at periodic intervals:

- Risk Assessment: The risk assessment is performed by the risk management personnel. Risk factors associated with the delivery or implementation of services to customers are evaluated considering process owners, dependencies, timelines and quality

- Health Information Security Risks: Health information security risks are assessed by the Vice President of Information Services. Risk factors associated with the organization are evaluated considering compliance obligations, laws and regulations, policies and procedures, contracts and best practices to which the organization has committed to. Information security assessments carried out by risk management personnel are rolled up to the CEO and the COO of the organization

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 all Profisee 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
- Access control
- Physical security

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

Security Awareness Training

Profisee employees receive security awareness training for health information security as part of the onboarding process. This training is reinforced by security awareness communications on current issues which are distributed annually. Additionally, employees are also required to participate in annual security awareness training.

Periodic Testing and Evaluation

Profisee completes evaluations throughout each calendar year regarding the effectiveness of the health information security program that include, but are not limited to, the following:

- Internal risk assessments
- Corrective action plans
- Management reviews

Remediation and Continuous Improvement

Areas of non-compliance in Profisee'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

Profisee 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 in the Last 12 Months

Profisee launched the Profisee SaaS environment in Feb of 2022, no changes were made to the overall strategy of Profisee but were applied to the SaaS environment.

Incidents in the Last 12 Months

During the last 12 months no major incidents were identified that resulted in significant failure or major outages.

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 Safeguard	164.308(a)(4)(ii)(A)	The entity is not a healthcare clearinghouse.
	164.308(b)(1)	The entity is not a covered entity.
Organizational Requirement	164.314(a)(2)(ii)	The entity is not a government entity.
	164.314(b)(1)	The entity is not a plan sponsor.
	164.314(b)(2)	The entity is not a group health plan.
Physical Safeguard	164.310(c)	The entity is not a covered entity.
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 cloud computing services provided by Azure.

Complementary Subservice Organization Controls

Profisee'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 Profisee's services to be solely achieved by Profisee control procedures. Accordingly, subservice organizations, in conjunction with the services, should establish their own internal controls or procedures to complement those of Profisee.

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

Subservice Organization - Azure		
Category	**Criteria**	**Control**
Common Criteria/Security	CC6.1 CC6.3 CC6.6	Access to the underlying network, virtualization management, and storage devices for its cloud hosting services where certain instances of the application reside is restricted to authorized personnel.
	CC6.4, 164.310(a)(1), 164.310(a)(2)(ii), 164.310(a)(2)(iii)	Physical access to data centers is approved by an authorized individual.
		Physical access is revoked within 24 hours of the employee or vendor record being deactivated.
		Physical access to data centers is reviewed on a quarterly basis by appropriate personnel.
		Physical access points to server locations are recorded by closed circuit television camera (CCTV). Images are retained for 90 days, unless limited by legal or contractual obligations.
		Physical access points to server locations are managed by electronic access control devices.
		Electronic intrusion detection systems are installed within data server locations to monitor, detect, and automatically alert appropriate personnel of security incidents.
	164.310(a)(2)(iv)	Policies and procedures are in place to document repairs and modifications to the physical components of the data center facility.
	164.310(d)(1), 164.310(d)(2)(iii)	Offsite backups are tracked and managed to maintain accuracy of the inventory information.
		Production data is encrypted on backup media.

Profisee management, along with the subservice organization, 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, Profisee performs monitoring of the subservice organization controls, including the following procedures:

- Reviewing and reconciling output reports
- Holding discussions with vendors and subservice organization
- Making regular site visits to vendor and subservice organization's facilities
- Testing controls performed by vendors and subservice organization
- Reviewing attestation reports over services provided by vendors and subservice organization
- Monitoring external communications, such as customer complaints relevant to the services by the subservice organization

COMPLEMENTARY USER ENTITY CONTROLS

Profisee'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 related to Profisee's services to be solely achieved by Profisee control procedures. Accordingly, user entities, in conjunction with the services, should establish their own internal controls or procedures to complement those of Profisee's.

The following complementary user entity controls should be implemented by user entities to provide additional assurance that the Trust Services Criteria 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 organizations should implement sound and consistent internal controls regarding general IT system access and system usage appropriateness for all internal user organization components associated with Profisee.
2. User organizations should practice removal of user accounts for any users who have been terminated and were previously involved in any material functions or activities associated with Profisee's services.
3. Transactions for user organizations relating to Profisee's services should be appropriately authorized, and transactions should be secure, timely, and complete.
4. For user organizations sending data to Profisee, data should be protected by appropriate methods to ensure confidentiality, privacy, integrity, availability, and non-repudiation.
5. User organizations should implement controls requiring additional approval procedures for critical transactions relating to Profisee's services.
6. User organizations should report to Profisee in a timely manner any material changes to their overall control environment that may adversely affect services being performed by Profisee.
7. User organizations are responsible for notifying Profisee in a timely manner of any changes to personnel directly involved with services performed by Profisee. These personnel may be involved in financial, technical, or ancillary administrative functions directly associated with services provided by Profisee.
8. User organizations are responsible for adhering to the terms and conditions stated within their contracts with Profisee.
9. User organizations are responsible for developing, and if necessary, implementing a business continuity and disaster recovery plan (BCDRP) that will aid in the continuation of services provided by Profisee.

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.

Control Activities Specified by the Service Organization

The applicable trust criteria, risks, and related control activities are included in Section 4 of this report to eliminate the redundancy that would result from listing them in this section. Although the applicable trust criteria and related control activities are included in Section 4, they are, nevertheless, an integral part of Profisee's description of the system. Any applicable Trust Services Criteria that are not addressed by control activities at Profisee are described within Section 4 and within the Subservice Organization section above.

HEALTH INFORMATION SECURITY PROGRAM

Profisee has developed a health information security management program to meet the information security and compliance requirements related to Artificial Intelligence and Natural Language Processing services and its customer base. The program incorporates the elements of the HIPAA and the HITECH. The description below is a summary of safeguards that Profisee 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 Profisee 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:

- Documented physical security policies and procedures are in place to guide personnel in physical security administration.
- Physical access procedures are in place restrict access, log visitors, and terminate access to the office facility.
- 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 PHI transmitted electronically over open networks from being intercepted by anyone other than the intended recipient:

- Access to in-scope systems is 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 Requirements - 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 all 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 is documented to communicate workforce conduct standards and enforcement procedures.
		Upon hire, personnel are required to acknowledge the employee handbook.
		Upon hire, personnel are required to sign a non-disclosure agreement.
		Upon hire, personnel are required to complete a background check.
		Personnel are required to acknowledge the employee handbook on an annual basis.
		Performance evaluations are performed for personnel on an annual basis.
		Disciplinary policies, which include probation, suspension and termination, are in place for employee misconduct.
		Employees, third-parties and customers are directed on how to report unethical behavior in a confidential manner.
		The entity's third-party contract requires that third-parties have a code of conduct and employee handbook in place.
		Third-parties require their employees to complete a background check and acknowledge the employee handbook and code of conduct.
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 defines and documents the skills and expertise needed among its members.
		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 annually with operational management to assess the effectiveness and performance of internal controls within the environment.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
CC1.0	Control Environment	
Control Point	Criteria	Control Activity Specified by the Service Organization
CC1.3	COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	Executive management evaluates the skills and competencies of those that operate the internal controls within the environment annually. Operational management assigns responsibility for and monitors the effectiveness and performance of internal controls implemented within the environment. A third-party performs an independent assessment of the entity's controls environment annually to assess the effectiveness of internal controls within the environment. Outside executive council is brought in as needed to provide expertise and insight on the internal controls environment. 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. Roles and responsibilities are defined in written job descriptions and communicated to personnel through the entity's intranet. 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. Roles and responsibilities defined in written job descriptions consider and address specific requirements relevant to the system. A vendor risk management is performed on an annual basis which includes reviewing the activities performed by third-parties. Executive management considers the roles and responsibilities performed by third-parties when documenting the organizational chart and defining job descriptions. Executive management considers interactions with, and the need to monitor the activities of third-parties when documenting the organizational chart and defining job descriptions.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
CC1.0	**Control Environment**	
Control Point	**Criteria**	**Control Activity Specified by the Service Organization**
CC1.4	COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	Policies are in place that outline the performance evaluation process as well as the competency and training requirements for personnel. Performance 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's third-party contract requires that third-parties: • Consider the background, competencies and experience of its personnel • Provide regular training to its personnel as it relates to their job role and responsibilities Employees are required to attend continued training annually that relates to their job role and responsibilities. Executive management has created a training program for its employees. The entity has implemented a mentor program to develop its personnel. Executive management tracks and monitors compliance with continued professional education training requirements. As part of the performance evaluation process, the entity rewards its personnel for exceeding expectations as it relates to their job role and responsibilities. The entity assesses training needs on an annual basis. As part of the entity's contingency plan for job roles and assignments important to the operations and performance of controls, the entity cross trains its personnel. Prior to employment, 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 intranet.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
CC1.0	Control Environment	
Control Point	Criteria	Control Activity Specified by the Service Organization
		Upon hire, personnel are required to acknowledge the employee handbook which requires adherence to the personnel's job role and responsibilities. Personnel are required to acknowledge the employee handbook on an annual basis. Policies are in place that outline the performance evaluation process as well as the competency and training requirements for personnel. Executive management has established performance measures, including the incentives and rewards for exceeding expectations, as it relates to job roles and responsibilities. Performance evaluations are performed for personnel on an annual basis. As part of the performance evaluation process, the entity rewards its personnel for exceeding expectations and performs disciplinary actions for its employees who do not meet expectations as it relates to their job role and responsibilities. Executive management reviews the job requirements and responsibilities documented within job descriptions annually and makes updates, if necessary. Executive management reviews the responsibilities assigned to operational personnel annually and makes updates, if necessary. Disciplinary 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 intranet. Edit checks are in place to prevent incomplete or incorrect data from being entered into the system. Data flow diagrams, process flowcharts, narratives and procedures manuals 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. Data and information critical to the system is assessed annually for relevance and use.
		Roles and responsibilities are defined in written job descriptions and communicated to personnel through the entity's intranet. The entity's policies and procedures and employee handbook are made available to employees through the entity's intranet. Upon hire, employees are required to read and acknowledge the information security policies and procedures and complete information security and awareness training.
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.	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. Personnel are required to acknowledge the employee handbook on an annual basis. Upon hire, personnel are required to acknowledge the employee handbook which requires adherence to the personnel's job role and responsibilities. Executive management meets annually with operational management to discuss the entity's objectives as well as roles and responsibilities. Employees, third-parties, and customers are directed on how to report unethical behavior in a confidential manner. Changes to job roles and responsibilities are communicated to personnel through the entity's intranet.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
CC2.0	**Information and Communication**	
Control Point	**Criteria**	**Control Activity Specified by the Service Organization**
		Documented escalation procedures for reporting failures incidents, concerns and other complaints are in place and made available to employees through the entity's intranet. The entity's objectives, including changes made to the objectives, are communicated to its personnel through the entity's intranet. Employees are required to attend security awareness training annually. 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 contract delineates the boundaries of the system and describes relevant system components. The entity's third-party contract communicates the system commitments and requirements of third-parties. The information security policies and procedures that communicate the system commitments and requirements of external users are provided to external users prior to allowing them access to the system. The entity's third-party contract outlines and communicates the terms, conditions, and responsibilities of third-parties. The entity's contractor contract outlines and communicates the terms, conditions, and responsibilities of external users. Customer commitments, requirements and responsibilities are outlined and communicated through service agreements. Changes to commitments, requirements and responsibilities are communicated to third-parties, external users, and customers via e-mails. Documented escalation procedures for reporting failures incidents, concerns and other complaints are in place and shared with external parties. Executive management meets annually with operational management to discuss the results of assessments performed by third-parties. Employees, third-parties and customers are directed on how to report unethical behavior in a confidential manner.

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 has documented objectives that are specific, measurable, attainable, relevant and time-bound (SMART). Executive management identifies and assesses risks that could prevent the entity's objectives from being achieved. Executive management reviews policies, procedures and other control documents for alignment to the entity's objectives on an annual basis. Executive management reviews and addresses repeated control failures. Executive management has established key performance indicators for operational and internal controls effectiveness, including the acceptable level of control operation and failure. The entity has defined the desired level of performance and operation in order to achieve the established entity objectives. The operational reports reviewed by executive management define the acceptable level of operational performance and control failure. Key performance indicators of both the business performance and employee performance are developed in alignment with entity objectives and strategies. Executive management reviews operational and resourcing reports to evaluate performance and resourcing at least annually. Business plans and budgets align with the entity's strategies and objectives. Entity strategies, objectives and budgets are assessed on an annual basis. Executive management reviews key operational reports for precision and accuracy. The entity's internal controls framework is based on a recognized (NIST 800-53; COBIT; ISO; COSO) framework. The entity's internal controls environment takes into consideration affecting laws, regulations, standards, and legislatures. Applicable law, regulation, standard and legislature requirements are identified and integrated into the entity’s strategies and objectives.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
CC3.0	**Risk Assessment**	
Control Point	**Criteria**	**Control Activity Specified by the Service Organization**
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	The entity undergoes compliance audits at least annually to show compliance to relevant laws, regulations and standards. Documented policies and procedures are in place to guide personnel when performing a risk assessment. Management has defined a formal risk management 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 management 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. Risks identified as a part of the risk assessment process are addressed using the mitigation risk strategy. Management develops risk mitigation strategies to address risks identified during the risk management 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. The annual comprehensive risk assessment results are reviewed and approved by appropriate levels of management.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
CC3.0	**Risk Assessment**	
Control Point	**Criteria**	**Control Activity Specified by the Service Organization**
		As part of the annual risk assessment, management reviews the potential threats and vulnerabilities arising from its customers, vendors and third-parties.
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 (e.g., fraudulent reporting, loss of assets, unauthorized system access, overriding controls) that could impact their business and operations. Identified fraud risks are reviewed and addressed using one of the following strategies: • Mitigate the risk • Exclusion • Accept the risk 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. As part of management's assessment of fraud risks, management considers how personnel could engage in or justify fraudulent activities. As part of management's assessment of fraud risks, management considers threats and vulnerabilities that arise from the use of IT (e.g., unauthorized access, inadequate segregation of duties, default accounts, inadequate password management, unauthorized changes)
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. Changes in vendor and third-party relationships 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. Key systems, tools, and applications are reviewed internally for compliance against documented policies and procedures by operational management annually or continuously using a compliance monitoring tool. 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. Management reviews the frequency of compliance evaluations annually and adjusts it based on changes to the environment and operational performance. A third-party performs a penetration testing annually to identify and exploit vulnerabilities identified within the environment. A third-party performs an independent assessment of the controls environment annually to assess the effectiveness of controls within the 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. Senior management assesses the results of the compliance, control and risk assessments performed on the environment.
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.	Senior management is made aware of high-risk vulnerabilities, deviations and controls gaps identified as part of the compliance, control and risk assessments performed.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
CC4.0	**Monitoring Activities**	
Control Point	**Criteria**	**Control Activity Specified by the Service Organization**
		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. 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.	As part of the risk assessment process, controls within the environment are modified and implemented to mitigate identified vulnerabilities, deviations and control gaps. Controls within the environment are modified and implemented to mitigate vulnerabilities, deviations and control gaps identified as part of the various evaluations (e.g., risk assessments, vulnerability scans) performed. Performance of the internal controls implemented within the environment are assigned to appropriate process owners and operational personnel based on roles and responsibilities. Prior to the development and implementation of internal controls into the environment, management considers the complexity, nature, and scope of its operations. 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. An analysis of incompatible operational duties is performed on at least an annual basis, and where incompatible responsibilities are identified, compensating controls are put into place.
CC5.2	COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.	Management has documented the relationship and linkage between business processes, the relevant technologies used to support the business processes, and the controls in place to help secure those business processes. Organizational and information security policies and procedures are documented and made available to employees through the entity's intranet. Management has documented the controls implemented around the entity's technology infrastructure.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
CC5.0	**Control Activities**	
Control Point	**Criteria**	**Control Activity Specified by the Service Organization**
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.	Management has established controls around the entity's technology infrastructure to address the risks of incomplete, inaccurate, and unavailable technology processing. As part of the risk assessment process, the use of technology in business processes is evaluated by management. 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 Management has established controls around the acquisition, development and maintenance of the entity's technology infrastructure. Organizational and information security policies and procedures are documented and made available to employees through the entity's intranet. The incident response policy 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 intranet. Performance of the internal controls implemented within the environment are assigned to appropriate process owners and operational personnel based on roles and responsibilities. Process owners and management operate the controls implemented within the entity's environment based on the frequency defined in the organizational and information security policies and procedures. Process owners and management investigate and troubleshoot control failures. Effectiveness of the internal controls implemented within the environment are evaluated annually.

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, authentication, access, and security monitoring.
	Network (Microsoft Azure)	
		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: • Evolve Security Contractor • Software Architect • DevOps Engineer • Sr. QA Engineer • Director of Technology Networks are configured to enforce password requirements that include: • Password history • Password age (minimum) • Password length Network account lockout settings are in place that include: • Account lockout duration • Account lockout threshold Network audit logging settings are in place that include: • Account logon events • Object access • Policy changes • Process tracking • System events Network audit logs are maintained and reviewed as needed.
	Operating System (Application, Web, and Database Servers)	
		Operating system 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**
		Operating system administrative access is restricted to user accounts accessible by the following personnel: • Evolve Security Contractor • Software Architect • DevOps Engineer • Sr. QA Engineer • Director of Technology Operating systems are configured to enforce password requirements that include: • Password history • Password age (minimum) • Password length Operating system account lockout settings are in place that include: • Account lockout duration • Account lockout threshold Operating system audit logging settings are in place that include: • Account logon events • Object access • Policy changes • Process tracking • System events Operating system audit logs are maintained and reviewed as needed.
	Database (Azure SQL)	
		Database user access is restricted via role-based security privileges defined within the access control system. Database administrative access is restricted to user accounts accessible by the following personnel: • Software Architect • Sr. QA Engineer Databases are configured to enforce password requirements that include: • Password history • Password age (minimum) • Password length Database account lockout settings are in place that include: • Account lockout duration • Account lockout threshold

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
CC6.0	**Logical and Physical Access**	
Control Point	**Criteria**	**Control Activity Specified by the Service Organization**
		Database audit logging settings are in place that include: • Account logon events • Logon events • Process tracking • System events 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. Application administrative access is restricted to user accounts accessible by the following personnel: • Evolve Security Contractor • Software Architect • DevOps Engineer • Sr. QA Engineer • Director of Technology The application is configured to enforce password requirements that include: • Password history • Password age (minimum) • Password length Application account lockout settings are in place that include: • Account lockout duration • Account lockout threshold Application audit policy settings are in place that include: • Account logon events • Logon events • Process tracking • System events Application audit logs are maintained and reviewed as needed.
	Remote Access	
		VPN user access is restricted via role-based security privileges defined within the access control system. The ability to administer VPN access is restricted to user accounts accessible by the following personnel: • Software Architect • Director of Technology

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
CC6.0	**Logical and Physical Access**	
Control Point	**Criteria**	**Control Activity Specified by the Service Organization**
		VPN users are authenticated via multi-factor authentication (username, password, and PIN/OTP/Token) prior to being granted remote access to the system. The entity's various networks are segmented to keep information and data isolated and restricted to authorized personnel. Access into the environment by outside entities requires a valid user ID and password and invalid login attempts are configured to be logged. Data coming into the environment is secured and monitored through the use of firewalls and an IDPS A demilitarized zone (DMZ) is in place to isolate outside access and data from the entity's environment. Server certificate-based authentication is used as part of the Secure Sockets Layer (SSL) / Transport Layer Security (TLS) encryption with a trusted certificate authority. Stored passwords are encrypted. Critical data is stored in encrypted format using software supporting the transparent data encryption. Encryption keys are protected during generation, storage, use, and destruction. The entity restricts access to its environment using the following mechanisms: • Classifying data • User identification Control self-assessments that include logical access reviews are performed on at least an annual basis. 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, authentication, 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.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
CC6.0	**Logical and Physical Access**	
Control Point	**Criteria**	**Control Activity Specified by the Service Organization**
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.	Control self-assessments that include logical access reviews are performed on at least an annual basis. Privileged access to sensitive resources is restricted to authorized personnel. Documented policies and procedures are in place regarding system settings, authentication, 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. Access rights are reviewed for employees that transfer job function or role. An analysis of incompatible operational duties is performed on at least an annual basis, and where incompatible responsibilities are identified, compensating controls are put into place. 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.
	Network (Azure)	
		Network access reviews are completed by management annually. Network user access is restricted via role-based security privileges defined within the access control system.
	Operating System (Application, Web, and Database Servers)	
		Operating system access reviews are completed by management annually. Operating system user access is restricted via role-based security privileges defined within the access control system.
	Database (Azure SQL)	
		Database access reviews are completed by management annually. 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**
	Application	
		Application access reviews are completed by management annually. Application user access is restricted via role-based security privileges defined within the access control system.
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.	Policies and procedures are in place to guide personnel in physical security activities.
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 data, hardware and software disposal and destruction. Data that is no longer required for business purposes is rendered unreadable. Policies and procedures are in place for removal of media storing critical data or software.
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. VPN, SSL and other encryption technologies are used for defined points of connectivity. VPN users are authenticated via multi-factor authentication (username, password, and PIN/OTP/Token) prior to being granted remote access to the system. Server certificate-based authentication is used as part of the TLS encryption with a trusted certificate authority. Transmission of digital output beyond the boundary of the system is encrypted. Remote connectivity users are authenticated via an authorized user account and password before establishing a VPN session. Logical access to stored data is restricted to authorized personnel. 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 Intrusion Detection and Prevention System (IDPS) is utilized to analyze network events and report possible or actual network security breaches. The IDPS is configured to notify personnel upon intrusion detection.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
CC6.0	Logical and Physical Access	
Control Point	Criteria	Control Activity Specified by the Service Organization
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.	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 weekly basis. Critical data is stored in encrypted format using software supporting the TDE. A DMZ is in place to isolate outside access and data from the entity's environment. Use of removable media is prohibited by policy except when authorized by management. Logical access to stored data is restricted to authorized personnel. Backup media is rotated off-site by a third-party vendor daily. The ability to recall backed up data is restricted to authorized personnel. The entity secures its environment a using multi-layered defense approach that includes firewalls, antivirus software and a DMZ. VPN, SSL and other encryption technologies are used for defined points of connectivity. Server certificate-based authentication is used as part of the TLS encryption with a trusted certificate authority. Remote connectivity users are authenticated via an authorized user account and password before establishing a VPN session. 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 IDPS is utilized to analyze network events and report possible or actual network security breaches. The IDPS is configured to notify personnel upon intrusion detection.

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.	Critical data is stored in encrypted format using software supporting the TDE. Backup media is stored in an encrypted format. Transmission of digital output beyond the boundary of the system is encrypted. Use of removable media is prohibited by policy except when authorized by management. Mobile devices (e.g., laptops, smart phones) are protected through the use of secured, encrypted connections. A warning notification appears when an employee attempts to download an application or software. 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 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.

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 when thresholds have been exceeded. Key systems, tools, and applications are reviewed internally for compliance against documented policies and procedures by operational management annually or continuously using a compliance monitoring tool. An IDPS is utilized to analyze network events and report possible or actual network security breaches. The IDPS is configured to notify personnel upon intrusion detection. 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 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 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 and penetration tests are performed on at least an annual basis and remedial actions are taken where necessary. 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.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
CC7.0	**System Operations**	
Control Point	**Criteria**	**Control Activity Specified by the Service Organization**
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.	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 when thresholds have been exceeded. Monitoring software is used to identify and evaluate ongoing system performance, capacity, security threats, changing resource utilization needs and unusual system activity. An IDPS is utilized to analyze network events and report possible or actual network security breaches. The IDPS is configured to notify personnel upon intrusion detection. 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 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 weekly basis. The entity's third-party contract requires third-parties to implement detective controls and provide notice if the third-party's environment is compromised. Use of removable media is prohibited by policy except when authorized by management.
	Network	
		Network account lockout settings are in place that include: • Account lockout duration • Account lockout threshold

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
CC7.0	**System Operations**	
Control Point	**Criteria**	**Control Activity Specified by the Service Organization**
		Network audit logging settings are in place that include: • Account logon events • Object access • Policy changes • Process tracking • System events • Network audit logs are maintained and reviewed as needed.
	Operating System (Application, Web, and Database Servers)	
		Operating system account lockout settings are in place that include: • Account lockout duration • Account lockout threshold Operating system audit logging settings are in place that include: • Account logon events • Object access • Policy changes • Process tracking • System events • 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 Database audit logging settings are in place that include: • Account logon events • Logon events • Process tracking • System events • Database audit logs are maintained and reviewed as needed.
	Application	
		Application account lockout settings are in place that include: • Account lockout duration • Account lockout threshold

<table>
<tr><th colspan="3">TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY</th></tr>
<tr><th>CC7.0</th><th colspan="2">System Operations</th></tr>
<tr><th>Control Point</th><th>Criteria</th><th>Control Activity Specified by the Service Organization</th></tr>
<tr><td>CC7.3</td><td>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.</td><td>Application audit policy settings are in place that include:
• Account logon events
• Logon events
• Process tracking
• System events
• Application audit logs are maintained and reviewed as needed.
Management reviews reports on an annual basis summarizing incidents, root cause of incidents, and corrective action plans and as part of the review, management identifies the need for system changes and implementation of additional controls based on incident patterns and root causes.
Management monitors the effectiveness of detection tools and controls implemented within the environment.
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 severity.
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.
A security incident analysis is performed for critical incidents to determine the root cause, system impact and resolution.
Identified incidents are reviewed, monitored and investigated by an incident response team.
Identified incidents are analyzed, classified and prioritized based on system impact to determine the appropriate containment strategy, including a determination of the appropriate response time frame and the determination and execution of the containment approach.
Roles and responsibilities for the design, implementation, maintenance, and execution of the incident response program are defined and documented.</td></tr>
</table>

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
CC7.0	**System Operations**	
Control Point	**Criteria**	**Control Activity Specified by the Service Organization**
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.	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. The actions taken to address identified security incidents are documented and communicated to affected parties. Documented incident response and escalation procedures are in place to guide personnel in addressing the threats posed by security incidents. Critical security incidents that result in a service/business operation disruption are communicated to those affected through e-mails. 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 system impact to determine the appropriate containment strategy, including a determination of the appropriate response time frame and the determination and execution of the containment approach. A security incident analysis is performed for critical incidents to determine the root cause, system impact and resolution. The risks associated with identified vulnerabilities are addressed using one of the following strategies: • Avoid the risk • Mitigate the risk • Transfer the risk • Accept the risk The incident response and escalation procedures are reviewed at least annually for effectiveness. Management reviews reports on an annual basis summarizing incidents, root cause of incidents, and corrective action plans and as part of the review, management identifies the need for system changes and implementation of additional controls based on incident patterns and root causes. Change management requests are opened for incidents that require permanent fixes.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
CC7.0	**System Operations**	
Control Point	**Criteria**	**Control Activity Specified by the Service Organization**
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	The entity restores system operations for incidents impacting the environment through activities that include, but are not limited to: • Rebuilding systems • Updating software • Installing patches • Removing unauthorized access • Changing configurations Data backup and restore procedures are in place to guide personnel in performing backup activities. Control self-assessments that include backup restoration tests are performed on at least an annual basis. Management reviews reports on an annual basis summarizing incidents, root cause of incidents, and corrective action plans and as part of the review, management identifies the need for system changes and implementation of additional controls based on incident patterns and root causes. A security incident analysis is performed for critical incidents to determine the root cause, system impact and resolution. On an annual basis, preventative and detective controls are evaluated and changed, as necessary. After critical incidents are investigated and addressed, lessons learned are documented and analyzed, and incident response plans and recovery procedures are updated based on the lessons learned. 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. The disaster recovery plan is tested on an annual basis. The business continuity and disaster recovery plan and procedures are updated based on disaster recovery plan test results.

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-owner or business unit manager • Development-application design and support department • Testing-quality assurance department • Implementation software change management group 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. Back out procedures are documented within each change implementation to allow for rollback of changes when changes impair system operation. System changes are tested prior to implementation. Types of testing performed depend on the nature of the change. System changes implemented to the production environment are evaluated for impact to the entity's objectives. System changes implemented for remediating incidents follow the standard change management process. 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 implementing changes in an emergency situation.

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 policy are in place to guide personnel in performing risk mitigation activities.
		Management has defined a formal risk management 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.
		Risks identified as a part of the risk assessment process are addressed using the mitigation risk strategy.
		Management develops risk mitigation strategies to address risks identified during the risk management process.
		The entity has purchased insurance to offset the financial loss that could result from a critical security incident or exploitation of a vulnerability.
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 scope of services • Roles and responsibilities • Terms of the business relationship • Communication protocols • Compliance requirements • Service levels • Just cause for terminating the relationship
		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.
		A formal third-party risk assessment is performed on an annual basis to identify threats that could impair system commitments and requirements.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
CC9.0	Risk Mitigation	
Control Point	Criteria	Control Activity Specified by the Service Organization
		Management has established exception handling procedures for services provided by third-parties. The entity has documented procedures for addressing issues identified with third-parties. The entity has documented procedures for terminating third-party relationships.

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 are in place to guide personnel in addressing the threats posed by security incidents. 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 when thresholds have been exceeded. Monitoring software is used to identify and evaluate ongoing system performance, capacity, security threats, changing resource utilization needs and unusual system activity. An IDPS is utilized to analyze network events and report possible or actual network security breaches. The IDPS is configured to notify personnel upon intrusion detection. 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 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 WEEKLY basis. Internal and external vulnerability scans and penetration tests 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 (a)(1)(ii)(A)	**Risk analysis:** an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information (ePHI).	A formal risk assessment is performed on an annual basis to identify threats that could impair systems security, confidentiality, integrity, and availability of ePHI.
164.308 (a)(1)(ii)(B)	**Risk management:** Ensures the company implements security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with §164.306. 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	Management develops risk mitigation strategies to address risks identified during the risk assessment process. Internal and external vulnerability scans and penetration tests are performed on at least an annual basis and remedial actions are taken where necessary.
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.	The entity maintains policy and procedure documents that outline the process of sanctioning personnel who fail to comply with the security policies and procedures.
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.	Regular monitoring and review of logins and log-in attempts to the system is in place. Discrepancies and potentially inappropriate or illegal activities are reported to senior management, legal counsel and/or human resources, as appropriate.
	Network	
		Network audit logging settings are in place that include: • Account logon events • Account management • Directory Service Access • Logon events • Object access • Policy changes • Privilege use • Process tracking • System events Network audit logs are maintained and reviewed as needed.

ADMINISTRATIVE 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 changes • Privilege use • Process tracking • System events Operating system audit logs are maintained and reviewed as needed.
	Database	
		Database audit logging settings are in place that include: • Account logon events • Logon events • Process tracking • System events Database audit logs are maintained and reviewed as needed.
	Application	
		Application audit policy settings are in place that include: • Account logon events • Logon events • Process tracking • System events Application audit logs are maintained and reviewed as needed. 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.
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 entity.	Responsibility for the development, implementation, and regular maintenance of the policies and procedures that govern the security of protected ePHI is assigned to the Security Engineer.

ADMINISTRATIVE SAFEGUARDS		
Ref	**Regulation**	**Control Activity Specified by the Service Organization**
164.308 (a)(3)(i)	**Workforce security:** Policies and procedures are implemented to ensure that all members of the workforce have appropriate access to ePHI, 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.	Documented policies and procedures are in place regarding system settings, authentication, access, and security monitoring. Control self-assessments that include logical access reviews are performed on at least an annual basis. 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. Access rights are reviewed for employees that transfer job function or role.
	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: Software Architect.
	Operating System (Application, Web, and Database Servers)	
		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: Software Architect.
	Database	
		Database user access is restricted via role-based security privileges defined within the access control system. Database administrative access is restricted to user accounts accessible by the following personnel: • Software Architect • Sr. QA Engineer
	Application	
		Application user access is restricted via role-based security privileges defined within the access control system.

ADMINISTRATIVE SAFEGUARDS		
Ref	**Regulation**	**Control Activity Specified by the Service Organization**
		Application administrative access is restricted to user accounts accessible by the following personnel: • Evolve Security Contractor • Software Architect • DevOps Engineer • Sr. QA Engineer • Director of Technology
	Remote Access	
		VPN user access is restricted via role-based security privileges defined within the access control system. The ability to administer VPN access is restricted to user accounts accessible by the following personnel: • Software Architect • Director of Technology
	Physical Access (CARVE OUT - MICROSOFT AZURE)	
164.308 (a)(3)(ii)(A) 164.308 (a)(3)(ii)(B)	**Authorization and/or supervision:** Ensures the authorization and/or supervision of workforce members who work with ePHI or in locations where it might be accessed. **Workforce clearance procedure:** Access of a workforce member (employee or computing device) to ePHI is appropriate.	Part of this criterion is the responsibility of the subservice organization. Refer to the Subservice Organizations section below for controls managed by the subservice organization Documented policies and procedures are in place regarding system settings, authentication, access, and security monitoring. Control self-assessments that include physical and logical access reviews are performed on at least an annual basis. 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. Access rights are reviewed for employees that transfer job function or role. Access control and role-based build procedures are in place to restrict access to systems that maintain ePHI to only authorized personnel. Control self-assessments that include physical and logical access reviews are performed on at least an annual basis. 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.

ADMINISTRATIVE SAFEGUARDS		
Ref	**Regulation**	**Control Activity Specified by the Service Organization**
164.308 (a)(3)(ii)(C)	**Termination procedures:** Ensure that access to ePHI is terminated as soon as possible when a workforce member's employment ends.	Documented policies and procedures are in place regarding system settings, authentication, access, and security monitoring. Logical access to systems is revoked as a component of the termination process.
164.308 (a)(4)(i)	**Information access management:** Policies and procedures are implemented that ensure authorizing access to ePHI and 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.	Management maintains policies and procedures that ensure the authorization of access to ePHI and are consistent with the applicable requirements of the Privacy Rule.
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 ePHI 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.	Access control and role-based build procedures are in place to restrict access to systems that maintain ePHI to only authorized personnel. Logical access to systems is approved and granted to an employee as a component of the hiring process.
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.	Access control and role-based build procedures are in place to restrict access to systems that maintain ePHI to only 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. Access rights are reviewed for employees that transfer job function or role. Control self-assessments that include physical and logical access reviews are performed on at least an annual basis.

ADMINISTRATIVE SAFEGUARDS		
Ref	**Regulation**	**Control Activity Specified by the Service Organization**
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.	Management conducts periodic security awareness training to establish the organization's commitments and requirements for employees. Policies are in place that outline the performance evaluation process as well as the competency and training requirements for personnel. 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. Employees are required to attend security awareness training annually.
164.308 (a)(5)(ii)(A)	**Security reminders:** Periodic security updates.	Users are made aware of security updates and updates to security policies via e-mail notifications.
164.308 (a)(5)(ii)(B)	**Protection from malicious software:** Procedures for guarding against, detecting, and reporting malicious software.	A program of techniques, technologies, and methods to guard against, detect, and report the presence of malicious software is in place. 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 weekly basis. Monitoring software is used to identify and evaluate ongoing system performance, capacity, security threats, changing resource utilization needs and unusual system activity. An IDPS is utilized to analyze network events and report possible or actual network security breaches. The IDPS is configured to notify personnel upon intrusion detection.
164.308 (a)(5)(ii)(C)	**Log-in monitoring:** Procedures for monitoring log-in attempts and reporting discrepancies.	Regular monitoring and review of logins and log-in attempts to the system is in place. Discrepancies and potentially inappropriate or illegal activities are reported to senior management, legal counsel and/or human resources, as appropriate.

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 changes • Privilege use • Process tracking • System events 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 changes • Privilege use • Process tracking • System events Operating system audit logs are maintained and reviewed as needed.
	Database	
		Database audit logging settings are in place that include: • Account logon events • Logon events • Process tracking • System events Database audit logs are maintained and reviewed as needed.
	Application	
		Application audit policy settings are in place that include: • Account logon events • Logon events • Process tracking • System events Application audit logs are maintained and reviewed as needed.

ADMINISTRATIVE SAFEGUARDS		
Ref	**Regulation**	**Control Activity Specified by the Service Organization**
		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.
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 for network devices and servers.
	Network	
		Networks are configured to enforce password requirements that include: • Password history • Password age (minimum and maximum) • Password length
	Operating System (Application, Web, and Database Servers)	
		Operating systems are configured to enforce password requirements that include: • Password history • Password age (minimum and maximum) • Password length
	Database	
		Databases are configured to enforce password requirements that include: • Password history • Password age (minimum and maximum) • Password length
	Application	
		The application is configured to enforce password requirements that include: • Password history • Password age (minimum and maximum) • Password length
	Remote Access	
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. 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 severity. 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)(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.	Incidents are documented and tracked in a standardized ticketing system and updated to reflect the planned incident and problem resolution. A security incident analysis is performed for critical incidents to determine the root cause, system impact and resolution. Identified incidents are reviewed, monitored and investigated by an incident response team. 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 system impact to determine the appropriate containment strategy, including a determination of the appropriate response time frame and the determination and execution of the containment approach. 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 severity. 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. A security incident analysis is performed for critical incidents to determine the root cause, system impact and resolution. Identified incidents are reviewed, monitored and investigated by an incident response team. 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 system impact to determine the appropriate containment strategy, including a determination of the appropriate response time frame and the determination and execution of the containment approach.

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.	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. A business continuity plan is documented and in place that outlines the range of disaster scenarios and steps the business will take in a disaster to ensure the timely resumption of critical business operations. The business continuity plan is tested on an annual basis and includes: • Various testing scenarios based on threat likelihood • Identifying the critical systems required for business operations • Assigning roles and responsibilities in the event of a disaster • Assessing and mitigating risks identified as a result of the test disaster
164.308 (a)(7)(ii)(A)	**Data backup plan:** Establish and implement procedures to create and maintain retrievable exact copies of ePHI.	Procedures are in place to provide for complete, accurate, and timely storage of data. The ways in which critical data are backed up and stored are documented and reviewed annually. Data backup and restore procedures are in place to guide personnel in performing backup activities. Full backups of certain application and database components are performed on a daily. When a backup job fails, the backup tool sends an alert to the backup administrators who investigate and resolve the failure. Backup media is rotated off-site by a third-party vendor on a monthly basis. Data backed up is replicated to an offsite facility in real-time. Backups of critical data are maintained securely offsite by a third-party. Control self-assessments that include Backup restoration tests are performed on at least an annual basis.
164.308 (a)(7)(ii)(B)	**Disaster recovery plan:** Establish (and implement as needed) procedures to restore any loss of data.	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. The disaster recovery plan includes moving the business operations and supporting systems to a warm site.

ADMINISTRATIVE SAFEGUARDS		
Ref	**Regulation**	**Control Activity Specified by the Service Organization**
		A business continuity plan is documented and in place that outlines the range of disaster scenarios and steps the business will take in a disaster to ensure the timely resumption of critical business operations. The business continuity plan is tested on an annual basis and includes: • Various testing scenarios based on threat likelihood • Identifying the critical systems required for business operations • Assigning roles and responsibilities in the event of a disaster • Assessing and mitigating risks identified as a result of the test disaster Data Backup restoration tests are performed at least annual. Redundant architecture is in place to migrate business operations to alternate infrastructure in the event normal processing infrastructure becomes unavailable.
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.	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. The disaster recovery plan includes moving the business operations and supporting systems to a hot site. A business continuity plan is documented and in place that outlines the range of disaster scenarios and steps the business will take in a disaster to ensure the timely resumption of critical business operations. The business continuity plan is tested on an annual basis and includes: • Various testing scenarios based on threat likelihood • Identifying the critical systems required for business operations • Assigning roles and responsibilities in the event of a disaster • Assessing and mitigating risks identified as a result of the test disaster Data Backup restoration tests are performed at least annual. Redundant architecture is in place to migrate business operations to alternate infrastructure in the event normal processing infrastructure becomes unavailable.

ADMINISTRATIVE SAFEGUARDS		
Ref	**Regulation**	**Control Activity Specified by the Service Organization**
164.308 (a)(7)(ii)(D)	**Testing and revision procedures:** Implement procedures for periodic testing and revision of contingency plans.	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. The business continuity plan is tested on an annual basis and includes: • Various testing scenarios based on threat likelihood • Identifying the critical systems required for business operations • Assigning roles and responsibilities in the event of a disaster • Assessing and mitigating risks identified as a result of the test disaster
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.	The entity has defined what critical data is processed and how it is processed. Data and information critical to the system is assessed annually for relevance and use. For each critical system, the entity defines and documents what data and information is critical to support the system. The entity has defined the following components of the data critical to supporting the system • A description of what the critical data is and is used for • Source of the data • How the data is stored and transmitted 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)(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.	Changes to the regulatory, economic and physical environment in which the entity operates are considered and evaluated as part of the annual comprehensive risk assessment. 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. Changes in vendor and third-party relationships are considered and evaluated as part of the annual comprehensive risk assessment.
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 has no Business Associate that access ePHI information, all is handled by internal employees and there is row security enable, in which they cannot have access to client data.
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) [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 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.	This criterion is the responsibility of the subservice organization. Refer to the Subservice Organizations section below 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.	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. The business continuity plan is tested on an annual basis and includes: • Various testing scenarios based on threat likelihood • Identifying the critical systems required for business operations • Assigning roles and responsibilities in the event of a disaster • Assessing and mitigating risks identified as a result of the test disaster
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.	This criterion is the responsibility of the subservice organization. Refer to the Subservice Organizations section below 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.	This criterion is the responsibility of the subservice organization. Refer to the Subservice Organizations section below 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).	This criterion is the responsibility of the subservice organization. Refer to the Subservice Organizations section below 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 workstations 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.	Not applicable. The entity is not a covered entity.
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 data, hardware and software disposal and destruction.

PHYSICAL SAFEGUARDS		
Ref	**Regulation**	**Control Activity Specified by the Service Organization**
		The entity purges data stored on backup tapes and backup drives, per a defined schedule. The entity purges confidential data after it is no longer required to achieve the purpose for which the data was collected and processed. An inventory log is maintained of assets with confidential data, and as confidential data meets the retention period, the data is destroyed or purged. Policies and procedures are in place for removal of media storing critical data or software.
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.	The entity purges confidential data after it is no longer required to achieve the purpose for which the data was collected and processed. An inventory log is maintained of assets with confidential data. Confidential information is protected from erasure or destruction during the specified retention period.
164.310 (d)(2)(iii)	**Accountability:** Maintain a record of the movements of hardware and electronic media and any person responsible therefore.	Procedures are in place to provide for complete, accurate, and timely storage of data. Part of this criterion is the responsibility of the subservice organization. Refer to the Subservice Organizations section below for controls managed by the subservice organization.
164.310 (d)(2)(iv)	**Data backup and storage:** Create a retrievable, exact copy of ePHI, when needed, before movement of equipment.	The ways in which critical data are backed up and stored are documented and reviewed annually. Data backup and restore procedures are in place to guide personnel in performing backup activities. Full backups of certain application and database components are performed on a monthly basis and incremental backups are performed on a daily basis. When a backup job fails, the backup tool sends an alert to the backup administrators who investigate and resolve the failure. Data backed up is replicated to an offsite facility in real-time. Backups of critical data are maintained securely offsite by a third-party. Control self-assessments that include Backup restoration tests are performed on at least 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).	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.
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.	Documented policies and procedures are in place regarding system settings, authentication, access, and security monitoring.
	Network	
		Network user access is restricted via role-based security privileges defined within the access control system. Network audit logging settings are in place that include: • Account logon events • Account management • Directory Service Access • Logon events • Object access • Policy changes • Privilege use • Process tracking • System events Network audit logs are maintained and reviewed as needed.
	Operating System - SaaS Environment (Application, Web, and Database Servers)	
		Operating system user access is restricted via role-based security privileges defined within the access control system.

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 changes • Privilege use • Process tracking • System events 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. Database audit policy settings are in place that include: • Account logon event • Account management • Directory Service Access • Logon events • Object access • Policy changes • Privilege use • Process tracking • System events 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. Application audit policy settings are in place that include: • Account logon event • Account management • Directory Service Access • Logon events • Object access • Policy changes • Privilege use • Process tracking • System events Application audit logs are maintained and reviewed as needed.

TECHNICAL SAFEGUARDS		
Ref	**Regulation**	**Control Activity Specified by the Service Organization**
	Remote Access	
		VPN user access is restricted via role-based security privileges defined within the access control system. Access into the environment by outside entities requires a valid user ID and password and invalid login attempts are configured to be logged.
164.312 (a)(2)(ii)	**Emergency access procedure:** Establish (and implement as needed) procedures for obtaining necessary ePHI during an emergency.	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. A business continuity plan is documented and in place that outlines the range of disaster scenarios and steps the business will take in a disaster to ensure the timely resumption of critical business operations. The business continuity plan is tested on an annual basis and includes: • Various testing scenarios based on threat likelihood • Identifying the critical systems required for business operations • Assigning roles and responsibilities in the event of a disaster • Assessing and mitigating risks identified as a result of the test disaster The ways in which critical data are backed up and stored are documented and reviewed annually. Data backup and restore procedures are in place to guide personnel in performing backup activities. Full backups of certain application and database components are performed on a monthly basis and incremental backups are performed on a daily basis. When a backup job fails, the backup tool sends an alert to the backup administrators who investigate and resolve the failure. Data backed up is replicated to an offsite facility in real-time. Backups of critical data are maintained securely offsite by a third-party. Control self-assessments that include backup restoration tests are performed on at least an annual basis.
164.312 (a)(2)(iii)	**Automatic logoff:** Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.	Documented policies and procedures are in place regarding system settings, authentication, access, and security monitoring.

TECHNICAL SAFEGUARDS		
Ref	**Regulation**	**Control Activity Specified by the Service Organization**
	Network	
		Network account lockout settings are in place that include: • Account lockout duration • Account lockout threshold
	Operating System (Application, Web, and Database Servers)	
		Operating system account lockout settings are in place that include: • Account lockout duration • Account lockout threshold
	Database	
		Database account lockout settings are in place that include: • Account lockout duration • Account lockout threshold
	Application	
		Application account lockout settings are in place that include: • Account lockout duration • Account lockout threshold
	Remote Access	
		VPN account lockout settings are in place that include: • Account lockout duration • Account lockout threshold
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 TLS1.2 encryption with a trusted certificate authority. VPN, SSL and other encryption technologies are used for defined points of connectivity. Critical data is stored in encrypted format using AES, 3DES, RSA, ECC, DES and Diffie-Hellman.
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.	Regular monitoring and review of logins and log-in attempts to the system is in place. Discrepancies and potentially inappropriate or illegal activities are reported to senior management, legal counsel and/or human resources, as appropriate.

TECHNICAL 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 changes • Privilege use • Process tracking • System events 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 changes • Privilege use • Process tracking • System events Operating system audit logs are maintained and reviewed as needed.
	Database	
		Database audit logging settings are in place that include: • Account logon events • Account management • Directory Service Access • Logon events • Object access • Policy changes • Privilege use • Process tracking • System events Database audit logs are maintained and reviewed as needed.

TECHNICAL SAFEGUARDS		
Ref	**Regulation**	**Control Activity Specified by the Service Organization**
	Application	
		Application audit policy settings are in place that include: • Account logon events • Account management • Directory Service Access • Logon events • Object access • Policy changes • Privilege use • Process tracking • System events Application audit logs are maintained and reviewed as needed.
	Physical access	
		The badge access system logs successful and failed physical access attempts. The logs can be pulled for review if necessary.
164.312 (c)(1)	**Integrity:** Implement policies and procedures to protect ePHI from improper alteration or destruction.	Data that entered into the system, processed by the system and output from the system is protected from unauthorized access.
		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 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.	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 when thresholds have been exceeded.
		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 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	
		Network user access is restricted via role-based security privileges defined within the access control system.

TECHNICAL SAFEGUARDS		
Ref	**Regulation**	**Control Activity Specified by the Service Organization**
		Network administrative access is restricted to user accounts accessible by the following personnel: • Evolve Security Contractor • Software Architect • DevOps Engineer • Sr. QA Engineer • Director of Technology Networks are configured to enforce password requirements that include: • Password history • Password age (minimum and maximum) • Password length Network account lockout settings are in place that include: • Account lockout duration • Account lockout threshold Network audit logging settings are in place that include: • Account logon events • Object access • Policy changes • Process tracking • System events Network audit logs are maintained and reviewed as needed.
	Operating System (Application, Web, and Database Servers)	
		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: • Evolve Security Contractor • Software Architect • DevOps Engineer • Sr. QA Engineer • Director of Technology Operating systems are configured to enforce password requirements that include: • Password history • Password age (minimum and maximum) • Password length Operating system account lockout settings are in place that include: • Account lockout duration • Account lockout threshold

TECHNICAL SAFEGUARDS		
Ref	Regulation	Control Activity Specified by the Service Organization
		Operating system audit logging settings are in place that include: • Account logon events • Object access • Policy changes • Process tracking • System events 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. Database administrative access is restricted to user accounts accessible by the following personnel: • Software Architect • Sr. QA Engineer Databases are configured to enforce password requirements that include: • Password history • Password age (minimum and maximum) • Password length • Complexity Database account lockout settings are in place that include: • Account lockout duration • Account lockout threshold Database audit logging settings are in place that include: • Account logon events • Object access • Policy changes • Process tracking • System events 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.

TECHNICAL SAFEGUARDS		
Ref	**Regulation**	**Control Activity Specified by the Service Organization**
		Application administrative access is restricted to user accounts accessible by the following personnel: • Evolve Security Contractor • Software Architect • DevOps Engineer • Sr. QA Engineer • Director of Technology The application is configured to enforce password requirements that include: • Password history • Password age (minimum and maximum) • Password length • Complexity Application account lockout settings are in place that include: • Account lockout duration • Account lockout threshold Application audit policy settings are in place that include: • Account logon events • Object access • Policy changes • Process tracking • System events Application audit logs are maintained and reviewed as needed.
	Remote Access	
		VPN user access is restricted via role-based security privileges defined within the access control system. The ability to administer VPN access is restricted to user accounts accessible by the following personnel: • Software Architect • Director of Technology VPN users are authenticated via multi-factor authentication (username, password, and PIN/OTP/Token) prior to being granted remote access to the system. Access into the environment by outside entities requires a valid user ID and password and invalid login attempts are configured to be logged.
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 TLS1.2 encryption with a trusted certificate authority. VPN, SSL and other encryption technologies are used for defined points of connectivity.

TECHNICAL SAFEGUARDS		
Ref	Regulation	Control Activity Specified by the Service Organization
		Transmission of digital output beyond the boundary of the system is encrypted.
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 TLS1.2 encryption with a trusted certificate authority. VPN, SSL and other encryption technologies are used for defined points of connectivity. Transmission of digital output beyond the boundary of the system is encrypted. 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 when thresholds have been exceeded. 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 IT personnel via e-mail alert when a change to the production application code files is detected.
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 TLS1.2 encryption with a trusted certificate authority. VPN, SSL and other encryption technologies are used for defined points of connectivity. Transmission of digital output beyond the boundary of the system is encrypted. Critical data is stored in encrypted format using AES, 3DES, RSA, ECC, DES and Diffe-Hellman. Backup media is stored in an encrypted format.

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."	Not applicable. The entity has no Business Associate that access ePHI information, all is handled by internal employees and there is row security enable, in which they cannot have access to client data.
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."	Not applicable. The entity has no Business Associate that access ePHI information, all is handled by internal employees and there is row security enable, in which they cannot have access to client data.
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.	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.	Management reviews policies, procedures and other control documents for accuracy and applicability on an annual basis. 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, intranet.
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.	Management reviews policies, procedures and other control documents for accuracy and applicability on an annual basis. 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 intranet.
164.316 (b)(1)(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.	The entity retains all documentation for a minimum period of six (6) years from the date of its creation or modification, or the date when it was last in effect.
164.316 (b)(1)(ii)	**Availability:** Make documentation available to those persons responsible for implementing the procedures to which the documentation pertains.	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 intranet.

ORGANIZATIONAL REQUIREMENTS		
Ref	**Regulation**	**Control Activity Specified by the Service Organization**
164.316 (b)(1)(ii)	**Updates:** Review documentation periodically, and update as needed, in response to environmental or operational changes affecting the security of the ePHI.	Management reviews policies, procedures and other control documents for accuracy and applicability on an annual basis.

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. Notification procedures include: • Notice to parties alerting them to breaches “without unreasonable delay,” but no later than 60 days after discovery of the breach • Notice to covered entities when breach is discovered • Notice to the secretary of Human Health Services (HHS) and prominent media outlets about breaches involving more than 500 individual subject’s records • Notice to next of kin about breaches involving parties who are deceased • Notices to include what happened, the details of the breached unsecure PHI, steps to help mitigate harm to the party, and the covered entity’s response • Annual notice to the secretary of HHS 60 days before the end of the calendar year about unsecure PHI breaches involving fewer than 500 patient records
164.404 (a)(1)	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 (a)(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. Notification procedures include: • Notice to parties alerting them to breaches “without unreasonable delay,” but no later than 60 days after discovery of the breach • Notice to covered entities when breach is discovered • Notice to the secretary of Human Health Services (HHS) and prominent media outlets about breaches involving more than 500 individual subject’s records • Notice to next of kin about breaches involving parties who are deceased • Notices to include what happened, the details of the breached unsecure PHI, steps to help mitigate harm to the party, and the covered entity’s response • Annual notice to the secretary of HHS 60 days before the end of the calendar year about unsecure PHI breaches involving fewer than 500 patient records

BREACH NOTIFICATION		
Ref	Regulation	Control Activity Specified by the Service Organization
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 whose unsecured ePHI has been accessed during the breach is disclosed during notification procedures.
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.

BREACH NOTIFICATION		
Ref	**Regulation**	**Control Activity Specified by the Service Organization**
164.414	**Administrative requirements and burden of proof**: 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 Profisee was limited to the Trust Services Criteria and HIPAA/HITECH requirements, related criteria and control activities specified by the management of Profisee and did not encompass all aspects of Profisee's 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.

SECTION 5

OTHER INFORMATION PROVIDED BY THE SERVICE ORGANIZATION

MANAGEMENT'S RESPONSE TO TESTING EXCEPTIONS

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results	Management's Response
CC2.1	Data that entered into the system, processed by the system and output from the system is protected from unauthorized access.	Inspected IDPS configurations to determine that data entered into the system, processed by the system and output from the system was protected from unauthorized access.	Testing of the control activity disclosed that no IDPS configurations were made during the review period.	Profisee will deploy IDPS sensors as part of the 1.2 update to the SaaS environment. Data is inspected and sanitized prior to entry by the Profisee application.
CC3.1	Executive management has established key performance indicators for operational and internal controls effectiveness, including the acceptable level of control operation and failure.	Inspected the documented key performance indicators for operational and internal controls effectiveness to determine that executive management established key performance indicators for operational and internal controls effectiveness, including the acceptable level of control operation and failure.	Testing of the control activity disclosed that no performance metrics were made during the review period.	Profisee tracks OKRs (Objectives and Key Results) by department on a quarterly basis which are reviewed by the Profisee Board.
CC6.6	An Intrusion Detection and Prevention System (IDPS) is utilized to analyze network events and report possible or actual network security breaches.	Inspected the network diagram to determine that an IDPS was utilized to analyze network events and report possible or actual network security breaches.	Testing of the control activity disclosed that no IDPS configurations were made during the review period.	Profisee will deploy IDPS sensors as part of the 1.2 update to the SaaS environment.
CC6.7	The entity secures its environment a using multi-layered defense approach that includes firewalls, antivirus software and a DMZ.	Inspected the IDPS configurations to determine that the entity secured its environment a using multi-layered defense approach that included an IDPS.	Testing of the control activity disclosed that no IDPS configurations were made during the review period.	Profisee will deploy IDPS sensors as part of the 1.2 update to the SaaS environment. All other controls covered in CC6.7 were present.
CC7.1	The monitoring software is configured to alert IT personnel when thresholds have been exceeded.	Inspected an example log extract from the IDPS and an example IDPS alert notification to determine that the monitoring software was configured to alert IT personnel when thresholds were exceeded.	Testing of the control activity disclosed that no IDPS configurations were made during the review period.	Profisee will deploy IDPS sensors as part of the 1.2 update to the SaaS environment.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results	Management's Response
CC7.2	The monitoring software is configured to alert IT personnel when thresholds have been exceeded.	Inspected an example log extract from the IDPS and an example IDPS alert notification to determine that the monitoring software was configured to alert IT personnel when thresholds were exceeded.	Testing of the control activity disclosed that no IDPS configurations were made during the review period.	Profisee will deploy IDPS sensors as part of the 1.2 update to the SaaS environment.