Profisee

System and Organization Controls (SOC) for Service Organizations and Healthcare insurance Portability and Accountability Act (HIPAA)

SOC 2 + HIPAA

For The

Database and File Management Software Services

A Type II Report on Profisee Group, Inc.'s Description of Its System and on the Suitability of the Design and Operating Effectiveness of Its Controls Relevant to Security Trust Services Criteria, HIPAA Security Rule, and the HITECH Breach Notification Requirements

April 1, 2024, to March 31, 2025

AssurancePoint
CPAs and Compliance Advisors

Report of Independent Service Auditors issued by AssurancePoint, LLC

TABLE OF CONTENTS

SECTION 1 INDEPENDENT SERVICE AUDITOR'S REPORT 1

SECTION 2 MANAGEMENT'S ASSERTION 6

SECTION 3 DESCRIPTION OF THE SYSTEM 8

OVERVIEW OF OPERATIONS 9
PRINCIPAL SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS 9
COMPONENTS OF THE SYSTEM 10
SIGNIFICANT CHANGES DURING THE REVIEW PERIOD 14
SUBSERVICE ORGANIZATIONS 14
CONTROL ENVIRONMENT 15
RISK ASSESSMENT 17
CRITERIA AND RELATED CONTROL ACTIVITIES 18
COMMUNICATION AND INFORMATION SYSTEMS 19
MONITORING 19
SYSTEM INCIDENTS IDENTIFIED DURING THE REVIEW PERIOD 20
COMPLEMENTARY USER ENTITY CONTROLS 20

SECTION 4 TRUST SERVICES CRITERIA + HIPAA REQUIREMENTS, RELATED CONTROLS, AND TESTS OF CONTROLS 22

TESTS OF OPERATING EFFECTIVENESS AND RESULTS OF TESTS 23
SECURITY CATEGORY 25
HIPAA SECURITY RULE 47
HITECH BREACH NOTIFICATION RULE 82

SECTION 5 ADDITIONAL INFORMATION PROVIDED BY MANAGEMENT 87

SECTION I

INDEPENDENT SERVICE AUDITOR'S REPORT

INDEPENDENT SERVICE AUDITOR'S REPORT

To Profisee Group, Inc.:

Scope

We have examined Profisee Group, Inc.'s ("Profisee" or the "service organization") accompanying description of its Database and File Management Software Services system, in Section 3, throughout the period April 1, 2024, to March 31, 2025, (the "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 and operating effectiveness of controls stated in the description throughout the period April 1, 2024, to March 31, 2025, 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, *Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria),* and the information security program operated and conformed to the applicable implementation specifications within the Health Insurance Portability and Accountability Act ("HIPAA"") Security Standards for the Protection of Electronic Protected Health Information ("HIPAA Security Rule") and the Notification in the Case of Breach of Unsecured Protected Health Information enacted as part of the American Recovery and Reinvestment Act of 2009 ("HITECH Breach Notification Requirements"), (collectively, the "applicable HIPAA criteria"), as described in Part 164 of CFR 45, throughout the period April 1, 2024, to March 31, 2025, in accordance with the criteria set forth in Section 2 ("management's assertion").

Profisee uses a subservice organization for cloud hosting 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 and HIPAA criteria. The description presents Profisee's controls; the applicable trust services and HIPAA criteria; 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 information included in Section 5, "Other Information Provided by Profisee" is presented by Profisee management to provide additional information and is not a part of the description. Information about Profisee management's responses to exceptions noted 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 and HIPAA criteria.

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 and meet the HIPAA criteria. Profisee has provided the accompanying assertion, in Section 2, ("assertion") about the description and the suitability of design and operating effectiveness 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 and HIPAA criteria, 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 and operating effectiveness 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 and operated effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services and HIPAA criteria. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

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

An examination of the description of a service organization's system and the suitability of the design and operating effectiveness 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 or did not operate effectively;
- 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 on the applicable trust services and HIPAA criteria;
- Testing the operating effectiveness of controls stated in the description to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services and HIPAA criteria; and
- Evaluating the overall presentation of the description.

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

Inherent Limitations

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

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements are achieved based on the applicable trust services and HIPAA criteria. Also, the projection to the future of any conclusions about the suitability of the design and operating effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Description of Test of Controls

The specific controls we tested, and the nature, timing, and results of those tests are presented in section 4 of our report titled "Trust Services + HIPAA Criteria, Related Controls, and Tests of Controls."

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 throughout the period April 1, 2024, to March 31, 2025, in accordance with the description criteria;

b. the controls stated in the description were suitably designed throughout the period April 1, 2024, to March 31, 2025, to provide reasonable assurance that Profisee's service commitments and system requirements would be achieved based on the applicable trust services and HIPAA criteria, if its controls operated effectively throughout that period and if the subservice organization applied the complementary controls assumed in the design of Profisee's controls throughout that period; and

c. the controls stated in the description operated effectively throughout the period April 1, 2024, to March 31, 2025, to provide reasonable assurance that Profisee's service commitments and system requirements were achieved based on the applicable trust services and HIPAA criteria, if complementary subservice organization controls assumed in the design of Profisee's controls operated effectively throughout that period.

Emphasis-of-Matter

Profisee's description of its Database and File Management Software Services system states that incidents are documented and tracked in a standardized ticketing system; updated to reflect the planned incident and problem resolution; and analyzed to determine the root cause and system impact. The system also states that security incidents resulting in the unauthorized use or disclosure of personal information are communicated to the affected users. However, during the period April 1, 2024, to March 31, 2025, there were no security incidents identified by Profisee that would warrant the operation of the aforementioned controls. Because those controls did not operate during the period, we were unable to test, and did not test, the operating effectiveness of those controls as evaluated using trust services criteria: CC7.3, "The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures"; and 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"; and HIPAA criteria §164.308(a)(6)(ii), "Response and Reporting"; §164.410, "Notification by a Business Associate"; and §164.414(b), "Burden of proof" as defined in Section 4. Our opinion is not modified with respect to this matter.

Restricted Use

This report, including the description of tests of controls and results thereof in section 4, is intended solely for the information and use of Profisee; user entities of Profisee's Database and File Management Software Services system during some or all of the period April 1, 2024, to March 31, 2025, 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 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 and HIPAA criteria; and
- 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.

AssurancePoint, LLC

Atlanta, Georgia
July 2, 2025

SECTION 2

MANAGEMENT'S ASSERTION

MANAGEMENT'S ASSERTION

We have prepared the accompanying description of Profisee's Database and File Management Software Services system, in Section 3, throughout the period April 1, 2024, to March 31, 2025, (the "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, *Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria),* and the information security program operated and conformed to the applicable implementation specifications within the Health Insurance Portability and Accountability Act ("HIPAA") Security Standards for the Protection of Electronic Protected Health Information ("HIPAA Security Rule") and the Notification in the Case of Breach of Unsecured Protected Health Information enacted as part of the American Recovery and Reinvestment Act of 2009 ("HITECH Breach Notification Requirements"), (collectively, the "applicable HIPAA criteria"), as described in Part 164 of CFR 45.

Profisee uses a subservice organization for cloud hosting 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 and HIPAA criteria. The description presents Profisee's controls; the applicable trust services and HIPAA criteria; 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.

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 throughout the period April 1, 2024, to March 31, 2025, in accordance with the description criteria;

b. the controls stated in the description were suitably designed throughout the period April 1, 2024, to March 31, 2025, to provide reasonable assurance that Profisee's service commitments and system requirements would be achieved based on the applicable trust services and HIPAA criteria, if its controls operated effectively throughout that period, and if the subservice organizations applied the complementary controls assumed in the design of Profisee's controls throughout that period; and

c. the controls stated in the description operated effectively throughout the period April 1, 2024, to March 31, 2025, to provide reasonable assurance that Profisee's service commitments and system requirements were achieved based on the applicable trust services and HIPAA criteria if complementary subservice organization controls assumed in the design of Profisee's controls operated effectively throughout that period.

Oue description of our Database and File Management Software Services system states that incidents are documented and tracked in a standardized ticketing system; updated to reflect the planned incident and problem resolution; and analyzed to determine the root cause and system impact. Our system also states that security incidents resulting in the unauthorized use or disclosure of personal information are communicated to the affected users. However, during the period April 1, 2024, to March 31, 2025, there were no security incidents identified that would warrant the operation of the aforementioned controls. Because those controls did not operate during the period, we were unable to demonstrate the operating effectiveness of those controls as evaluated using trust services criteria: CC7.3, "The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures"; and 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"; and the HIPAA criteria §164.308(a)(6)(ii), "Response and Reporting"; §164.410, "Notification by a Business Associate"; and §164.414(b), "Burden of proof" as defined in Section 4.

SECTION 3

DESCRIPTION OF THE SYSTEM

Overview of Operations

Company Background

Founded in 2007 and headquartered in Atlanta, Georgia, Profisee is a leading global provider of cloud native Master Data Management (MDM) software. Profisee's MDM solution helps organizations realize the full potential of their data by unifying data from disparate systems, enhancing incomplete information, correcting duplicate or incorrect records, and continually harmonizing data across data silos, creating a trusted foundation of a company's critical information.

Profisee operates directly in the United States, Europe, and Australia, and extends its global reach through a network of value-added resellers, systems integrators, and professional consulting firms. Profisee provides 24/7 global customer support and is focused on delivering scalable and secure master data management solutions to organizations across a variety of industries.

Description of Services Provided

The Database and File Management Software Services is a cloud-native MDM platform that helps organizations create a trusted, consistent view of their critical data. It enables standardization, validation, and synchronization across disparate systems, reducing duplication and inaccuracies to support better data governance and reporting.

The platform offers flexible deployment options — Software-as-a-Service (SaaS), on-premise, and hybrid—allowing customers to meet their infrastructure and compliance needs. Designed to lower total cost of ownership and speed implementation, it includes automation and AI features to enhance data stewardship. The scope of this report is limited to the SaaS deployment model.

Principal Service Commitments and System Requirements

Profisee designs its processes and procedures related to its Database and File Management Software Services system to meet its objectives for its SaaS platform. These objectives are based on the service commitments that Profisee makes to user entities; the laws and regulations that govern the provision of SaaS services; and the financial, operational, and compliance requirements that Profisee has established for the services.

Commitments are declarations made by management to customers regarding the performance of the Database and File Management Software Services system. Security commitments are documented and communicated in the Profisee SaaS Subscription Agreement, which is required to be signed by for customers using the SaaS model. The principal security commitments are standardized and include the following:

- Profisee's security policies and practices are made accessible on the company's website.
- Profisee shall not access customer user accounts, including customer data, except to respond to service or technical problems or at the customer's request.
- Only Designated Support Contacts (DSCs) are authorized to register support issues on the customers' behalf and respond to registered support issues. In limited cases, and at Profisee's discretion, additional users with production-related questions will be allowed to temporarily register support issues, with all related communications copied to registrant and DSCs.
- Profisee will provide support services for customers during support hours (8:30AM to 8:00PM, Eastern Time) on business days with observance of public holidays. Profisee has defined priority levels and response time SLAs to respond to support issues during support hours.
- A Profisee Support Portal is available for customers as a special extension of Profisee's website and is only available to registered users.

- In the case any special patch version or hotfix is developed, especially for a customer as a result of a support issue, Profisee will, provided the customer makes models and databases available, test the fix-on-fail release against the customer's model specifically.
- Escalation procedures are made available for customers in the event that a customer is unable to solve a problem or issue with the assistance of Profisee. Escalation procedures define escalation levels and include contact information for each escalation level.

Profisee establishes operational requirements that support the achievement of security commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in Profisee's system policies and procedures, system design documentation, and the SaaS Subscription Agreement. Information security policies define an organization-wide approach to how systems and data are protected. These include policies around how the service is designed and developed; how the system is operated; how the internal business systems and networks are managed; and how employees are hired and trained. In addition to these policies, standard operating procedures have been documented on how to carry out specific manual and automated processes required in the operation and development of the Database and File Management Software Services system.

In accordance with our assertion, and the description criteria, the aforementioned service commitments and requirements are those principal service commitments and requirements common to the broad base of users of the system and may therefore not fully address the specific service commitments and requirements made to all system users, in each individual case.

COMPONENTS OF THE SYSTEM

System Boundaries

A system is designed, implemented, and operated to achieve specific business objectives in accordance with management-specified requirements. The purpose of the system description is to delineate the boundaries of the system, which includes the services outlined above and the five components described below: infrastructure, software, people, procedures, and data.

Infrastructure and Software

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.

Primary infrastructure used to provide the Database and File Management Software Services System includes the following:

Primary Infrastructure	
Infrastructure Component	**Business Function Description**
Azure Kubernetes Services	Managed Kubernetes service utilized to deploy and manage Kubernetes clusters within the production cloud environment for SaaS environment
Azure Virtual Machines	Virtual servers hosting the SaaS environment including jump box virtual servers used to control access.
SQL Databases	Host data for SaaS customers
Azure VPN	Virtual private network (VPN) services to establish secured connections to SaaS environment
Terraform	Infrastructure as Code (IaC) services

Primary Infrastructure	
Infrastructure Component	**Business Function Description**
Microsoft Entra	Provides authentication and Single Sign-On (SSO) services for the SaaS environment by utilizing Azure Active Directory (AD) for internal users, and customers integrate their Azure AD for SSO authentication to the Profisee SaaS environment.

Additionally, the following secondary systems and software are used to support the system:

Secondary Systems and Software	
Software	**Business Function Description**
Azure Firewall	Web application firewall monitoring the production SaaS environment. Also provides intrusion detection prevention system (IDPS) services
Azure DevOps	CI/CD system that provides version control and source code repository services
Microsoft Intune	Mobile Device Management for workstations
Microsoft Defender	Anti-malware and data loss prevention for workstations
Microsoft Defender for Cloud	Anti-malware and data loss prevention for production servers and databases
Microsoft Sentinel	Provides Security Information and Event Management (SIEM) services and alerting
Azure Key Vault	Provides secure storage of managed secrets such as encryption keys
Freshservice	Ticketing system used for system access provisioning and security incident tracking
Profisee Support Portal	Customer support portal
Office 365 suite	Business communications and internal SharePoint

People

Personnel involved in the operation and use of the system are:

- **Executive Team** – 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.
- **SaaS Operations** – Responsible for 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** – Responsible for the operation, maintenance and administration of any device, IT service, hardware, software, or network service.
- **Security** – Responsible for implementing and managing the organization's security policies, monitoring security events, and ensuring compliance with security requirements. This team may work in coordination with IT and SaaS Operations but is called out separately to reflect its role in safeguarding systems and data.
- **Sales** – Responsible for providing demonstration of the product, working with prospective customers, answers questions and any other activity during the sales process.
- **Professional Services** – Responsible for providing troubleshooting, aiding in the deployment of Profisee and resolving issues a customers may have in 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.
- **People Operations (Human Resources (HR))** – Responsible for HR-related controls that support overall system operations, including employee onboarding, role-based access, background checks, training, and other activities that ensure personnel meet the organization's security and compliance requirements.

Data and Electronic Protected Health Information (ePHI)

Data that is uploaded to the Database and File Management Software Services system is at the discretion of the customer who retains ultimate ownership of data and ePHI that is stored. Profisee processes and stores any data and ePHI that a customer uploads.

Because Profisee does not have insight into customer data, all data is treated with equal protection, which may include ePHI data. Data is stored, processed or otherwise hosted on technologies described above, within Microsoft Azure cloud premises. Customers are able to utilize Profisee's MDM platform as a Service offering to clean, update and master their data, on secure systems.

Procedures

Logical Access Infrastructure, Software, and Architecture

Logical access controls have been implemented to restrict system access to authorized personnel and to enforce consistent authentication and authorization requirements across infrastructure components. An inventory of system assets and components is maintained to classify and manage information assets subject to logical access controls.

The company's network domains is composed of a corporate network domain and a production network domain. The network domains are configured using Microsoft Entra to authenticate users via unique user accounts and enforce minimum password requirements, including multi-factor authentication (MFA). Account lockout thresholds and durations are also configured to mitigate brute-force attacks. Administrative access privileges to network domains are restricted to user accounts assigned to authorized IT personnel.

Production servers and databases are configured to enforce SSO authentication and inherit the same password and MFA requirements defined by the corporate and production network domains. Administrative access to these systems is restricted to authorized IT personnel. Role-based access is assigned through predefined user access groups that segment access based on job responsibilities and system requirements.

Remote access to internal systems is provided through Azure VPN. VPN users are required to authenticate using multi-factor authentication. The ability to administer VPN access is restricted to authorized IT personnel.

Workstations are configured to automatically terminate inactive sessions after five minutes of inactivity using Microsoft Intune configuration settings. Production data is encrypted at rest, and encryption keys are securely stored and managed using Azure Key Vault.

Access Authorization and Access Revocation

Logical access to systems is provisioned based on formal procedures designed to enforce the principle of least privilege and ensure that access aligns with job responsibilities. System access for new personnel is approved and initiated by authorized HR personnel through a documented onboarding ticketing process. Upon approval, IT personnel provision access based on predefined role requirements.

Profisee personnel access to production databases containing customer data is further restricted. Requests for such access must include documented business justification and requires the submission of a customer support portal ticket. Such access is limited to support-related purposes.

Access revocation is performed as part of the personnel termination process. Upon notification of termination or role change, IT personnel revoke system access in coordination with HR to ensure removal is completed. This process includes disabling user credentials and removing access to relevant systems, including production resources.

Perimeter Security and Data Transmissions

Perimeter and endpoint security controls are implemented to monitor and restrict unauthorized access, protect sensitive information, and reduce exposure to known vulnerabilities. Azure Firewall is used as the firewall system and is deployed to filter unauthorized inbound network traffic from external sources. In addition, the firewall system provides IDPS services and is configured to monitor network activity and generate alerts to designated personnel upon detection of potential or actual security breaches.

Remote connectivity is conducted through encrypted VPN sessions via Azure VPN to protect access to internal systems over public networks. Production web application sessions are encrypted using secure transport protocols to ensure the confidentiality of data transmitted over the Internet.

Microsoft Intune is used to centrally manage personnel workstations. Workstations are configured with disk encryption to protect data stored locally and are restricted from writing to removable storage devices to reduce the risk of data loss or exfiltration. System updates and patches are required to be installed according to defined maintenance schedules to ensure workstations remain protected against known threats.

Microsoft Defender for Cloud is configured to provide continuous vulnerability scanning for production machines to proactively identify security vulnerabilities. In addition, third-party penetration testing is conducted at least annually for both the web application and the internal network. These tests are performed to identify and assess potential exploitable vulnerabilities within the environment and are used to inform the organization’s remediation efforts.

Access to backup systems is restricted to authorized SaaS Operations personnel. Controls are in place to ensure that only designated individuals may initiate backup recovery or restoration activities.

Anti-malware

Centrally managed antivirus software is installed on employee workstations, production servers, and databases to detect and prevent malware threats. Endpoint protection for employee workstations is managed through Microsoft Defender, which provides real-time scanning, threat detection, and response capabilities.

For server infrastructure, Microsoft Defender for Cloud is utilized to monitor production systems. Defender for Cloud provides continuous threat monitoring, including malware detection, and integrates with the organization’s SIEM tool Microsoft Sentinel to support centralized alerting and response.

System Monitoring

System monitoring controls are established to support the identification and investigation of security events. Management has defined configuration standards within the organization’s documented information security policies and procedures. These standards provide baseline requirements for system setup to ensure that deployed infrastructure aligns with security expectations.

Policies and procedures are also in place to support the detection, logging, and monitoring of unknown or unauthorized components introduced into the environment. These procedures outline the responsibilities for identifying deviations from approved configurations and specify requirements for the generation and review of system event logs to detect potential security incidents.

Additional system monitoring controls related to the firewall system, IDPS, vulnerability scanning, and penetration testing, please refer to the *Perimeter Security and Data Transmissions* section above.

Incident Response

Documented incident response policies and procedures define roles, responsibilities, and required activities for analyzing, responding to, communicating, and recovering from security incidents. These procedures include guidance for considering applicable laws, regulations, or statutory requirements that may impact the resolution of an incident.

Incidents are documented and tracked in a standardized ticketing system and updated to reflect the planned incident and problem resolution. Security incident analyses are performed to determine the root cause and assess the impact on systems. Security incidents that result in unauthorized use or disclosure of personal information are communicated to the affected users.

Management reviews the company's incident response and escalation procedures annually to evaluate their effectiveness. A disaster recovery and business continuity plan is documented to identify and reduce risks, limit the consequences of damaging incidents, and ensure the timely resumption of essential operations.

Change Management

Documented change control policies and procedures are in place to guide personnel in the change management process. System change requests are documented and tracked in a ticketing system to ensure that changes are reviewed, authorized, and implemented in a controlled manner.

Application changes are tested prior to implementation, and system changes require management authorization and approval before being deployed to the production environment. Back out procedures for production application changes are documented to support rollback in the event that changes impair system functionality.

The organization utilizes Azure DevOps as its CI/CD system. The CI/CD system is configured to require at least one peer reviewer before code can be merged into the production branch. Version control and rollback capabilities are in place to support the integrity of source code repositories.

Administrative access to the CI/CD system is restricted to authorized IT personnel. The ability to migrate changes into the production environment is limited to authorized users. Development and test environments are logically separated from the production environment to prevent unauthorized or unintended changes from affecting live systems.

Significant Changes During the Review Period

There were no significant changes that are likely to affect report users' understanding of how the in-scope system is used to provide the services covered by this examination during the period.

Subservice Organizations

The cloud hosting services provided by Microsoft Azure was not included within the scope of this examination.

The following table presents the applicable trust services and HIPAA criteria that are intended to be met by controls at Microsoft Azure, alone or in combination with controls at Profisee, and the types of controls expected to be implemented at Microsoft Azure to achieve Profisee's service commitments and system requirements based on the applicable trust services and HIPAA criteria.

Control Activity Expected to be Implemented by Microsoft Azure	Applicable Trust Services and HIPAA Criteria
Microsoft Azure is responsible for restricting physical access to data centers housing hardware and physical infrastructure in which production data resides.	CC6.4 §164.310(a)(1) §164.310(a)(2)(i) §164.310(a)(2)(ii) §164.310(a)(2)(iii) §164.310(a)(2)(iv)
Microsoft Azure is responsible for diminishing the ability to read and recover data and software from physical assets prior to discontinuing logical and physical protections over those assets.	CC6.5
Microsoft Azure is responsible for controlling the receipt and removal of hardware and electronic media for the data centers housing physical infrastructure in which production data resides.	§164.310(d)(1)
Microsoft Azure is responsible for addressing the final disposition of hardware and electronic media for the data centers housing physical infrastructure in which production data resides.	§164.310(d)(2)(i)
Microsoft Azure is responsible for implementing procedures regarding the removal and re-use of electronic media related to the data centers housing physical infrastructure in which production data resides.	§164.310(d)(2)(ii)
Microsoft Azure is responsible for maintaining a record of the movements of hardware and electronic media for the data centers housing physical infrastructure in which production data resides.	§164.310(d)(2)(iii) §164.310(d)(2)(iv)

Control Environment

The control environment at Profisee is the foundation for the other areas of internal control. It sets the tone of the organization and influences the control consciousness of its personnel. The components of the control environment factors include the integrity and ethical values; management's commitment to competence; its organizational structure; the assignment of authority and responsibility; and the oversight and direction provided by executive management and the Information Security Committee (ISC).

Integrity and Ethical Values

Profisee has established a formal control environment that emphasizes integrity and ethical behavior through documented policies and personnel practices. An Employee Handbook is maintained that includes a code of conduct and outlines workforce conduct standards and enforcement procedures. The handbook defines disciplinary actions, including suspension or termination, for violations of stated policies.

Employees are required to acknowledge the Employee Handbook during the onboarding process. The handbook includes confidentiality and nondisclosure requirements designed to support ethical handling of sensitive information. In addition, organizational and information security policies and procedures are documented and made available to personnel through the company's SharePoint site to promote awareness and understanding of expected behaviors.

As part of the hiring process, background checks are performed for new employees to validate candidate integrity. Management also performs performance and conduct evaluations on at least an annual basis to assess employee behavior and competencies in alignment with company expectations.

Executive Management and ISC Oversight

Profisee has established formal governance structures to oversee the development and performance of internal controls and the organization's information security program. A documented Security Governance Policy defines oversight, structures, authorities, and responsibilities related to information security management.

Policies and procedures assign responsibility for the design, implementation, and maintenance of internal controls to designated individuals and teams across the organization. The ISC is responsible for coordinating the development and implementation of security requirements aligned with the organization's information security objectives.

An annual information security meeting is conducted by the ISC to review the performance of the information security program and communicate findings and priorities to the CEO. In addition, the Information Security Team holds weekly meetings to review the Security Planner tracker, which is used to monitor the status and progress of ongoing security initiatives.

Organizational Structure and Assignment of Authority and Responsibility

Profisee has established an organizational structure that defines reporting lines, roles, and areas of responsibility. A documented organizational chart is maintained within the HR system to outline the company's structure and formal lines of authority. Job descriptions are documented for new employees and define specific roles and responsibilities aligned with organizational objectives.

Oversight for the information security program is defined within the company's Security Governance Policy, which outlines structures, authorities, and responsibilities related to internal control. Policies and procedures formally assign accountability for the development and operation of internal controls to designated individuals and teams across the organization.

The ISC is responsible for coordinating the implementation of information security requirements. The Information Security Team supports this oversight through weekly meetings to review the Security Planner tracker, which is used to track ongoing security initiatives and operational tasks.

Commitment to Competence

Profisee has established policies and procedures to promote the hiring and development of competent personnel. Screening and competency requirements for candidates are defined as part of the hiring process, and job descriptions are documented for new employees to outline roles and responsibilities.

New employees receive security training during the onboarding process to ensure awareness of relevant policies and expected practices. In addition, management utilizes a security training system to conduct annual phishing exercises as part of its ongoing efforts to assess and reinforce employee security awareness.

Management also performs annual performance and conduct evaluations to assess employee skills, role alignment, and adherence to organizational expectations. These activities support the organization's commitment to maintaining a competent workforce capable of meeting internal control and security objectives.

Accountability

Profisee has implemented controls to promote individual accountability for internal control responsibilities. Job descriptions are documented for new employees and define the roles and responsibilities associated with each position.

An Employee Handbook is maintained to communicate workforce conduct standards and enforcement procedures. The handbook includes a code of conduct and outlines disciplinary actions, including termination or suspension, for violations of established policies. Employees are required to acknowledge the Employee Handbook during onboarding, including acceptance of confidentiality and nondisclosure requirements.

Management conducts performance and conduct evaluations on at least an annual basis to assess whether employees are fulfilling their assigned responsibilities and adhering to organizational standards. These measures support the enforcement of accountability across the organization.

Risk Assessment

Profisee has implemented a risk assessment program to identify, assess, and respond to risks that could affect the achievement of its information security objectives. The risk assessment process considers internal and external threats, evaluates the potential for fraud, and supports the implementation of appropriate risk mitigation strategies. The program is supported by documented policies and oversight activities that ensure risks are addressed in a structured and consistent manner.

Objective Setting

Profisee maintains a documented Security Objectives Guidelines policy that defines information security objectives to ensure alignment with business goals, identified information security risks, and applicable regulatory requirements. Management performs an annual risk assessment to identify risks that could impact the achievement of the company's information security objectives. Identified risks are assessed using a risk rating methodology to support prioritization and alignment of the organization's security program with its defined objectives.

Risk Identification and Analysis

Profisee has defined a formal risk assessment policy that outlines the process for identifying and evaluating internal and external threats and vulnerabilities, establishing risk tolerances, and selecting risk treatment responses. The policy includes procedures for assessing how risks may impact the achievement of system commitments and information security objectives.

The annual risk assessment process is used to identify and evaluate risks that could affect the organization's ability to meet its objectives. This process includes the consideration of internal and external factors, including changes in vendor and third-party relationships. The risk assessment process also includes the identification and assessment of fraud risks that could impact the achievement of objectives. As part of this process, management considers factors related to incentives, opportunities, employee conduct, and technology-related threats that could enable or justify fraudulent activity. Identified risks are assessed using a documented risk rating methodology.

Risk Mitigation

Profisee has established a formal process for selecting and implementing risk treatment plans based on the results of its annual risk assessment. Treatment plans include the implementation of mitigating controls to reduce residual risk to acceptable levels and are assigned to designated process owners for execution. The use of technology in the design and selection of controls is evaluated by management as part of the annual risk assessment process. Third-party risk is also considered within the annual risk assessment.

Profisee conducts an internal audit of its information security management system and internal controls annually to assess the appropriateness and effectiveness of the controls in place.

An annual information security meeting is conducted by the ISC to report on the performance of the information security program to the CEO and support strategic risk mitigation efforts. Additionally, the Information Security Team meets weekly to review the Security Planner tracker, which documents ongoing initiatives and control activities.

Business continuity and disaster recovery controls have been established to support risk mitigation. Profisee maintains a documented disaster recovery and business continuity plan designed to reduce the impact of damaging incidents and ensure the timely resumption of operations. The plan is updated and approved annually, and a disaster recovery failover test that includes data backup restoration is performed each year. Full and incremental backups of SQL databases are completed according to predefined schedules.

To further mitigate risk, Profisee maintains cybersecurity insurance to help offset the financial impact of critical security incidents or vulnerability exploitation. Documented policies are in place for managing third parties, and management obtains and reviews compliance reports from vendors on an annual basis to evaluate the effectiveness of controls within the vendor environments.

Criteria and Related Control Activities

Selection and Development of Control Activities

The applicable trust services criteria and HIPAA requirements were used to evaluate the suitability of the design and operating effectiveness of controls stated within the description. The criteria and related control activities designed, implemented, and operated to meet them are included in Section 4 of this report. Although the applicable criteria and related control activities are included in Section 4, they are, nevertheless, an integral part of Profisee's description of the system.

Trust Services Criteria Not Applicable to the In-Scope System

All criteria within the security category are applicable to the Database and File Management Software Services system.

HIPAA Requirements Not Applicable to the In-Scope System

The HIPAA requirements presented below are not applicable to the Database and File Management Software Services system within the scope of this examination. As a result, an associated control is not required to be in place at the service organization for the omitted applicable HIPAA requirement. The following table presents the HIPAA requirements that are not applicable for the Database and File Management Software Services system at Profisee. The HIPAA requirements that are not applicable are also described in Section 4.

Requirement #	Reason for Omitted Requirment
HIPAA Security Rule	
§164.308(a)(4)(ii)(A)	Profisee is not a covered entity or a health care clearinghouse.
§164.308(b)(1)	Profisee is not a covered entity.
§164.314(a)(2)(ii)	Profisee is not a covered entity or government entity.
§164.314(a)(b)(1)	Profisee is not a group health plan.
§164.314(b)(2)	Profisee is not a group health plan.
HITECH Breach Notification	
§164.404(a)(1)	Profisee is not a covered entity.
§164.404(a)(2)	Profisee is not a covered entity.
§164.404(b)	Profisee is not a covered entity.
§164.404(c)	Profisee is not a covered entity.
§164.404(d)	Profisee is not a covered entity.
§164.406	Profisee is not a covered entity.
§164.408	Profisee is not a covered entity.
§164.414(a)	Profisee is not a covered entity.

Communication and Information 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. Profisee maintains documented architecture diagrams to identify system components, data flows, and network segmentation. These diagrams support understanding of the system design and communication pathways. Management reviews policies, procedures, and other control documents on at least an annual basis to ensure accuracy and continued relevance.

Production resources are reviewed annually by SaaS Operations personnel for relevance and active use. Additionally, Profisee conducts an internal audit of its information security management system and internal controls each year to evaluate control effectiveness and alignment with internal requirements.

Internal Communications

Organizational and information security policies and procedures are documented and made available to personnel through Profisee's SharePoint site. Security training is provided during the onboarding process to communicate relevant responsibilities to employees. Job descriptions and an Employee Handbook are maintained to define individual roles and conduct expectations. Documented incident response procedures are in place to guide personnel in reporting and escalating security incidents.

All-hands meetings are conducted at least monthly to provide organizational updates. The ISC holds an annual meeting to review and report on the performance of the information security program to the CEO.

External Communications

Security commitments and customer responsibilities are documented in the SaaS subscription agreement. The agreement also defines procedures for customers to report system issues through a support portal. A structured escalation path and priority-based response times are established to ensure appropriate handling of customer-reported issues.

Monitoring

Management monitors controls to ensure that they are operating as intended and that controls are modified as conditions change. 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 are also monitored.

Ongoing Monitoring and Separate Evaluations

Profisee has implemented ongoing monitoring and separate evaluation activities to assess the effectiveness of internal controls and the information security program. The Information Security Team conducts weekly meetings to review the Security Planner tracker, which is used to monitor the status of security initiatives and control activities.

An annual information security meeting is conducted by the ISC to review the performance of the security program and report findings and priorities to the CEO. In addition, Profisee conducts an internal audit of its information security management system and internal controls on an annual basis to evaluate the design and operating effectiveness of control activities and identify areas for improvement.

Subservice Organization Monitoring

Profisee's management team reviews third-party compliance reports (such as SOC 2) on at least an annual basis for subservice organizations to help ensure that the subservice organizations comply with the organization's security requirements. This process includes a review of issues or deviations noted in the reports and an evaluation to determine their impact on the service. Profisee also monitors external communications, such as customer complaints relevant to the services provided by the subservice organization.

Evaluating and Communicating Deficiencies

Profisee has developed protocols to help ensure findings of internal control deficiencies are reported to the individuals responsible for the function or activity involved and are in a position to take corrective action. This process enables responsible individuals to provide needed support or oversight for taking corrective action, and to communicate with others in the organization whose activities may be affected.

Deficiencies in the internal control system may surface from multiple sources, including the company's ongoing monitoring procedures, separate evaluations of the internal control system, and external parties. To facilitate the evaluation and communication of internal control deficiencies, Profisee has implemented procedures to evaluate and communicate control deficiencies through a combination of operational oversight, internal audit activities, and incident reporting processes. The Information Security Team conducts weekly meetings to review the Security Planner tracker, which monitors the status of security initiatives and identifies potential gaps in control performance. An annual information security meeting is conducted by the ISC to assess the performance of the information security program and report outcomes to the CEO. Profisee also conducts an internal audit of its information security management system and internal controls annually to evaluate the design and operating effectiveness of controls and to identify deficiencies requiring remediation. In addition, documented incident response procedures are in place to ensure that security incidents are properly identified, reported, and communicated to appropriate stakeholders. These procedures support timely evaluation of control breakdowns and the implementation of corrective actions.

System Incidents Identified During the Review Period

No incidents were identified or reported during the review period of this report that could have impaired the achievement of our service commitments, system requirements, or the HIPAA criteria.

Complementary User Entity Controls

Profisee's controls are designed to provide reasonable assurance that the principal service commitments, system requirements, and HIPAA criteria can be achieved without the implementation of complementary controls at user entities. As a result, complementary user entity controls are not required, or significant, to achieve the principal service commitments and system requirements based on the applicable trust services and HIPAA criteria.

User Entity Responsibilities

However, in order for user entities to benefit from the Database and File Management Software Services system and its controls, the following responsibilities should be considered by user entities:

#	User Entity Responsibilities
1.	User entities are responsible for implementing internal controls regarding general IT system access and system usage appropriateness for internal user organization components associated with Profisee.
2.	User entities are responsible for 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.	User entities are responsible for implementing security controls to protect any data sent to Profisee.
4.	User entities are responsible for implementing controls that require approval procedures for critical transactions relating to Profisee's services.
5.	User entities are responsible for reporting to Profisee any material changes to their overall control environment that may adversely affect services being performed by Profisee.
6.	User entities are responsible for notifying Profisee of any changes to personnel directly involved with services performed by Profisee.

#	User Entity Responsibilities
7.	User entities are responsible for adhering to the terms and conditions stated within their SaaS subscription agreements with Profisee.
8.	User entities are responsible for developing, and if necessary, implementing a business continuity and disaster recovery plan that will aid in the continuation of services provided by Profisee.

SECTION 4

TRUST SERVICES CRITERIA + HIPAA REQUIREMENTS, RELATED CONTROLS, AND TESTS OF CONTROLS

TESTS OF OPERATING EFFECTIVENESS AND RESULTS OF TESTS

Scope

This report relates to the Database and File Management Software Services system provided by Profisee and the relevant controls designed and operated during the period April 1, 2024, to March 31, 2025, specified by management of Profisee that are believed by management to be relevant to user entities of this report. The scope of AssurancePoint's testing was restricted to the Trust Services and HIPAA criteria selected by management of Profisee and the boundaries of the Database and File Management Software Services system defined in Section 3. AssurancePoint's examination was performed in accordance with American Institute of Certified Public Accountants ("AICPA") Statements on Standards for Attestation Engagements, specifically AT-C section 105 *"Concepts Common to All Attestation Engagements"* and AT-C section 205, *"Examination Engagements"*.

Tests of Operating Effectiveness

The tests applied by AssurancePoint to test the operating effectiveness of controls are listed alongside each of the respective control activities within the Testing Matrices. Such tests were considered necessary to evaluate whether the controls were sufficient to provide reasonable, but not absolute, assurance that the applicable trust services and HIPAA criteria were achieved during the review period. In selecting tests of controls, AssurancePoint considered various factors, including but not limited to, the following:

- The nature of the control and the frequency with which it operates
- The control risk mitigated by the control
- The effectiveness of entity-level controls
- The degree to which the control relies on the effectiveness of other controls
- Whether the control is performed manually or is automated

The types of tests performed with respect to the operating effectiveness of the control activities detailed in this section are described below:

Test Approach	Description
Inquiry	Inquired of relevant personnel with the requisite knowledge and experience regarding the performance and application of the related control activity. This included in-person interviews, telephone calls, e-mails, web-based conferences, or a combination of the preceding. Inquiry alone is not deemed sufficient to evidence operating effectiveness of a control activity and is always accompanied by a testing method that provides greater levels of assurance.
Observation	Observed the relevant processes or procedures during fieldwork. This included, but was not limited to, witnessing the performance of controls or evidence of control performance with relevant personnel, systems, or locations relevant to the performance of control policies and procedures.
Inspection	Inspected the relevant audit records. This included, but was not limited to, documents, system configurations and settings, or the existence of sampling attributes, such as signatures, approvals, or logged events. In some cases, inspection testing involved tracing events forward to consequent system documentation or processes (e.g., resolution, detailed documentation, alarms, etc.) or vouching backwards for prerequisite events (e.g., approvals, authorizations, etc.).
Re-performance	Re-performed procedures or controls that were originally performed by the service organization to independently validate conclusions or results.

Sampling

Consistent with AICPA authoritative literature, AssurancePoint utilizes professional judgment to consider the tolerable deviation rate, the expected deviation rate, the audit risk, the characteristics of the control population, and other factors, in order to determine the number of items to be selected in a sample for a particular test. AssurancePoint, in accordance with AICPA authoritative literature, selected samples in such a way that the samples were expected to be representative of the population. This included judgmental selection methods, where applicable, to ensure representative samples were obtained.

System-generated population listings were obtained whenever possible to ensure completeness prior to selecting samples. In some instances, full populations were tested in cases including, but not limited to, the uniqueness of the event or low overall population size.

Reliability of Information Provided by the Service Organization

Observation and inspection procedures were performed related to certain system-generated reports, listings, and queries to assess the accuracy and completeness (reliability) of the information used in the performance of our testing of the controls.

Results of Tests

The results of each test applied are listed alongside each respective test applied within the Testing Matrices. Test results not deemed as control deviations are noted by the phrase “No exceptions noted.” in the test result column of the Testing Matrices. Any phrase, other than the aforementioned, constitutes either a test result that is the result of non-occurrence, a change in the application of the control activity, or a deficiency in the operating effectiveness of the control activity. Testing deviations identified within the Testing Matrices are not necessarily weaknesses in the total system of controls, as this determination can only be made after consideration of controls in place at user entities and subservice organizations, if applicable, and other factors. Control considerations that should be implemented by user entities and subservice organizations, in order to complement the control activities and achieve the applicable trust services and HIPAA criteria are presented in the “Subservice Organizations” section within Section 3.

Testing Matrices Begin on the Following Page

SECURITY CATEGORY

Control #	Description of Service Organization's Controls	Service Auditor's Tests of Controls	Test Results
CC1.0: Control Environment			
CC1.1 COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.			
CC1.1.1	An Employee Handbook including a code of conduct is documented to communicate workforce conduct standards and enforcement procedures to employees. The handbook includes disciplinary actions for employee misconduct or violations of the employee handbook standards, which can include termination and suspension.	Inspected the Employee Handbook to determine that an Employee Handbook included a code of conduct and was documented to communicate workforce conduct standards and enforcement procedures to employees including disciplinary actions for employee misconduct or violations of the employee handbook standards, which included termination and suspension.	No exceptions noted.
CC1.1.2	Employees are required to acknowledge the Employee Handbook during onboarding which includes confidentiality and nondisclosure requirements.	Inspected the signed Employee Handbook acknowledgement for a sample of employees hired during the review period to determine that each sampled employee acknowledged the Employee Handbook during onboarding which included confidentiality and nondisclosure requirements.	No exceptions noted.
CC1.1.3	Organizational and information security policies and procedures are documented and made available to personnel through the Profisee's SharePoint site.	Inspected the company SharePoint site to determine that organizational and information security policies and procedures were documented and made available to personnel through the Profisee's SharePoint site.	No exceptions noted.
CC1.1.4	Background checks are required to be completed on employees.	Inspected the completed background check for a sample of employees hired during the review period to determine that a background check was completed for each employee sampled.	No exceptions noted.
CC1.1.5	Management performs performance and conduct evaluations for employees on at least an annual basis to evaluate the skills and competencies of employees.	Inspected the completed performance and conduct evaluation documentation for a sample of current employees with a tenure of greater than one year to determine that management performed a performance and conduct evaluation during the review period to evaluate the skills and competencies for each employee sampled.	No exceptions noted.

Control #	Description of Service Organization's Controls	Service Auditor's Tests of Controls	Test Results
CC1.2 COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.			
CC1.2.1	A Security Governance Policy has been formally documented to define the oversight, structures, authorities, and responsibilities associated with the organization's information security program.	Inspected the Security Governance Policy to determine that the Security Governance Policy was formally documented and defined the oversight, structures, authorities, and responsibilities associated with the organization's information security program.	No exceptions noted.
CC1.2.2	Policies and procedures formally assign responsibility for the development, and performance of internal control to individuals and teams throughout the organization. The ISC is responsible for coordinating the development and implementation of the information security requirements associated with the organization's information security objectives.	Inspected the Security Governance Policy and the Security Objectives Guidelines to determine that policies and procedures formally assigned responsibility for the development, and performance of internal control to individuals and teams throughout the organization and that the ISC was responsible for coordinating the development and implementation of the information security requirements associated with the organization's information security objectives.	No exceptions noted.
CC1.2.3	An annual information security meeting is conducted for the ISC to plan and report on the performance of the information security program to the CEO.	Inspected the most recent annual information security meeting minutes and calendar invite to determine that the information security meeting was conducted within the review period for the ISC to plan and report on the performance of the information security program to the CEO.	No exceptions noted.
CC1.2.4	The Information Security Team conducts a weekly meeting to review the Security Planner tracker, which tracks information security initiatives and status updates.	Inspected the Information Security Team weekly reoccurring meeting invite and the Security Planning tracker to determine that the Information Security Team conducted weekly meetings to review the Security Planner tracker, which tracked information security initiatives and status updates.	No exceptions noted.
CC1.3 COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.			
CC1.3.1	A documented organizational chart is in place within the HR system that defines organizational structures, lines of reporting, and areas of authority.	Inspected the organizational chart within the HR system to determine that a documented organizational chart was in place within the HR system that defined organizational structures, lines of reporting, and areas of authority.	No exceptions noted.

Control #	Description of Service Organization's Controls	Service Auditor's Tests of Controls	Test Results
CC1.3.2	Job descriptions are documented for new employees and include roles and responsibilities.	Inspected the job description for a sample of employees hired during the review period to determine that a job description was documented and included roles and responsibilities for each employee sampled.	No exceptions noted.
CC1.3.3	A Security Governance Policy has been formally documented to define the oversight, structures, authorities, and responsibilities associated with the organization's information security program.	Inspected the Security Governance Policy to determine that the Security Governance Policy was formally documented and defined the oversight, structures, authorities, and responsibilities associated with the organization's information security program.	No exceptions noted.
CC1.3.4	Policies and procedures formally assign responsibility for the development, and performance of internal control to individuals and teams throughout the organization. The ISC is responsible for coordinating the development and implementation of the information security requirements associated with the organization's information security objectives.	Inspected the Security Governance Policy and the Security Objectives Guidelines to determine that policies and procedures formally assigned responsibility for the development, and performance of internal control to individuals and teams throughout the organization and that the ISC was responsible for coordinating the development and implementation of the information security requirements associated with the organization's information security objectives.	No exceptions noted.
CC1.3.5	The Information Security Team conducts a weekly meeting to review the Security Planner tracker, which tracks information security initiatives and status updates.	Inspected the Information Security Team weekly reoccurring meeting invite and the Security Planning tracker to determine that the Information Security Team conducted weekly meetings to review the Security Planner tracker, which tracked information security initiatives and status updates.	No exceptions noted.
CC1.4 COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.			
CC1.4.1	Policies and procedures are in place that outline screening and competency requirements for candidates.	Inspected the Employee Handbook and the Security Governance Policy to determine that policies and procedures were in place that outlined screening and competency requirements for candidates.	No exceptions noted.
CC1.4.2	Security training is provided to employees during the onboarding process.	Inspected the onboarding presentation and meeting invite for a sample of employees hired during the review period to determine that security training was provided during the onboarding process for each employee sampled.	No exceptions noted.

Control #	Description of Service Organization's Controls	Service Auditor's Tests of Controls	Test Results
CC1.4.3	Management utilizes a security training system to conduct a phishing exercise on an annual basis to monitor employees' security awareness.	Inspected the security training system monitoring reports to determine that management utilized a security training system to conduct a phishing exercise during the review period to monitor employee's security awareness.	No exceptions noted.
CC1.4.4	Management performs performance and conduct evaluations for employees on at least an annual basis to evaluate the skills and competencies of employees.	Inspected the completed performance and conduct evaluation documentation for a sample of current employees with a tenure of greater than one year to determine that management performed a performance and conduct evaluation during the review period to evaluate the skills and competencies for each employee sampled.	No exceptions noted.
CC1.4.5	Job descriptions are documented for new employees and include roles and responsibilities.	Inspected the job description for a sample of employees hired during the review period to determine that a job description was documented and included roles and responsibilities for each employee sampled.	No exceptions noted.
CC1.5 COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.			
CC1.5.1	Job descriptions are documented for new employees and include roles and responsibilities.	Inspected the job description for a sample of employees hired during the review period to determine that a job description was documented and included roles and responsibilities for each employee sampled.	No exceptions noted.
CC1.5.2	An Employee Handbook including a code of conduct is documented to communicate workforce conduct standards and enforcement procedures to employees. The handbook includes disciplinary actions for employee misconduct or violations of the employee handbook standards, which can include termination and suspension.	Inspected the Employee Handbook to determine that an Employee Handbook included a code of conduct and was documented to communicate workforce conduct standards and enforcement procedures to employees including disciplinary actions for employee misconduct or violations of the employee handbook standards, which included termination and suspension.	No exceptions noted.
CC1.5.3	Employees are required to acknowledge the Employee Handbook during onboarding which includes confidentiality and nondisclosure requirements.	Inspected the signed Employee Handbook acknowledgement for a sample of employees hired during the review period to determine that each sampled employee acknowledged the Employee Handbook during onboarding which included confidentiality and nondisclosure requirements.	No exceptions noted.

Control #	Description of Service Organization's Controls	Service Auditor's Tests of Controls	Test Results
CC1.5.4	Management performs performance and conduct evaluations for employees on at least an annual basis to evaluate the skills and competencies of employees.	Inspected the completed performance and conduct evaluation documentation for a sample of current employees with a tenure of greater than one year to determine that management performed a performance and conduct evaluation during the review period to evaluate the skills and competencies for each employee sampled.	No exceptions noted.
CC2.0: Communication and Information			
CC2.1 COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.			
CC2.1.1	Organizational and information security policies and procedures are documented and made available to personnel through the Profisee's SharePoint site.	Inspected the company SharePoint site to determine that organizational and information security policies and procedures were documented and made available to personnel through the Profisee's SharePoint site.	No exceptions noted.
CC2.1.2	Management reviews policies, procedures, and other control documents on an annual basis.	Inspected the most recent management review to determine that management reviewed policies, procedures, and other control documents during the review period.	No exceptions noted.
CC2.1.3	Architecture diagrams are documented and maintained by management to identify system components, data flows, and network segmentation.	Inspected the architecture diagram to determine that architecture diagrams were documented and maintained by management that identified system components, data flows, and network segmentation.	No exceptions noted.
CC2.1.4	Production resources are reviewed by SaaS Operations personnel on at least an annual basis for relevance and use.	Inspected the production resource review documentation to determine that production resources were reviewed by SaaS Operations personnel during the review period for relevance and use.	No exceptions noted.
CC2.1.5	Profisee conducts an internal audit of their information security management system and internal controls annually.	Inspected the most recently completed internal audit report and meeting invite to determine that Profisee conducted an internal audit of their information security management system and internal controls during the review period.	No exceptions noted.

Control #	Description of Service Organization's Controls	Service Auditor's Tests of Controls	Test Results
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.			
CC2.2.1	Organizational and information security policies and procedures are documented and made available to personnel through the Profisee's SharePoint site.	Inspected the company SharePoint site to determine that organizational and information security policies and procedures were documented and made available to personnel through the Profisee's SharePoint site.	No exceptions noted.
CC2.2.2	All-hands meetings are held on at least a monthly basis to communicate organizational updates with employees.	Inspected the all-hands meeting invite and/or recordings for a sample of months during the review period to determine that an all-hands meeting was held to communicate organizational updates with employees for each month sampled.	No exceptions noted.
CC2.2.3	Job descriptions are documented for new employees and include roles and responsibilities.	Inspected the job description for a sample of employees hired during the review period to determine that a job description was documented and included roles and responsibilities for each employee sampled.	No exceptions noted.
CC2.2.4	Documented incident response policies and procedures are in place to guide personnel in identifying, reporting, handling, and communicating security incidents.	Inspected the Security Governance Policy and the Incident Response Policy to determine that documented incident response policies and procedures were in place to guide personnel in identifying, reporting, handling, and communicating security incidents.	No exceptions noted.
CC2.2.5	An Employee Handbook including a code of conduct is documented to communicate workforce conduct standards and enforcement procedures to employees. The handbook includes disciplinary actions for employee misconduct or violations of the employee handbook standards, which can include termination and suspension.	Inspected the Employee Handbook to determine that an Employee Handbook included a code of conduct and was documented to communicate workforce conduct standards and enforcement procedures to employees including disciplinary actions for employee misconduct or violations of the employee handbook standards, which included termination and suspension.	No exceptions noted.
CC2.2.6	Security training is provided to employees during the onboarding process.	Inspected the onboarding presentation and meeting invite for a sample of employees hired during the review period to determine that security training was provided during the onboarding process for each employee sampled.	No exceptions noted.

Control #	Description of Service Organization's Controls	Service Auditor's Tests of Controls	Test Results
CC2.2.7	An annual information security meeting is conducted for the ISC to plan and report on the performance of the information security program to the CEO.	Inspected the most recent annual information security meeting minutes and calendar invite to determine that the information security meeting was conducted within the review period for the ISC to plan and report on the performance of the information security program to the CEO.	No exceptions noted.
CC2.3 COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.			
CC2.3.1	Security commitments and customer responsibilities are documented and communicated to customers within the SaaS subscription agreement.	Inspected the SaaS subscription agreement to determine that security commitments and customer responsibilities were documented and communicated to customers within the SaaS subscription agreement.	No exceptions noted.
CC2.3.2	The SaaS subscription agreement is used to communicate documented procedures for external parties to report system issues through a support portal. A defined escalation path and priority-based response times are established to ensure timely resolution.	Inspected the SaaS subscription agreement to determine that documented procedures were communicated to external parties to report system issues through a support portal, including that a defined escalation path and priority-based response times were established to ensure timely resolution.	No exceptions noted.
CC3.0: Risk Assessment			
CC3.1 COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.			
CC3.1.1	The organization maintains a documented Security Objectives Guidelines policy that defines information security objectives to be aligned with business goals, information security risks, and regulatory requirements.	Inspected the Security Objectives Guidelines to determine that the organization maintained a documented policy that defined information security objectives to be aligned with business goals, information security risks, and regulatory requirements.	No exceptions noted.
CC3.1.2	Management performs an annual risk assessment to identify risks that could impact the achievement of the company's information security objectives. Identified risks are assessed using a risk rating methodology.	Inspected the risk assessment matrix to determine that management performed a formal risk assessment during the review period that identified risks to the company's security objectives and that identified risks were assessed using a risk documented risk rating methodology.	No exceptions noted.

Control #	Description of Service Organization's Controls	Service Auditor's Tests of Controls	Test Results
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.			
CC3.2.1	Management has defined a formal risk assessment policy that specified the process for identifying internal and external threats and vulnerabilities, evaluating and addressing risks, and defining specified risk tolerances.	Inspected the Risk Management Policy to determine that management defined a formal risk assessment policy that specified the process for identifying internal and external threats and vulnerabilities, evaluating and addressing risks and defined specified risk tolerances.	No exceptions noted.
CC3.2.2	Management performs an annual risk assessment to identify risks that could impact the achievement of the company's information security objectives. Identified risks are assessed using a risk rating methodology.	Inspected the risk assessment matrix to determine that management performed a formal risk assessment during the review period that identified risks to the company's security objectives and that identified risks were assessed using a risk documented risk rating methodology.	No exceptions noted.
CC3.2.3	Management selects and documents risk treatment plans to address risks identified during the annual risk assessment process. Treatment plans include the implementation of mitigating controls to reduce residual risk to acceptable levels and are assigned to process owners.	Inspected the risk assessment matrix to determine that management selected and documented risk treatment plans for risks identified during the risk assessment process performed during the review period and that those plans included mitigating controls to reduce residual risk to acceptable levels and were assigned to process owners.	No exceptions noted.
CC3.3 COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.			
CC3.3.1	A formal risk assessment is performed on an annual basis that identifies and assesses the types of fraud that could impact the achievement of objectives.	Inspected the risk assessment matrix to determine that a formal risk assessment was performed during the review period that identified and assessed the types of fraud that could impact the achievement of objectives.	No exceptions noted.
CC3.3.2	Management considers fraud risks related to incentives, opportunities, employee conduct, and technology-related threats that could enable or justify fraudulent activity as part of the annual risk assessment.	Inspected the risk assessment matrix to determine that management considered fraud risks related to incentives, opportunities, employee conduct, and technology-related threats that could enable or justify fraudulent activity as part of the risk assessment performed during the review period.	No exceptions noted.

Control #	Description of Service Organization's Controls	Service Auditor's Tests of Controls	Test Results
CC3.4 COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.			
CC3.4.1	Management has defined a formal risk assessment policy that specified the process for identifying internal and external threats and vulnerabilities, evaluating and addressing risks, and defining specified risk tolerances.	Inspected the Risk Management Policy to determine that management defined a formal risk assessment policy that specified the process for identifying internal and external threats and vulnerabilities, evaluating and addressing risks and defined specified risk tolerances.	No exceptions noted.
CC3.4.2	A formal risk assessment is performed on an annual basis to identify internal and external threats and vulnerabilities that could impair system commitments and requirements.	Inspected the risk assessment matrix to determine that a formal risk assessment was performed during the review period that identified internal and external threats and vulnerabilities that could impair system commitments and requirements.	No exceptions noted.
CC3.4.3	Changes in vendor and third-party relationships are considered and evaluated as part of the annual risk assessment.	Inspected the risk assessment matrix to determine that management considered and evaluated changes in vendor and third-party relationships as part of the risk assessment performed during the review period.	No exceptions noted.
CC4.0: Monitoring Activities			
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.			
CC4.1.1	Profisee conducts an internal audit of their information security management system and internal controls annually.	Inspected the internal audit report and meeting invite to determine that Profisee conducted an internal audit of their information security management system and internal controls during the review period.	No exceptions noted.
CC4.1.2	An annual information security meeting is conducted for the ISC to plan and report on the performance of the information security program to the CEO.	Inspected the most recent annual information security meeting minutes and calendar invite to determine that the information security meeting was conducted within the review period for the ISC to plan and report on the performance of the information security program to the CEO.	No exceptions noted.
CC4.1.3	The Information Security Team conducts a weekly meeting to review the Security Planner tracker, which tracks information security initiatives and status updates.	Inspected the Information Security Team weekly reoccurring meeting invite and the Security Planning tracker to determine that the Information Security Team conducted weekly meetings to review the Security Planner tracker, which tracked information security initiatives and status updates.	No exceptions noted.

Control #	Description of Service Organization's Controls	Service Auditor's Tests of Controls	Test Results
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.			
CC4.2.1	An annual information security meeting is conducted for the ISC to plan and report on the performance of the information security program to the CEO.	Inspected the most recent annual information security meeting minutes and calendar invite to determine that the information security meeting was conducted within the review period for the ISC to plan and report on the performance of the information security program to the CEO.	No exceptions noted.
CC4.2.2	The Information Security Team conducts a weekly meeting to review the Security Planner tracker, which tracks information security initiatives and status updates.	Inspected the Information Security Team weekly reoccurring meeting invite and the Security Planning tracker to determine that the Information Security Team conducted weekly meetings to review the Security Planner tracker, which tracked information security initiatives and status updates.	No exceptions noted.
CC4.2.3	Profisee conducts an internal audit of their information security management system and internal controls annually.	Inspected the internal audit report and meeting invite to determine that Profisee conducted an internal audit of their information security management system and internal controls during the review period.	No exceptions noted.
CC4.2.4	Documented incident response policies and procedures are in place to guide personnel in identifying, reporting, handling, and communicating security incidents.	Inspected the Security Governance Policy and the Incident Response Policy to determine that documented incident response policies and procedures were in place to guide personnel in identifying, reporting, handling, and communicating security incidents.	No exceptions noted.
CC5.0: Control Activities			
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.			
CC5.1.1	Management selects and documents risk treatment plans to address risks identified during the annual risk assessment process. Treatment plans include the implementation of mitigating controls to reduce residual risk to acceptable levels and are assigned to process owners.	Inspected the risk assessment matrix to determine that management selected and documented risk treatment plans for risks identified during the risk assessment process performed during the review period and that those plans included mitigating controls to reduce residual risk to acceptable levels and were assigned to process owners.	No exceptions noted.

Control #	Description of Service Organization's Controls	Service Auditor's Tests of Controls	Test Results
CC5.1.2	Profisee conducts an internal audit of their information security management system and internal controls annually.	Inspected the internal audit report and meeting invite to determine that Profisee conducted an internal audit of their information security management system and internal controls during the review period.	No exceptions noted.
CC5.2 COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.			
CC5.2.1	The use of technology in the selection and development of controls is evaluated by management as part of the annual risk assessment.	Inspected the risk assessment matrix to determine that management evaluated the use of technology in the selection and development of controls as part of the risk assessment performed during the review period.	No exceptions noted.
CC5.2.2	An annual information security meeting is conducted for the ISC to plan and report on the performance of the information security program to the CEO.	Inspected the most recent annual information security meeting minutes and calendar invite to determine that the information security meeting was conducted within the review period for the ISC to plan and report on the performance of the information security program to the CEO.	No exceptions noted.
CC5.2.3	The Information Security Team conducts a weekly meeting to review the Security Planner tracker, which tracks information security initiatives and status updates.	Inspected the Information Security Team weekly reoccurring meeting invite and the Security Planning tracker to determine that the Information Security Team conducted weekly meetings to review the Security Planner tracker, which tracked information security initiatives and status updates.	No exceptions noted.
CC5.2.4	Profisee conducts an internal audit of their information security management system and internal controls annually.	Inspected the internal audit report and meeting invite to determine that Profisee conducted an internal audit of their information security management system and internal controls during the review period.	No exceptions noted.
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.			
CC5.3.1	A Security Governance Policy has been formally documented to define the oversight, structures, authorities, and responsibilities associated with the organization's information security program.	Inspected the Security Governance Policy to determine that the Security Governance Policy was formally documented and defined the oversight, structures, authorities, and responsibilities associated with the organization's information security program.	No exceptions noted.

Control #	Description of Service Organization's Controls	Service Auditor's Tests of Controls	Test Results
CC5.3.2	Policies and procedures formally assign responsibility for the development, and performance of internal control to individuals and teams throughout the organization. The ISC is responsible for coordinating the development and implementation of the information security requirements associated with the organization's information security objectives.	Inspected the Security Governance Policy and the Security Objectives Guidelines to determine that policies and procedures formally assigned responsibility for the development, and performance of internal control to individuals and teams throughout the organization and that the ISC was responsible for coordinating the development and implementation of the information security requirements associated with the organization's information security objectives.	No exceptions noted.
CC5.3.3	Organizational and information security policies and procedures are documented and made available to personnel through the Profisee's SharePoint site.	Inspected the company SharePoint site to determine that organizational and information security policies and procedures were documented and made available to personnel through the Profisee's SharePoint site.	No exceptions noted.
CC5.3.4	Management reviews policies, procedures, and other control documents on an annual basis.	Inspected the most recent management review to determine that management reviewed policies, procedures, and other control documents during the review period.	No exceptions noted.
CC6.0: Logical and Physical Access Controls			
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.			
CC6.1.1	An inventory of system assets and components is maintained to classify and manage the information assets.	Inspected the system inventory listing to determine that an inventory of system assets and components was maintained to classify and manage the information assets.	No exceptions noted.
CC6.1.2	The company network domains are configured to authenticate users via a unique user account and minimum password requirements including MFA.	Inspected the company network domains password configurations and user account listings to determine that company network domains were configured to authenticate users via a unique user account and minimum password requirements including MFA.	No exceptions noted.
CC6.1.3	The company network domains are configured to enforce an account lockout threshold and duration.	Inspected the company network domain lockout configurations to determine that the company network domains were configured to enforce an account lockout threshold and duration.	No exceptions noted.

Control #	Description of Service Organization's Controls	Service Auditor's Tests of Controls	Test Results
CC6.1.4	Production servers are configured to enforce SSO authentication and inherits the unique user account and minimum password requirements (including MFA) enforced via the company's corporate network domain.	Inspected the production server SSO authentication configurations to determine that production servers were configured to enforce SSO authentication and inherited the unique user account and minimum password requirements (including MFA) enforced via the company's corporate network domain.	No exceptions noted.
CC6.1.5	Production databases are configured to enforce SSO authentication and inherits the unique user account and minimum password requirements (including MFA) enforced via the company's production network domain.	Inspected the production database SSO authentication configurations to determine that production databases were configured to enforce SSO authentication and inherited the unique user account and minimum password requirements (including MFA) enforced via the company's production network domain.	No exceptions noted.
CC6.1.6	VPN users are authenticated via MFA prior to being granted remote access to the system.	Inspected the VPN authentication configurations to determine that VPN users were authenticated via MFA prior to being granted remote access to the system.	No exceptions noted.
CC6.1.7	Administrative access privileges to company network domains are restricted to user accounts accessible by authorized IT personnel.	Inspected the company network domains administrator listings with the assistance of the senior security engineer to determine that administrative access privileges to company network domains were restricted to user accounts accessible by authorized IT personnel.	No exceptions noted.
CC6.1.8	Administrative access privileges to production servers and databases are restricted to user accounts accessible by authorized IT personnel.	Inspected the production server and database administrator listings with the assistance of the senior security engineer to determine that administrative access privileges to production servers and databases were restricted to user accounts accessible by authorized IT personnel.	No exceptions noted.
CC6.1.9	The ability to administer VPN access is restricted to authorized IT personnel.	Inspected the listing of users with the ability to administer the VPN with the assistance of the senior security engineer to determine that the ability to administer VPN access was restricted to authorized IT personnel.	No exceptions noted.

Control #	Description of Service Organization's Controls	Service Auditor's Tests of Controls	Test Results
CC6.1.10	Predefined user access groups are utilized to assign role-based access privileges and segregate access to in-scope systems.	Inspected the user access listings to the company network domains, production servers and databases, and VPN to determine that predefined user access groups were utilized to assign role-based access privileges and segregate access to in-scope systems.	No exceptions noted.
CC6.1.11	Production data is encrypted at rest.	Inspected the data encryption configurations to determine that production data was encrypted at rest.	No exceptions noted.
CC6.1.12	The organization utilizes Azure Key Vault to securely store encryption keys.	Inspected the Azure Key Vault settings to determine that the organization utilized Azure Key Vault to securely store encryption keys.	No exceptions noted.
CC6.1.13	Workstations are configured to terminate inactive sessions after five minutes of inactivity.	Inspected the display lock configuration to determine that workstations were configured to terminate inactive sessions after five minutes of inactivity.	No exceptions noted.
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.			
CC6.2.1	Logical access to systems is approved and initiated by authorized HR personnel through an onboarding ticketing process and provisioned by IT personnel.	Inspected the onboarding request tickets for a sample of employees hired during the review period to determine logical access to systems was approved and initiated by authorized HR personnel and that access was provisioned by IT personnel through a documented ticketing process for each employee sampled.	No exceptions noted.
CC6.2.2	Personnel access requests to production databases containing customer data require a documented business case and support portal ticket.	Inspected the documented business case and support portal ticket for a sample of personnel access requests to production databases during the review period to determine that each access request sampled to production databases containing customer data required a documented business case and support portal ticket.	No exceptions noted.
CC6.2.3	Logical access to systems is revoked from personnel as a component of the termination process.	Inspected the user access listings and offboarding emails for a sample of employees terminated during the review period to determine that logical access to systems was revoked for each employee sampled as a component of the termination process.	No exceptions noted.

Control #	Description of Service Organization's Controls	Service Auditor's Tests of Controls	Test Results
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.			
CC6.3.1	Logical access to systems is approved and initiated by authorized HR personnel through an onboarding ticketing process and provisioned by IT personnel.	Inspected the onboarding request tickets for a sample of employees hired during the review period to determine logical access to systems was approved and initiated by authorized HR personnel and that access was provisioned by IT personnel through a documented ticketing process for each employee sampled.	No exceptions noted.
CC6.3.2	Personnel access requests to production databases containing customer data require a documented business case and support portal ticket.	Inspected the documented business case and support portal ticket for a sample of personnel access requests to production databases during the review period to determine that each access request sampled to production databases containing customer data required a documented business case and support portal ticket.	No exceptions noted.
CC6.3.3	Logical access to systems is revoked from personnel as a component of the termination process.	Inspected the user access listings and offboarding emails for a sample of employees terminated during the review period to determine that logical access to systems was revoked for each employee sampled as a component of the termination process.	No exceptions noted.
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.			
	Microsoft Azure is responsible for restricting physical access to data centers housing hardware and physical infrastructure in which production data resides.		
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.			
	Microsoft Azure is responsible for diminishing the ability to read and recover data and software from physical assets prior to discontinuing logical and physical protections over those assets.		
CC6.6 The entity implements logical access security measures to protect against threats from sources outside its system boundaries.			
CC6.6.1	An IDPS is utilized to monitor network events for possible or actual network security breaches and is configured to notify personnel upon intrusion detection.	Inspected the IDPS alerting dashboard and configurations, and example alert generated during the review period to determine that an IDPS was utilized to monitor network events for possible or actual network security breaches and was configured to notify personnel upon intrusion detection.	No exceptions noted.

Control #	Description of Service Organization's Controls	Service Auditor's Tests of Controls	Test Results
CC6.6.2	A firewall system is in place to filter unauthorized inbound network traffic from the Internet.	Inspected the firewall system ruleset configurations to determine that a firewall system was in place to filter unauthorized inbound network traffic from the Internet.	No exceptions noted.
CC6.6.3	Encrypted VPN sessions are utilized for remote connectivity users.	Inspected the VPN encryption settings to determine that encrypted VPN sessions were utilized for remote connectivity users.	No exceptions noted.
CC6.6.4	Production web sessions are encrypted to protect the transmission of information over the Internet.	Inspected the TLS encryption configurations to determine that production web sessions were encrypted to protect the transmission of information over the Internet.	No exceptions noted.
CC6.6.5	Employee workstations are restricted from writing to removable storage devices.	Inspected the MDM endpoint configuration to determine that employee workstations were restricted from writing to removable storage devices.	No exceptions noted.
CC6.6.6	Employee workstations are configured to require system patches and updates to be installed during predefined schedules.	Inspected the MDM device update configuration to determine that employee workstations were configured to require system patches and updates to be installed during predefined schedules.	No exceptions noted.
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.			
CC6.7.1	Personnel laptops are provisioned with disk encryption.	Inspected the disk encryption settings for a sample of current employees to determine that personnel laptops were provisioned with disk encryption for each employee sampled.	No exceptions noted.
CC6.7.2	The ability to recall data backups is restricted to authorized SaaS Operations personnel.	Inspected the listing of users with the ability to recall data backups to determine that the ability to recall data backups was restricted to authorized SaaS Operations personnel.	No exceptions noted.
CC6.7.3	Encrypted VPN sessions are utilized for remote connectivity users.	Inspected the VPN encryption settings to determine that encrypted VPN sessions were utilized for remote connectivity users.	No exceptions noted.
CC6.7.4	Production web sessions are encrypted to protect the transmission of information over the Internet.	Inspected the TLS encryption configurations to determine that production web sessions were encrypted to protect the transmission of information over the Internet.	No exceptions noted.

Control #	Description of Service Organization's Controls	Service Auditor's Tests of Controls	Test Results
CC6.7.5	Employee workstations are restricted from writing to removable storage devices.	Inspected the endpoint device restriction configuration to determine that employee workstations were restricted from writing to removable storage devices.	No exceptions noted.
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.			
CC6.8.1	Centrally managed antivirus software is installed on employee workstations and production servers and databases to scan and prevent malware.	Inspected the antivirus software listing of registered devices to determine that centrally managed antivirus software was installed on employee workstations to scan and prevent malware.	No exceptions noted.
		Inspected the antivirus software listing of registered devices to determine that centrally managed antivirus software was installed on production servers and databases to scan and prevent malware.	No exceptions noted.
CC6.8.2	An IDPS is utilized to monitor network events for possible or actual network security breaches and is configured to notify personnel upon intrusion detection.	Inspected the IDPS alerting dashboard and configurations, and example alert generated during the review period to determine that an IDPS was utilized to monitor network events for possible or actual network security breaches and was configured to notify personnel upon intrusion detection.	No exceptions noted.
CC7.0: System Operations			
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.			
CC7.1.1	Management has defined configuration standards in the information security policies and procedures.	Inspected the Security Governance Policy to determine that management defined configuration standards in the information security policies and procedures.	No exceptions noted.
CC7.1.2	Policies and procedures are in place regarding the detection, logging, and monitoring of unknown or unauthorized components into the environment.	Inspected the Security Governance Policy to determine that documented policies and procedures were in place regarding the detection, logging, and monitoring of unknown or unauthorized components in the environment.	No exceptions noted.
CC7.1.3	Continuous vulnerability scanning is configured for production machines to identify vulnerabilities.	Inspected Defender for Cloud vulnerability settings to determine that continuous vulnerability scanning was configured for production machines to identify vulnerabilities.	No exceptions noted.

Control #	Description of Service Organization's Controls	Service Auditor's Tests of Controls	Test Results
CC7.1.4	A third party performs a penetration test at least annually to identify and exploit vulnerabilities for the web application.	Inspected the web application penetration test report to determine that a third party performed a penetration test during the review period to identify and exploit vulnerabilities for the web application.	No exceptions noted.
CC7.1.5	A third party performs a penetration test at least annually to identify and exploit vulnerabilities for the internal network.	Inspected the internal network penetration test report to determine that a third party performed a penetration test during the review period to identify and exploit vulnerabilities for the internal network.	No exceptions noted.
CC7.1.5	An IDPS is utilized to monitor network events for possible or actual network security breaches and is configured to notify personnel upon intrusion detection.	Inspected the IDPS alerting dashboard and configurations, and example alert generated during the review period to determine that an IDPS was utilized to monitor network events for possible or actual network security breaches and was configured to notify personnel upon intrusion detection.	No exceptions noted.
CC7.1.6	A firewall system is in place to filter unauthorized inbound network traffic from the Internet.	Inspected the firewall system ruleset configurations to determine that a firewall system was in place to filter unauthorized inbound network traffic from the Internet.	No exceptions noted.
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.			
CC7.2.1	Documented incident response policies and procedures are in place to guide personnel in identifying, reporting, handling, and communicating security incidents.	Inspected the Security Governance Policy and the Incident Response Policy to determine that documented incident response policies and procedures were in place to guide personnel in identifying, reporting, handling, and communicating security incidents.	No exceptions noted.
CC7.2.2	Continuous vulnerability scanning is configured for production machines to identify vulnerabilities.	Inspected Defender for Cloud vulnerability settings to determine that continuous vulnerability scanning was configured for production machines to identify vulnerabilities.	No exceptions noted.
CC7.2.3	A third party performs a penetration test at least annually to identify and exploit vulnerabilities for the web application.	Inspected the web application penetration test report to determine that a third party performed a penetration test during the review period to identify and exploit vulnerabilities for the web application.	No exceptions noted.

Control #	Description of Service Organization's Controls	Service Auditor's Tests of Controls	Test Results
CC7.2.3	A third party performs a penetration test at least annually to identify and exploit vulnerabilities for the internal network.	Inspected the internal network penetration test report to determine that a third party performed a penetration test during the review period to identify and exploit vulnerabilities for the internal network.	No exceptions noted.
CC7.2.3	An IDPS is utilized to monitor network events for possible or actual network security breaches and is configured to notify personnel upon intrusion detection.	Inspected the IDPS alerting dashboard and configurations, and example alert generated during the review period to determine that an IDPS was utilized to monitor network events for possible or actual network security breaches and was configured to notify personnel upon intrusion detection.	No exceptions noted.
CC7.3 The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.			
CC7.3.1	Documented incident response policies and procedures define roles, responsibilities, and required activities for analyzing, responding to, and recovering from security incidents.	Inspected the Incident Response Policy to determine that documented incident response policies and procedures defined roles, responsibilities, and required activities for analyzing, responding to, and recovering from security incidents.	No exceptions noted.
CC7.3.2	Incidents are documented and tracked in a standardized ticketing system and updated to reflect the planned incident and problem resolution.	Nonoccurrence: Inspected the ticketing system used to track security incidents and determined that no security incidents were identified during the review period; therefore, no testing of operating effectiveness was performed.	
CC7.3.3	A security incident analysis is performed for security incidents to determine the root cause and system impact.	Nonoccurrence: Refer to the test results for control activity CC7.3.2.	
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.			
CC7.4.1	Documented incident response policies and procedures define roles, responsibilities, and required activities for analyzing, responding to, and recovering from security incidents.	Inspected the Incident Response Policy to determine that documented incident response policies and procedures defined roles, responsibilities, and required activities for analyzing, responding to, and recovering from security incidents.	No exceptions noted.
CC7.4.2	Incidents are documented and tracked in a standardized ticketing system and updated to reflect the planned incident and problem resolution.	Nonoccurrence: Refer to the test results for control activity CC7.3.2.	
CC7.4.3	A security incident analysis is performed for security incidents to determine the root cause and system impact.	Nonoccurrence: Refer to the test results for control activity CC7.3.2.	

Control #	Description of Service Organization's Controls	Service Auditor's Tests of Controls	Test Results
CC7.4.4	Security incidents resulting in the unauthorized use or disclosure of personal information are communicated to the affected users.	Nonoccurrence: Refer to the test results for control activity CC7.3.2.	
CC7.5 The entity identifies, develops, and implements activities to recover from identified security incidents.			
CC7.5.1	Documented incident response policies and procedures define roles, responsibilities, and required activities for analyzing, responding to, and recovering from security incidents.	Inspected the Incident Response Policy to determine that documented incident response policies and procedures defined roles, responsibilities, and required activities for analyzing, responding to, and recovering from security incidents.	No exceptions noted.
CC7.5.2	Management reviews the company's incident response and escalation procedures annually for effectiveness.	Inspected the most recent annual information security meeting minutes, calendar invite, and meeting transcript to determine that management reviewed the company's incident response and escalation procedures during the review period for effectiveness	No exceptions noted.
CC7.5.3	Incidents are documented and tracked in a standardized ticketing system and updated to reflect the planned incident and problem resolution.	Nonoccurrence: Refer to the test results for control activity CC7.3.2.	
CC7.5.4	A security incident analysis is performed for security incidents to determine the root cause and system impact.	Nonoccurrence: Refer to the test results for control activity CC7.3.2.	
CC7.5.5	A disaster recovery and business continuity plan is documented to identify and reduce risks, limit the consequences of damaging incidents, and ensure the timely resumption of essential operations.	Inspected the Disaster Recovery and Business Continuity Plan to determine that it was documented to identify and reduce risks, limit the consequences of damaging incidents, and ensure the timely resumption of essential operations.	No exceptions noted.
CC8.0: Change Management			
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.			
CC8.1.1	Documented change control policies and procedures are in place to guide personnel in the change management process.	Inspected the Change Management Procedure to determine that documented change control policies and procedures were in place to guide personnel in the change management process.	No exceptions noted.
CC8.1.2	System change requests are documented and tracked in a ticketing system.	Inspected change request tickets for a sample of changes completed during the review period to determine each change sampled was documented and tracked in the ticketing system.	No exceptions noted.

Control #	Description of Service Organization's Controls	Service Auditor's Tests of Controls	Test Results
CC8.1.3	Application changes are tested prior to implementation.	Inspected change request tickets for a sample of changes completed during the review period to determine that each application change sampled was tested prior to implementation.	No exceptions noted.
CC8.1.4	System changes are authorized and approved by management prior to implementation.	Inspected change request tickets for a sample of changes completed during the review period to determine each change sampled was authorized and approved by management prior to implementation.	No exceptions noted.
CC8.1.5	The ability to migrate changes into the production environment is restricted to authorized users.	Inspected the listing of users with the ability to migrate changes to determine that the ability to migrate changes into the production environment was restricted to authorized users.	No exceptions noted.
CC8.1.6	Back out procedures for production application changes are documented to allow for rollback of changes when changes impair system operation.	Inspected change request tickets for a sample of changes completed during the review period to determine that back out procedures for each application change sampled was documented to allow for rollback of changes when changes impair system operation.	No exceptions noted.
CC8.1.7	The CI/CD system is configured to require at least one peer reviewer prior to pushing a pull request to the production branch.	Inspected the CI/CD branch protection policy configuration to determine that the CI/CD system was configured to require at least one peer reviewer prior to pushing a pull request to the production branch.	No exceptions noted.
CC8.1.8	The CI/CD system provides version control and rollback capability for source code repositories.	Inspected the CI/CD commit history to determine that the CI/CD system provided version control and rollback capability for source code repositories.	No exceptions noted.
CC8.1.9	Administrative access privileges to CI/CD system are restricted to user accounts accessible by authorized IT personnel.	Inspected the CI/CD administrator listings with the assistance of the senior security engineer to determine that administrative access privileges to the CI/CD system was restricted to user accounts accessible by authorized IT personnel.	No exceptions noted.
CC8.1.10	Development and test environments are logically separated from the production environment.	Inspected the Azure region subscriptions to determine that development and test environments were logically separated from the production environment.	No exceptions noted.

Control #	Description of Service Organization's Controls	Service Auditor's Tests of Controls	Test Results
CC9.0: Risk Mitigation			
CC9.1 The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.			
CC9.1.1	A disaster recovery and business continuity plan is documented to identify and reduce risks, limit the consequences of damaging incidents, and ensure the timely resumption of essential operations.	Inspected the Disaster Recovery and Business Continuity Plan to determine that it was documented to identify and reduce risks, limit the consequences of damaging incidents, and ensure the timely resumption of essential operations.	No exceptions noted.
CC9.1.2	The disaster recovery and business continuity plan is updated and approved on an annual basis.	Inspected the Disaster Recovery and Business Continuity Plan to determine that it was updated and reviewed during the review period.	No exceptions noted.
CC9.1.3	A disaster recovery failover test that includes data backup restoration is performed on an annual basis.	Inspected the most recently completed disaster recovery test to determine that a disaster recovery failover test that included a data backup restoration was performed during the review period.	No exceptions noted.
CC9.1.4.	Full and incremental backups of the SQL databases are performed based on predefined schedules.	Inspected the backup system schedule configuration to determine that full and incremental backups of the SQL databases were performed based on predefined schedules.	No exceptions noted.
CC9.1.5	The entity maintains cybersecurity insurance coverage to offset the financial loss that could result from a critical security incident or exploitation of a vulnerability.	Inspected the active cybersecurity policy coverage to determine that the entity maintained cybersecurity insurance coverage to offset the financial loss that could result from a critical security incident or exploitation of a vulnerability.	No exceptions noted.
CC9.2 The entity assesses and manages risks associated with vendors and business partners.			
CC9.2.1	The entity has documented policies in place for managing third parties.	Inspected the Security Governance Policy to determine that the entity had documented policies in place for managing third parties.	No exceptions noted.
CC9.2.2	Management obtains and reviews compliance reports for vendors on an annual basis to evaluate the effectiveness of controls within the vendors environments.	Inspected the vendor management review documentation for a sample of current vendors to determine that management obtained and reviewed compliance reports during the review period to evaluate the effectiveness of controls within the vendors environments for each vendor sampled.	The test of the control activity disclosed that management did not obtain and review compliance reports during the review period for one of three vendors sampled.

Control #	Description of Service Organization's Controls	Service Auditor's Tests of Controls	Test Results
CC9.2.3	Changes in vendor and third-party relationships are considered and evaluated as part of the annual risk assessment.	Inspected the risk assessment matrix to determine that management considered and evaluated changes in vendor and third-party relationships as part of the risk assessment performed during the review period.	No exceptions noted.

HIPAA Security Rule

#	Description of Service Organization's Controls	Service Auditor's Tests of Controls	Test Results
§164.306(a): **General Requirements**. Covered entities and business associates must do the following:(1) Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits. (2) Protect against any reasonably anticipated threats or hazards to the security or integrity of such information. (3) Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under subpart E of this part; and (4) Ensure compliance with this subpart by its workforce.			
1.01	Policies and procedures formally assign responsibility for the development, and performance of internal control to individuals and teams throughout the organization. The ISC is responsible for coordinating the development and implementation of the information security requirements associated with the organization's information security objectives.	Inspected the Security Governance Policy and the Security Objectives Guidelines to determine that policies and procedures formally assigned responsibility for the development, and performance of internal control to individuals and teams throughout the organization and that the ISC was responsible for coordinating the development and implementation of the information security requirements associated with the organization's information security objectives.	No exceptions noted.
1.02	Management performs an annual risk assessment to identify risks that could impact the achievement of the company's information security objectives. Identified risks are assessed using a risk rating methodology.	Inspected the risk assessment matrix to determine that management performed a formal risk assessment during the review period that identified risks to the company's security objectives and that identified risks were assessed using a risk documented risk rating methodology.	No exceptions noted.
1.03	A formal risk assessment is performed on an annual basis to identify internal and external threats and vulnerabilities that could impair system commitments and requirements.	Inspected the risk assessment matrix to determine that a formal risk assessment was performed during the review period that identified internal and external threats and vulnerabilities that could impair system commitments and requirements.	No exceptions noted.

#	Description of Service Organization's Controls	Service Auditor's Tests of Controls	Test Results
1.04	Management selects and documents risk treatment plans to address risks identified during the annual risk assessment process. Treatment plans include the implementation of mitigating controls to reduce residual risk to acceptable levels and are assigned to process owners.	Inspected the risk assessment matrix to determine that management selected and documented risk treatment plans for risks identified during the risk assessment process performed during the review period and that those plans included mitigating controls to reduce residual risk to acceptable levels and were assigned to process owners.	No exceptions noted.
1.05	Continuous vulnerability scanning is configured for production machines to identify vulnerabilities.	Inspected Defender for Cloud vulnerability settings to determine that continuous vulnerability scanning was configured for production machines to identify vulnerabilities.	No exceptions noted.
1.06	A third party performs a penetration test at least annually to identify and exploit vulnerabilities for the web application.	Inspected the web application penetration test report to determine that a third party performed a penetration test during the review period to identify and exploit vulnerabilities for the web application.	No exceptions noted.
1.07	A third party performs a penetration test at least annually to identify and exploit vulnerabilities for the internal network.	Inspected the internal network penetration test report to determine that a third party performed a penetration test during the review period to identify and exploit vulnerabilities for the internal network.	No exceptions noted.
1.08	The use of technology in the selection and development of controls is evaluated by management as part of the annual risk assessment.	Inspected the risk assessment matrix to determine that management evaluated the use of technology in the selection and development of controls as part of the risk assessment performed during the review period.	No exceptions noted.
1.09	Documented incident response policies and procedures are in place to guide personnel in identifying, reporting, handling, and communicating security incidents.	Inspected the Security Governance Policy and the Incident Response Policy to determine that documented incident response policies and procedures were in place to guide personnel in identifying, reporting, handling, and communicating security incidents.	No exceptions noted.
1.10	Management reviews the company's incident response and escalation procedures annually for effectiveness.	Inspected the most recent annual information security meeting minutes, calendar invite, and meeting transcript to determine that management reviewed the company's incident response and escalation procedures during the review period for effectiveness	No exceptions noted.

#	Description of Service Organization's Controls	Service Auditor's Tests of Controls	Test Results
1.11	An Employee Handbook including a code of conduct is documented to communicate workforce conduct standards and enforcement procedures to employees. The handbook includes disciplinary actions for employee misconduct or violations of the employee handbook standards, which can include termination and suspension.	Inspected the Employee Handbook to determine that an Employee Handbook included a code of conduct and was documented to communicate workforce conduct standards and enforcement procedures to employees including disciplinary actions for employee misconduct or violations of the employee handbook standards, which included termination and suspension.	No exceptions noted.
1.12	Employees are required to acknowledge the Employee Handbook during onboarding which includes confidentiality and nondisclosure requirements.	Inspected the signed Employee Handbook acknowledgement for a sample of employees hired during the review period to determine that each sampled employee acknowledged the Employee Handbook during onboarding which included confidentiality and nondisclosure requirements.	No exceptions noted.
1.13	Security training is provided to employees during the onboarding process.	Inspected the onboarding presentation and meeting invite for a sample of employees hired during the review period to determine that security training was provided during the onboarding process for each employee sampled.	No exceptions noted.
1.14	Management utilizes a security training system to conduct a phishing exercise on an annual basis to monitor employees' security awareness.	Inspected the security training system monitoring reports to determine that management utilized a security training system to conduct a phishing exercise during the review period to monitor employee's security awareness.	No exceptions noted.
§164.306(b): **Flexibility of Approach**. (1) Covered entities and business associates may use any security measures that allow the covered entity or business associate to reasonably and appropriately implement the standards and implementation specifications as specified in this subpart. (2) In deciding which security measures to use, a covered entity or business associate must take into account the following factors: (i) The size, complexity, and capabilities of the covered entity or business associate. (ii) The covered entity's or the business associate's technical infrastructure, hardware, and software security capabilities. (iii) The costs of security measures. (iv) The probability and criticality of potential risks to electronic protected health information.			
1.15	A Security Governance Policy has been formally documented to define the oversight, structures, authorities, and responsibilities associated with the organization's information security program.	Inspected the Security Governance Policy to determine that the Security Governance Policy was formally documented and defined the oversight, structures, authorities, and responsibilities associated with the organization's information security program.	No exceptions noted.

#	Description of Service Organization's Controls	Service Auditor's Tests of Controls	Test Results
1.16	Policies and procedures formally assign responsibility for the development, and performance of internal control to individuals and teams throughout the organization. The ISC is responsible for coordinating the development and implementation of the information security requirements associated with the organization's information security objectives.	Inspected the Security Governance Policy and the Security Objectives Guidelines to determine that policies and procedures formally assigned responsibility for the development, and performance of internal control to individuals and teams throughout the organization and that the ISC was responsible for coordinating the development and implementation of the information security requirements associated with the organization's information security objectives.	No exceptions noted.
1.17	An annual information security meeting is conducted for the ISC to plan and report on the performance of the information security program to the CEO.	Inspected the most recent annual information security meeting minutes and calendar invite to determine that the information security meeting was conducted within the review period for the ISC to plan and report on the performance of the information security program to the CEO.	No exceptions noted.
1.18	The Information Security Team conducts a weekly meeting to review the Security Planner tracker, which tracks information security initiatives and status updates.	Inspected the Information Security Team weekly reoccurring meeting invite and the Security Planning tracker to determine that the Information Security Team conducted weekly meetings to review the Security Planner tracker, which tracked information security initiatives and status updates.	No exceptions noted.
1.19	Management performs an annual risk assessment to identify risks that could impact the achievement of the company's information security objectives. Identified risks are assessed using a risk rating methodology.	Inspected the risk assessment matrix to determine that management performed a formal risk assessment during the review period that identified risks to the company's security objectives and that identified risks were assessed using a risk documented risk rating methodology.	No exceptions noted.
1.20	Management selects and documents risk treatment plans to address risks identified during the annual risk assessment process. Treatment plans include the implementation of mitigating controls to reduce residual risk to acceptable levels and are assigned to process owners.	Inspected the risk assessment matrix to determine that management selected and documented risk treatment plans for risks identified during the risk assessment process performed during the review period and that those plans included mitigating controls to reduce residual risk to acceptable levels and were assigned to process owners.	No exceptions noted.

#	Description of Service Organization's Controls	Service Auditor's Tests of Controls	Test Results
1.21	The use of technology in the selection and development of controls is evaluated by management as part of the annual risk assessment.	Inspected the risk assessment matrix to determine that management evaluated the use of technology in the selection and development of controls as part of the risk assessment performed during the review period.	No exceptions noted.
1.22	Security training is provided to employees during the onboarding process.	Inspected the onboarding presentation and meeting invite for a sample of employees hired during the review period to determine that security training was provided during the onboarding process for each employee sampled.	No exceptions noted.
1.23	Management utilizes a security training system to conduct a phishing exercise on an annual basis to monitor employees' security awareness.	Inspected the security training system monitoring reports to determine that management utilized a security training system to conduct a phishing exercise during the review period to monitor employee's security awareness.	No exceptions noted.
Administrative Safeguards			
§164.308(a): A covered entity or business associate must in accordance with 164.306:			
§164.308(a)(1)(i) **Security Management Process**: Implement policies and procedures to prevent, detect, contain, and correct security violations.			
1.24	Management has defined configuration standards in the information security policies and procedures.	Inspected the Security Governance Policy to determine that management defined configuration standards in the information security policies and procedures.	No exceptions noted.
1.25	Policies and procedures are in place regarding the detection, logging, and monitoring of unknown or unauthorized components into the environment.	Inspected the Security Governance Policy to determine that documented policies and procedures were in place regarding the detection, logging, and monitoring of unknown or unauthorized components in the environment.	No exceptions noted.
1.26	Documented incident response policies and procedures are in place to guide personnel in identifying, reporting, handling, and communicating security incidents.	Inspected the Security Governance Policy and the Incident Response Policy to determine that documented incident response policies and procedures were in place to guide personnel in identifying, reporting, handling, and communicating security incidents.	No exceptions noted.

#	Description of Service Organization's Controls	Service Auditor's Tests of Controls	Test Results
1.27	Documented incident response policies and procedures define roles, responsibilities, and required activities for analyzing, responding to, and recovering from security incidents.	Inspected the Incident Response Policy to determine that documented incident response policies and procedures defined roles, responsibilities, and required activities for analyzing, responding to, and recovering from security incidents.	No exceptions noted.
§164.308(a)(1)(ii)(A) **Risk Analysis**: Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity or business associate.			
1.28	The organization maintains a documented Security Objectives Guidelines policy that defines information security objectives to be aligned with business goals, information security risks, and regulatory requirements.	Inspected the Security Objectives Guidelines to determine that the organization maintained a documented policy that defined information security objectives to be aligned with business goals, information security risks, and regulatory requirements.	No exceptions noted.
1.29	Management performs an annual risk assessment to identify risks that could impact the achievement of the company's information security objectives. Identified risks are assessed using a risk rating methodology.	Inspected the risk assessment matrix to determine that management performed a formal risk assessment during the review period that identified risks to the company's security objectives and that identified risks were assessed using a risk documented risk rating methodology.	No exceptions noted.
1.30	Management has defined a formal risk assessment policy that specified the process for identifying internal and external threats and vulnerabilities, evaluating and addressing risks, and defining specified risk tolerances.	Inspected the Risk Management Policy to determine that management defined a formal risk assessment policy that specified the process for identifying internal and external threats and vulnerabilities, evaluating and addressing risks and defined specified risk tolerances.	No exceptions noted.
1.31	Management selects and documents risk treatment plans to address risks identified during the annual risk assessment process. Treatment plans include the implementation of mitigating controls to reduce residual risk to acceptable levels and are assigned to process owners.	Inspected the risk assessment matrix to determine that management selected and documented risk treatment plans for risks identified during the risk assessment process performed during the review period and that those plans included mitigating controls to reduce residual risk to acceptable levels and were assigned to process owners.	No exceptions noted.
1.32	A formal risk assessment is performed on an annual basis that identifies and assesses the types of fraud that could impact the achievement of objectives.	Inspected the risk assessment matrix to determine that a formal risk assessment was performed during the review period that identified and assessed the types of fraud that could impact the achievement of objectives.	No exceptions noted.

#	Description of Service Organization's Controls	Service Auditor's Tests of Controls	Test Results
1.33	Management considers fraud risks related to incentives, opportunities, employee conduct, and technology-related threats that could enable or justify fraudulent activity as part of the annual risk assessment.	Inspected the risk assessment matrix to determine that management considered fraud risks related to incentives, opportunities, employee conduct, and technology-related threats that could enable or justify fraudulent activity as part of the risk assessment performed during the review period.	No exceptions noted.
1.34	A formal risk assessment is performed on an annual basis to identify internal and external threats and vulnerabilities that could impair system commitments and requirements.	Inspected the risk assessment matrix to determine that a formal risk assessment was performed during the review period that identified internal and external threats and vulnerabilities that could impair system commitments and requirements.	No exceptions noted.
1.35	Changes in vendor and third-party relationships are considered and evaluated as part of the annual risk assessment.	Inspected the risk assessment matrix to determine that management considered and evaluated changes in vendor and third-party relationships as part of the risk assessment performed during the review period.	No exceptions noted.
1.36	Profisee conducts an internal audit of their information security management system and internal controls annually.	Inspected the internal audit report and meeting invite to determine that Profisee conducted an internal audit of their information security management system and internal controls during the review period.	No exceptions noted.
§164.308(a)(1)(ii)(B) **Risk Management**: Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with §164.306(a).			
1.37	Management selects and documents risk treatment plans to address risks identified during the annual risk assessment process. Treatment plans include the implementation of mitigating controls to reduce residual risk to acceptable levels and are assigned to process owners.	Inspected the risk assessment matrix to determine that management selected and documented risk treatment plans for risks identified during the risk assessment process performed during the review period and that those plans included mitigating controls to reduce residual risk to acceptable levels and were assigned to process owners.	No exceptions noted.
1.38	Profisee conducts an internal audit of their information security management system and internal controls annually.	Inspected the internal audit report and meeting invite to determine that Profisee conducted an internal audit of their information security management system and internal controls during the review period.	No exceptions noted.

#	Description of Service Organization's Controls	Service Auditor's Tests of Controls	Test Results
1.39	The use of technology in the selection and development of controls is evaluated by management as part of the annual risk assessment.	Inspected the risk assessment matrix to determine that management evaluated the use of technology in the selection and development of controls as part of the risk assessment performed during the review period.	No exceptions noted.
1.40	An annual information security meeting is conducted for the ISC to plan and report on the performance of the information security program to the CEO.	Inspected the most recent annual information security meeting minutes and calendar invite to determine that the information security meeting was conducted within the review period for the ISC to plan and report on the performance of the information security program to the CEO.	No exceptions noted.
1.41	The Information Security Team conducts a weekly meeting to review the Security Planner tracker, which tracks information security initiatives and status updates.	Inspected the Information Security Team weekly reoccurring meeting invite and the Security Planning tracker to determine that the Information Security Team conducted weekly meetings to review the Security Planner tracker, which tracked information security initiatives and status updates.	No exceptions noted.
§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.			
1.42	An Employee Handbook including a code of conduct is documented to communicate workforce conduct standards and enforcement procedures to employees. The handbook includes disciplinary actions for employee misconduct or violations of the employee handbook standards, which can include termination and suspension.	Inspected the Employee Handbook to determine that an Employee Handbook included a code of conduct and was documented to communicate workforce conduct standards and enforcement procedures to employees including disciplinary actions for employee misconduct or violations of the employee handbook standards, which included termination and suspension.	No exceptions noted.
1.43	Employees are required to acknowledge the Employee Handbook during onboarding which includes confidentiality and nondisclosure requirements.	Inspected the signed Employee Handbook acknowledgement for a sample of employees hired during the review period to determine that each sampled employee acknowledged the Employee Handbook during onboarding which included confidentiality and nondisclosure requirements.	No exceptions noted.

#	Description of Service Organization's Controls	Service Auditor's Tests of Controls	Test Results
§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.			
1.44	An annual information security meeting is conducted for the ISC to plan and report on the performance of the information security program to the CEO.	Inspected the most recent annual information security meeting minutes and calendar invite to determine that the information security meeting was conducted within the review period for the ISC to plan and report on the performance of the information security program to the CEO.	No exceptions noted.
1.45	The Information Security Team conducts a weekly meeting to review the Security Planner tracker, which tracks information security initiatives and status updates.	Inspected the Information Security Team weekly reoccurring meeting invite and the Security Planning tracker to determine that the Information Security Team conducted weekly meetings to review the Security Planner tracker, which tracked information security initiatives and status updates.	No exceptions noted.
1.46	Profisee conducts an internal audit of their information security management system and internal controls annually.	Inspected the internal audit report and meeting invite to determine that Profisee conducted an internal audit of their information security management system and internal controls during the review period.	No exceptions noted.
1.47	An IDPS is utilized to monitor network events for possible or actual network security breaches and is configured to notify personnel upon intrusion detection.	Inspected the IDPS alerting dashboard and configurations, and example alert generated during the review period to determine that an IDPS was utilized to monitor network events for possible or actual network security breaches and was configured to notify personnel upon intrusion detection.	No exceptions noted.
1.48	Management reviews the company's incident response and escalation procedures annually for effectiveness.	Inspected the most recent annual information security meeting minutes, calendar invite, and meeting transcript to determine that management reviewed the company's incident response and escalation procedures during the review period for effectiveness	No exceptions noted.
§164.308(a)(2) **Assigned Security Responsibility**: Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the covered entity or business associate.			
1.49	A Security Governance Policy has been formally documented to define the oversight, structures, authorities, and responsibilities associated with the organization's information security program.	Inspected the Security Governance Policy to determine that the Security Governance Policy was formally documented and defined the oversight, structures, authorities, and responsibilities associated with the organization's information security program.	No exceptions noted.

#	Description of Service Organization's Controls	Service Auditor's Tests of Controls	Test Results
1.50	Policies and procedures formally assign responsibility for the development, and performance of internal control to individuals and teams throughout the organization. The ISC is responsible for coordinating the development and implementation of the information security requirements associated with the organization's information security objectives.	Inspected the Security Governance Policy and the Security Objectives Guidelines to determine that policies and procedures formally assigned responsibility for the development, and performance of internal control to individuals and teams throughout the organization and that the ISC was responsible for coordinating the development and implementation of the information security requirements associated with the organization's information security objectives.	No exceptions noted.
1.51	An annual information security meeting is conducted for the ISC to plan and report on the performance of the information security program to the CEO.	Inspected the most recent annual information security meeting minutes and calendar invite to determine that the information security meeting was conducted within the review period for the ISC to plan and report on the performance of the information security program to the CEO.	No exceptions noted.
§164.308(a)(3)(i) **Workforce Security**: Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to electronic protected health information.			
1.52	The company network domains are configured to authenticate users via a unique user account and minimum password requirements including MFA.	Inspected the company network domains password configurations and user account listings to determine that company network domains were configured to authenticate users via a unique user account and minimum password requirements including MFA.	No exceptions noted.
1.53	The company network domains are configured to enforce an account lockout threshold and duration.	Inspected the company network domain lockout configurations to determine that the company network domains were configured to enforce an account lockout threshold and duration.	No exceptions noted.
1.54	Production servers are configured to enforce SSO authentication and inherits the unique user account and minimum password requirements (including MFA) enforced via the company's corporate network domain.	Inspected the production server SSO authentication configurations to determine that production servers were configured to enforce SSO authentication and inherited the unique user account and minimum password requirements (including MFA) enforced via the company's corporate network domain.	No exceptions noted.

#	Description of Service Organization's Controls	Service Auditor's Tests of Controls	Test Results
1.55	Production databases are configured to enforce SSO authentication and inherits the unique user account and minimum password requirements (including MFA) enforced via the company's production network domain.	Inspected the production database SSO authentication configurations to determine that production databases were configured to enforce SSO authentication and inherited the unique user account and minimum password requirements (including MFA) enforced via the company's production network domain.	No exceptions noted.
1.56	VPN users are authenticated via MFA prior to being granted remote access to the system.	Inspected the VPN authentication configurations to determine that VPN users were authenticated via MFA prior to being granted remote access to the system.	No exceptions noted.
1.57	Administrative access privileges to company network domains are restricted to user accounts accessible by authorized IT personnel.	Inspected the company network domains administrator listings with the assistance of the senior security engineer to determine that administrative access privileges to company network domains were restricted to user accounts accessible by authorized IT personnel.	No exceptions noted.
1.58	Administrative access privileges to production servers and databases are restricted to user accounts accessible by authorized IT personnel.	Inspected the production server and database administrator listings with the assistance of the senior security engineer to determine that administrative access privileges to production servers and databases were restricted to user accounts accessible by authorized IT personnel.	No exceptions noted.
1.59	The ability to administer VPN access is restricted to authorized IT personnel.	Inspected the listing of users with the ability to administer the VPN with the assistance of the senior security engineer to determine that the ability to administer VPN access was restricted to authorized IT personnel.	No exceptions noted.
1.60	Predefined user access groups are utilized to assign role-based access privileges and segregate access to in-scope systems.	Inspected the user access listings to the company network domains, production servers and databases, and VPN to determine that predefined user access groups were utilized to assign role-based access privileges and segregate access to in-scope systems.	No exceptions noted.
1.61	Production data is encrypted at rest.	Inspected the data encryption configurations to determine that production data was encrypted at rest.	No exceptions noted.

#	Description of Service Organization's Controls	Service Auditor's Tests of Controls	Test Results
1.62	The organization utilizes Azure Key Vault to securely store encryption keys.	Inspected the Azure Key Vault settings to determine that the organization utilized Azure Key Vault to securely store encryption keys.	No exceptions noted.
1.63	Workstations are configured to terminate inactive sessions after five minutes of inactivity.	Inspected the display lock configuration to determine that workstations were configured to terminate inactive sessions after five minutes of inactivity.	No exceptions noted.
1.64	Logical access to systems is approved and initiated by authorized HR personnel through an onboarding ticketing process and provisioned by IT personnel.	Inspected the onboarding request tickets for a sample of employees hired during the review period to determine logical access to systems was approved and initiated by authorized HR personnel and that access was provisioned by IT personnel through a documented ticketing process for each employee sampled.	No exceptions noted.
1.65	Personnel access requests to production databases containing customer data require a documented business case and support portal ticket.	Inspected the documented business case and support portal ticket for a sample of personnel access requests to production databases during the review period to determine that each access request sampled to production databases containing customer data required a documented business case and support portal ticket.	No exceptions noted.
§164.308(a)(3)(ii)(A) **Authorization and/or Supervisions (Addressable)**: Implement procedures for the authorization and/or supervision of workforce members who work with electronic protected health information or in locations where it might be accessed.			
1.66	Logical access to systems is approved and initiated by authorized HR personnel through an onboarding ticketing process and provisioned by IT personnel.	Inspected the onboarding request tickets for a sample of employees hired during the review period to determine logical access to systems was approved and initiated by authorized HR personnel and that access was provisioned by IT personnel through a documented ticketing process for each employee sampled.	No exceptions noted.
1.67	Personnel access requests to production databases containing customer data require a documented business case and support portal ticket.	Inspected the documented business case and support portal ticket for a sample of personnel access requests to production databases during the review period to determine that each access request sampled to production databases containing customer data required a documented business case and support portal ticket.	No exceptions noted.

#	Description of Service Organization's Controls	Service Auditor's Tests of Controls	Test Results
1.68	Policies and procedures formally assign responsibility for the development, and performance of internal control to individuals and teams throughout the organization. The ISC is responsible for coordinating the development and implementation of the information security requirements associated with the organization's information security objectives.	Inspected the Security Governance Policy and the Security Objectives Guidelines to determine that policies and procedures formally assigned responsibility for the development, and performance of internal control to individuals and teams throughout the organization and that the ISC was responsible for coordinating the development and implementation of the information security requirements associated with the organization's information security objectives.	No exceptions noted.
1.69	An annual information security meeting is conducted for the ISC to plan and report on the performance of the information security program to the CEO.	Inspected the most recent annual information security meeting minutes and calendar invite to determine that the information security meeting was conducted within the review period for the ISC to plan and report on the performance of the information security program to the CEO.	No exceptions noted.
1.70	The Information Security Team conducts a weekly meeting to review the Security Planner tracker, which tracks information security initiatives and status updates.	Inspected the Information Security Team weekly reoccurring meeting invite and the Security Planning tracker to determine that the Information Security Team conducted weekly meetings to review the Security Planner tracker, which tracked information security initiatives and status updates.	No exceptions noted.
§164.308(a)(3)(ii)(B) **Workforce Clearance Procedure (Addressable)**: Implement procedures to determine that the access of a workforce member to electronic protected health information is appropriate.			
1.71	Logical access to systems is approved and initiated by authorized HR personnel through an onboarding ticketing process and provisioned by IT personnel.	Inspected the onboarding request tickets for a sample of employees hired during the review period to determine logical access to systems was approved and initiated by authorized HR personnel and that access was provisioned by IT personnel through a documented ticketing process for each employee sampled.	No exceptions noted.
1.72	Personnel access requests to production databases containing customer data require a documented business case and support portal ticket.	Inspected the documented business case and support portal ticket for a sample of personnel access requests to production databases during the review period to determine that each access request sampled to production databases containing customer data required a documented business case and support portal ticket.	No exceptions noted.

#	Description of Service Organization's Controls	Service Auditor's Tests of Controls	Test Results
§164.308(a)(3)(ii)(C) **Termination Procedures (Addressable)**: Implement procedures for terminating access to electronic protected health information when the employment of, or other arrangement with, a workforce member ends or as required by determinations made as specified in paragraph (a)(3)(ii)(b) of this section.			
1.73	Logical access to systems is revoked from personnel as a component of the termination process.	Inspected the user access listings and offboarding emails for a sample of employees terminated during the review period to determine that logical access to systems was revoked for each employee sampled as a component of the termination process.	No exceptions noted.
§164.308(a)(4)(i) **Information Access Management**: Implement policies and procedures for authorizing access to electronic protected health information that are consistent with the applicable requirements of subpart E of this part.			
1.74	Logical access to systems is approved and initiated by authorized HR personnel through an onboarding ticketing process and provisioned by IT personnel.	Inspected the onboarding request tickets for a sample of employees hired during the review period to determine logical access to systems was approved and initiated by authorized HR personnel and that access was provisioned by IT personnel through a documented ticketing process for each employee sampled.	No exceptions noted.
1.75	Personnel access requests to production databases containing customer data require a documented business case and support portal ticket.	Inspected the documented business case and support portal ticket for a sample of personnel access requests to production databases during the review period to determine that each access request sampled to production databases containing customer data required a documented business case and support portal ticket.	No exceptions noted.
§164.308(a)(4)(ii)(A) **Isolating Health Care Clearinghouse Functions**: If a health care clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the electronic protected health information of the clearinghouse from unauthorized access by the larger organization.			
	Not Applicable – Profisee is not a covered entity or a health care clearinghouse.		
§164.308(a)(4)(ii)(B) **Access Authorization (Addressable)**: Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism.			
1.76	Management has defined configuration standards in the information security policies and procedures.	Inspected the Security Governance Policy to determine that management defined configuration standards in the information security policies and procedures.	No exceptions noted.

#	Description of Service Organization's Controls	Service Auditor's Tests of Controls	Test Results
1.77	The company network domains are configured to authenticate users via a unique user account and minimum password requirements including MFA.	Inspected the company network domains password configurations and user account listings to determine that company network domains were configured to authenticate users via a unique user account and minimum password requirements including MFA.	No exceptions noted.
1.78	Production servers are configured to enforce SSO authentication and inherits the unique user account and minimum password requirements (including MFA) enforced via the company's corporate network domain.	Inspected the production server SSO authentication configurations to determine that production servers were configured to enforce SSO authentication and inherited the unique user account and minimum password requirements (including MFA) enforced via the company's corporate network domain.	No exceptions noted.
1.79	Production databases are configured to enforce SSO authentication and inherits the unique user account and minimum password requirements (including MFA) enforced via the company's production network domain.	Inspected the production database SSO authentication configurations to determine that production databases were configured to enforce SSO authentication and inherited the unique user account and minimum password requirements (including MFA) enforced via the company's production network domain.	No exceptions noted.
1.80	VPN users are authenticated via MFA prior to being granted remote access to the system.	Inspected the VPN authentication configurations to determine that VPN users were authenticated via MFA prior to being granted remote access to the system.	No exceptions noted.
§164.308(a)(4)(ii)(C) **Access Establishment and Modification (Addressable)**: 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.			
1.81	Management has defined configuration standards in the information security policies and procedures.	Inspected the Security Governance Policy to determine that management defined configuration standards in the information security policies and procedures.	No exceptions noted.
1.82	Logical access to systems is approved and initiated by authorized HR personnel through an onboarding ticketing process and provisioned by IT personnel.	Inspected the onboarding request tickets for a sample of employees hired during the review period to determine logical access to systems was approved and initiated by authorized HR personnel and that access was provisioned by IT personnel through a documented ticketing process for each employee sampled.	No exceptions noted.

#	Description of Service Organization's Controls	Service Auditor's Tests of Controls	Test Results
1.83	Personnel access requests to production databases containing customer data require a documented business case and support portal ticket.	Inspected the documented business case and support portal ticket for a sample of personnel access requests to production databases during the review period to determine that each access request sampled to production databases containing customer data required a documented business case and support portal ticket.	No exceptions noted.
1.84	Logical access to systems is revoked from personnel as a component of the termination process.	Inspected the user access listings and offboarding emails for a sample of employees terminated during the review period to determine that logical access to systems was revoked for each employee sampled as a component of the termination process.	No exceptions noted.
§164.308(a)(5)(i) **Security Awareness Training**: Implement a security awareness and training program for all members of its workforce (including management).			
1.85	Security training is provided to employees during the onboarding process.	Inspected the onboarding presentation and meeting invite for a sample of employees hired during the review period to determine that security training was provided during the onboarding process for each employee sampled.	No exceptions noted.
1.86	Management utilizes a security training system to conduct a phishing exercise on an annual basis to monitor employees' security awareness.	Inspected the security training system monitoring reports to determine that management utilized a security training system to conduct a phishing exercise during the review period to monitor employee's security awareness.	No exceptions noted.
§164.308(a)(5)(ii)(A) **Security Reminders (Addressable)**: Implement periodic security updates.			
1.87	Management utilizes a security training system to conduct a phishing exercise on an annual basis to monitor employees' security awareness.	Inspected the security training system monitoring reports to determine that management utilized a security training system to conduct a phishing exercise during the review period to monitor employee's security awareness.	No exceptions noted.
1.88	All-hands meetings are held on at least a monthly basis to communicate organizational updates with employees.	Inspected the all-hands meeting invite and/or recordings for a sample of months during the review period to determine that an all-hands meeting was held to communicate organizational updates with employees for each month sampled.	No exceptions noted.

#	Description of Service Organization's Controls	Service Auditor's Tests of Controls	Test Results
§164.308(a)(5)(ii)(B) **Protection from Malicious Software (Addressable)**: Implement procedures for guarding against, detecting, and reporting malicious software.			
1.89	Documented incident response policies and procedures are in place to guide personnel in identifying, reporting, handling, and communicating security incidents.	Inspected the Security Governance Policy and the Incident Response Policy to determine that documented incident response policies and procedures were in place to guide personnel in identifying, reporting, handling, and communicating security incidents.	No exceptions noted.
1.90	Centrally managed antivirus software is installed on employee workstations and production servers and databases to scan and prevent malware.	Inspected the antivirus software listing of registered devices to determine that centrally managed antivirus software was installed on employee workstations to scan and prevent malware.	No exceptions noted.
		Inspected the antivirus software listing of registered devices to determine that centrally managed antivirus software was installed on production servers and databases to scan and prevent malware.	No exceptions noted.
1.91	Employee workstations are restricted from writing to removable storage devices.	Inspected the endpoint device restriction configuration to determine that employee workstations were restricted from writing to removable storage devices.	No exceptions noted.
1.92	Employee workstations are configured to require system patches and updates to be installed during predefined schedules.	Inspected the MDM device update configuration to determine that employee workstations were configured to require system patches and updates to be installed during predefined schedules.	No exceptions noted.
§164.308(a)(5)(ii)(C) **Log-In Monitoring (Addressable)**: Implement procedures for monitoring log-in attempts and reporting discrepancies.			
1.93	An IDPS is utilized to monitor network events for possible or actual network security breaches and is configured to notify personnel upon intrusion detection.	Inspected the IDPS alerting dashboard and configurations, and example alert generated during the review period to determine that an IDPS was utilized to monitor network events for possible or actual network security breaches and was configured to notify personnel upon intrusion detection.	No exceptions noted.
§164.308(a)(5)(ii)(D) **Password Management (Addressable)**: Implement procedures for creating, changing, and safeguarding passwords.			
1.94	Management has defined configuration standards in the information security policies and procedures.	Inspected the Security Governance Policy to determine that management defined configuration standards in the information security policies and procedures.	No exceptions noted.

#	Description of Service Organization's Controls	Service Auditor's Tests of Controls	Test Results
1.95	The company network domains are configured to authenticate users via a unique user account and minimum password requirements including MFA.	Inspected the company network domains password configurations and user account listings to determine that company network domains were configured to authenticate users via a unique user account and minimum password requirements including MFA.	No exceptions noted.
1.96	Production servers are configured to enforce SSO authentication and inherits the unique user account and minimum password requirements (including MFA) enforced via the company's corporate network domain.	Inspected the production server SSO authentication configurations to determine that production servers were configured to enforce SSO authentication and inherited the unique user account and minimum password requirements (including MFA) enforced via the company's corporate network domain.	No exceptions noted.
1.97	Production databases are configured to enforce SSO authentication and inherits the unique user account and minimum password requirements (including MFA) enforced via the company's production network domain.	Inspected the production database SSO authentication configurations to determine that production databases were configured to enforce SSO authentication and inherited the unique user account and minimum password requirements (including MFA) enforced via the company's production network domain.	No exceptions noted.
1.98	VPN users are authenticated via MFA prior to being granted remote access to the system.	Inspected the VPN authentication configurations to determine that VPN users were authenticated via MFA prior to being granted remote access to the system.	No exceptions noted.
§164.308(a)(6)(i) **Security Incident Procedures**: Implement policies and procedures to address security incidents.			
1.99	Documented incident response policies and procedures are in place to guide personnel in identifying, reporting, handling, and communicating security incidents.	Inspected the Security Governance Policy and the Incident Response Policy to determine that documented incident response policies and procedures were in place to guide personnel in identifying, reporting, handling, and communicating security incidents.	No exceptions noted.
1.100	Documented incident response policies and procedures define roles, responsibilities, and required activities for analyzing, responding to, and recovering from security incidents.	Inspected the Incident Response Policy to determine that documented incident response policies and procedures defined roles, responsibilities, and required activities for analyzing, responding to, and recovering from security incidents.	No exceptions noted.

#	Description of Service Organization's Controls	Service Auditor's Tests of Controls	Test Results
1.101	Management reviews the company's incident response and escalation procedures annually for effectiveness.	Inspected the most recent annual information security meeting minutes, calendar invite, and meeting transcript to determine that management reviewed the company's incident response and escalation procedures during the review period for effectiveness	No exceptions noted.
1.102	Incidents are documented and tracked in a standardized ticketing system and updated to reflect the planned incident and problem resolution.	Nonoccurrence: Refer to the test results for control activity CC7.3.2.	
1.103	A security incident analysis is performed for security incidents to determine the root cause and system impact.	Nonoccurrence: Refer to the test results for control activity CC7.3.2.	
1.104	Security incidents resulting in the unauthorized use or disclosure of personal information are communicated to the affected users.	Nonoccurrence: Refer to the test results for control activity CC7.3.2.	
§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.			
1.105	Documented incident response policies and procedures define roles, responsibilities, and required activities for analyzing, responding to, and recovering from security incidents.	Inspected the Incident Response Policy to determine that documented incident response policies and procedures defined roles, responsibilities, and required activities for analyzing, responding to, and recovering from security incidents.	No exceptions noted.
1.106	Incidents are documented and tracked in a standardized ticketing system and updated to reflect the planned incident and problem resolution.	Nonoccurrence: Refer to the test results for control activity CC7.3.2.	
1.107	A security incident analysis is performed for security incidents to determine the root cause and system impact.	Nonoccurrence: Refer to the test results for control activity CC7.3.2.	
1.108	Security incidents resulting in the unauthorized use or disclosure of personal information are communicated to the affected users.	Nonoccurrence: Refer to the test results for control activity CC7.3.2.	

#	Description of Service Organization's Controls	Service Auditor's Tests of Controls	Test Results
§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 electronic protected health information.			
1.109	A disaster recovery and business continuity plan is documented to identify and reduce risks, limit the consequences of damaging incidents, and ensure the timely resumption of essential operations.	Inspected the Disaster Recovery and Business Continuity Plan to determine that it was documented to identify and reduce risks, limit the consequences of damaging incidents, and ensure the timely resumption of essential operations.	No exceptions noted.
1.110	The disaster recovery and business continuity plan is updated and approved on an annual basis.	Inspected the Disaster Recovery and Business Continuity Plan to determine that it was updated and reviewed during the review period.	No exceptions noted.
1.111	A disaster recovery failover test that includes data backup restoration is performed on an annual basis.	Inspected the most recently completed disaster recovery test to determine that a disaster recovery failover test that included a data backup restoration was performed during the review period.	No exceptions noted.
1.112	Full and incremental backups of the SQL databases are performed based on predefined schedules.	Inspected the backup system schedule configuration to determine that full and incremental backups of the SQL databases were performed based on predefined schedules.	No exceptions noted.
1.113	The entity maintains cybersecurity insurance coverage to offset the financial loss that could result from a critical security incident or exploitation of a vulnerability.	Inspected the active cybersecurity policy coverage to determine that the entity maintained cybersecurity insurance coverage to offset the financial loss that could result from a critical security incident or exploitation of a vulnerability.	No exceptions noted.
§164.308(a)(7)(ii)(A) **Data Backup Plan**: Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information.			
1.114	A disaster recovery failover test that includes data backup restoration is performed on an annual basis.	Inspected the most recently completed disaster recovery test to determine that a disaster recovery failover test that included a data backup restoration was performed during the review period.	No exceptions noted.
1.115	Full and incremental backups of the SQL databases are performed based on predefined schedules.	Inspected the backup system schedule configuration to determine that full and incremental backups of the SQL databases were performed based on predefined schedules.	No exceptions noted.

#	Description of Service Organization's Controls	Service Auditor's Tests of Controls	Test Results
1.116	The ability to recall data backups is restricted to authorized SaaS Operations personnel.	Inspected the listing of users with the ability to recall data backups to determine that the ability to recall data backups was restricted to authorized SaaS Operations personnel.	No exceptions noted.
§164.308(a)(7)(ii)(B) **Disaster Recovery Plan**: Establish (and implement as needed) procedures to restore any loss of data.			
1.117	A disaster recovery and business continuity plan is documented to identify and reduce risks, limit the consequences of damaging incidents, and ensure the timely resumption of essential operations.	Inspected the Disaster Recovery and Business Continuity Plan to determine that it was documented to identify and reduce risks, limit the consequences of damaging incidents, and ensure the timely resumption of essential operations.	No exceptions noted.
1.118	The disaster recovery and business continuity plan is updated and approved on an annual basis.	Inspected the Disaster Recovery and Business Continuity Plan to determine that it was updated and reviewed during the review period.	No exceptions noted.
1.119	A disaster recovery failover test that includes data backup restoration is performed on an annual basis.	Inspected the most recently completed disaster recovery test to determine that a disaster recovery failover test that included a data backup restoration was performed during the review period.	No exceptions noted.
1.120	Full and incremental backups of the SQL databases are performed based on predefined schedules.	Inspected the backup system schedule configuration to determine that full and incremental backups of the SQL databases were performed based on predefined schedules.	No exceptions noted.
1.121	The entity maintains cybersecurity insurance coverage to offset the financial loss that could result from a critical security incident or exploitation of a vulnerability.	Inspected the active cybersecurity policy coverage to determine that the entity maintained cybersecurity insurance coverage to offset the financial loss that could result from a critical security incident or exploitation of a vulnerability.	No exceptions noted.
§164.308(a)(7)(ii)(C) **Emergency Mode Operation Plan**: Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of electronic protected health information while operating in emergency mode.			
1.122	A disaster recovery and business continuity plan is documented to identify and reduce risks, limit the consequences of damaging incidents, and ensure the timely resumption of essential operations.	Inspected the Disaster Recovery and Business Continuity Plan to determine that it was documented to identify and reduce risks, limit the consequences of damaging incidents, and ensure the timely resumption of essential operations.	No exceptions noted.

#	Description of Service Organization's Controls	Service Auditor's Tests of Controls	Test Results
1.123	The disaster recovery and business continuity plan is updated and approved on an annual basis.	Inspected the Disaster Recovery and Business Continuity Plan to determine that it was updated and reviewed during the review period.	No exceptions noted.
1.124	A disaster recovery failover test that includes data backup restoration is performed on an annual basis.	Inspected the most recently completed disaster recovery test to determine that a disaster recovery failover test that included a data backup restoration was performed during the review period.	No exceptions noted.
§164.308(a)(7)(ii)(D) **Testing and Revision Procedures (Addressable)**: Implement procedures for periodic testing and revision of contingency plans.			
1.125	The disaster recovery and business continuity plan is updated and approved on an annual basis.	Inspected the Disaster Recovery and Business Continuity Plan to determine that it was updated and reviewed during the review period.	No exceptions noted.
1.126	A disaster recovery failover test that includes data backup restoration is performed on an annual basis.	Inspected the most recently completed disaster recovery test to determine that a disaster recovery failover test that included a data backup restoration was performed during the review period.	No exceptions noted.
§164.308(a)(7)(ii)(E) **Applications and Data Criticality Analysis (Addressable)**: Assess the relative criticality of specific applications and data in support of other contingency plan components.			
1.127	An inventory of system assets and components is maintained to classify and manage the information assets.	Inspected the system inventory listing to determine that an inventory of system assets and components was maintained to classify and manage the information assets.	No exceptions noted.
1.128	A disaster recovery and business continuity plan is documented to identify and reduce risks, limit the consequences of damaging incidents, and ensure the timely resumption of essential operations.	Inspected the Disaster Recovery and Business Continuity Plan to determine that it was documented to identify and reduce risks, limit the consequences of damaging incidents, and ensure the timely resumption of essential operations.	No exceptions noted.
1.129	The disaster recovery and business continuity plan is updated and approved on an annual basis.	Inspected the Disaster Recovery and Business Continuity Plan to determine that it was updated and reviewed during the review period.	No exceptions noted.
1.130	A disaster recovery failover test that includes data backup restoration is performed on an annual basis.	Inspected the most recently completed disaster recovery test to determine that a disaster recovery failover test that included a data backup restoration was performed during the review period.	No exceptions noted.

#	Description of Service Organization's Controls	Service Auditor's Tests of Controls	Test Results
§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 operational changes affecting the security of electronic protected health information, which establishes the extent to which a covered entity's or business associate's security policies and procedures meet the requirements of this subpart.			
1.131	An annual information security meeting is conducted for the ISC to plan and report on the performance of the information security program to the CEO.	Inspected the most recent annual information security meeting minutes and calendar invite to determine that the information security meeting was conducted within the review period for the ISC to plan and report on the performance of the information security program to the CEO.	No exceptions noted.
1.132	The Information Security Team conducts a weekly meeting to review the Security Planner tracker, which tracks information security initiatives and status updates.	Inspected the Information Security Team weekly reoccurring meeting invite and the Security Planning tracker to determine that the Information Security Team conducted weekly meetings to review the Security Planner tracker, which tracked information security initiatives and status updates.	No exceptions noted.
1.133	Management performs an annual risk assessment to identify risks that could impact the achievement of the company's information security objectives. Identified risks are assessed using a risk rating methodology.	Inspected the risk assessment matrix to determine that management performed a formal risk assessment during the review period that identified risks to the company's security objectives and that identified risks were assessed using a risk documented risk rating methodology.	No exceptions noted.
1.134	Management selects and documents risk treatment plans to address risks identified during the annual risk assessment process. Treatment plans include the implementation of mitigating controls to reduce residual risk to acceptable levels and are assigned to process owners.	Inspected the risk assessment matrix to determine that management selected and documented risk treatment plans for risks identified during the risk assessment process performed during the review period and that those plans included mitigating controls to reduce residual risk to acceptable levels and were assigned to process owners.	No exceptions noted.
1.135	A formal risk assessment is performed on an annual basis to identify internal and external threats and vulnerabilities that could impair system commitments and requirements.	Inspected the risk assessment matrix to determine that a formal risk assessment was performed during the review period that identified internal and external threats and vulnerabilities that could impair system commitments and requirements.	No exceptions noted.

#	Description of Service Organization's Controls	Service Auditor's Tests of Controls	Test Results
1.136	Profisee conducts an internal audit of their information security management system and internal controls annually.	Inspected the internal audit report and meeting invite to determine that Profisee conducted an internal audit of their information security management system and internal controls during the review period.	No exceptions noted.
§164.308(b)(1) **Business Associate Contracts and Other Arrangements**: A covered entity may permit a business associate to create, receive, maintain, or transmit electronic protected health information on the covered entity's behalf only if the covered entity obtains satisfactory assurances, in accordance with § 164.314(a) that the business associate will appropriately safeguard the information. A covered entity is not required to obtain such satisfactory assurances from a business associate that is a subcontractor.			
	Not Applicable – Profisee is not a covered entity.		
§164.308(b)(2): A business associate may permit a business associate that is a subcontractor to create, receive, maintain, or transmit electronic protected health information 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.			
1.137	A business associate agreement is in place for subcontractors that may create, receive, maintain, or transmit ePHI.	Inspected the business associate agreements for subcontractors that may create, receive maintain, or transmit ePHI to determine that a business associate agreement was in place.	No exceptions noted.
1.138	The entity has documented policies in place for managing third parties.	Inspected the Security Governance Policy to determine that the entity had documented policies in place for managing third parties.	No exceptions noted.
1.139	Changes in vendor and third-party relationships are considered and evaluated as part of the annual risk assessment.	Inspected the risk assessment matrix to determine that management considered and evaluated changes in vendor and third-party relationships as part of the risk assessment performed during the review period.	No exceptions noted.
§164.308(b)(3) **Written Contract or Other Arrangement**: Document the satisfactory assurances required by paragraph (b)(1) or (b)(2) of this section through a written contract or other arrangement with the business associate that meets the applicable requirements of § 164.314(a).			
1.140	A business associate agreement is in place for subcontractors that may create, receive, maintain, or transmit ePHI.	Inspected the business associate agreements for subcontractors that may create, receive maintain, or transmit ePHI to determine that a business associate agreement was in place.	No exceptions noted.
Physical Safeguards. A covered entity or business associate must, in accordance with § 164.306:			
§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.			
	Microsoft Azure is responsible for restricting physical access to data centers housing hardware and physical infrastructure in which production data resides.		
§164.310(a)(2)(i) **Contingency Operations (Addressable)**: 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.			
	Microsoft Azure is responsible for restricting physical access to data centers housing hardware and physical infrastructure in which production data resides.		

#	Description of Service Organization's Controls	Service Auditor's Tests of Controls	Test Results
§164.310(a)(2)(ii) **Facility Security Plan (Addressable)**: Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.			
	Microsoft Azure is responsible for restricting physical access to data centers housing hardware and physical infrastructure in which production data resides.		
§164.310(a)(2)(iii) **Access Controls and Validation Procedures (Addressable)**: 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.			
	Microsoft Azure is responsible for restricting physical access to data centers housing hardware and physical infrastructure in which production data resides.		
§164.310(a)(2)(iv) **Maintenance Records (Addressable)**: 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).			
	Microsoft Azure is responsible for restricting physical access to data centers housing hardware and physical infrastructure in which production data resides.		
§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 electronic protected health information.			
1.141	An Employee Handbook including a code of conduct is documented to communicate workforce conduct standards and enforcement procedures to employees. The handbook includes disciplinary actions for employee misconduct or violations of the employee handbook standards, which can include termination and suspension.	Inspected the Employee Handbook to determine that an Employee Handbook included a code of conduct and was documented to communicate workforce conduct standards and enforcement procedures to employees including disciplinary actions for employee misconduct or violations of the employee handbook standards, which included termination and suspension.	No exceptions noted.
1.142	Workstations are configured to terminate inactive sessions after five minutes of inactivity.	Inspected the display lock configuration to determine that workstations were configured to terminate inactive sessions after five minutes of inactivity.	No exceptions noted.
1.143	Employee workstations are restricted from writing to removable storage devices.	Inspected the MDM endpoint configuration to determine that employee workstations were restricted from writing to removable storage devices.	No exceptions noted.
§164.310(c) **Workstation Security**: Implement physical safeguards for all workstations that access electronic protected health information, to restrict access to authorized users.			
1.144	Workstations are configured to terminate inactive sessions after five minutes of inactivity.	Inspected the display lock configuration to determine that workstations were configured to terminate inactive sessions after five minutes of inactivity.	No exceptions noted.
1.145	Employee workstations are restricted from writing to removable storage devices.	Inspected the MDM endpoint configuration to determine that employee workstations were restricted from writing to removable storage devices.	No exceptions noted.

#	Description of Service Organization's Controls	Service Auditor's Tests of Controls	Test Results
§164.310(d)(1) **Device and Media Controls**: Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic protected health information, into and out of a facility, and the movement of these items within the facility.			
1.146	Employee workstations are restricted from writing to removable storage devices.	Inspected the MDM endpoint configuration to determine that employee workstations were restricted from writing to removable storage devices.	No exceptions noted.
	Microsoft Azure is responsible for controlling the receipt and removal of hardware and electronic media for the data centers housing physical infrastructure in which production data resides.		
§164.310(d)(2)(i) **Disposal**: Implement policies and procedures to address the final disposition of electronic protected health information and/or the hardware or electronic media on which it is stored.			
	Microsoft Azure is responsible for addressing the final disposition of hardware and electronic media for the data centers housing physical infrastructure in which production data resides.		
§164.310(d)(2)(ii) **Media Re-Use**: Implement procedures for removal of electronic protected health information from electronic media before the media are made available for re-use.			
	Microsoft Azure is responsible for implementing procedures regarding the removal and re-use of electronic media related to the data centers housing physical infrastructure in which production data resides.		
§164.310(d)(2)(iii) **Accountability (Addressable)**: Maintain a record of the movements of hardware and electronic media and any person responsible therefore.			
	Microsoft Azure is responsible for maintaining a record of the movements of hardware and electronic media for the data centers housing physical infrastructure in which production data resides.		
§164.310(d)(2)(iv) **Data Backup and Storage (Addressable)**: Create a retrievable, exact copy of electronic protected health information, when needed, before movement of equipment.			
1.147	The ability to recall data backups is restricted to authorized SaaS Operations personnel.	Inspected the listing of users with the ability to recall data backups to determine that the ability to recall data backups was restricted to authorized SaaS Operations personnel.	No exceptions noted.
1.148	Full and incremental backups of the SQL databases are performed based on predefined schedules.	Inspected the backup system schedule configuration to determine that full and incremental backups of the SQL databases were performed based on predefined schedules.	No exceptions noted.
	Microsoft Azure is responsible for maintaining a record of the movements of hardware and electronic media for the data centers housing physical infrastructure in which production data resides.		
Technical Safeguards. A covered entity or business associate must, in accordance with § 164.306:			
§164.312(a)(1) **Access Control**: Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in § 164.308(a)(4).			
1.149	Administrative access privileges to company network domains are restricted to user accounts accessible by authorized IT personnel.	Inspected the company network domains administrator listings with the assistance of the senior security engineer to determine that administrative access privileges to company network domains were restricted to user accounts accessible by authorized IT personnel.	No exceptions noted.

#	Description of Service Organization's Controls	Service Auditor's Tests of Controls	Test Results
1.150	Administrative access privileges to production servers and databases are restricted to user accounts accessible by authorized IT personnel.	Inspected the production server and database administrator listings with the assistance of the senior security engineer to determine that administrative access privileges to production servers and databases were restricted to user accounts accessible by authorized IT personnel.	No exceptions noted.
1.151	The ability to administer VPN access is restricted to authorized IT personnel.	Inspected the listing of users with the ability to administer the VPN with the assistance of the senior security engineer to determine that the ability to administer VPN access was restricted to authorized IT personnel.	No exceptions noted.
1.152	Predefined user access groups are utilized to assign role-based access privileges and segregate access to in-scope systems.	Inspected the user access listings to the company network domains, production servers and databases, and VPN to determine that predefined user access groups were utilized to assign role-based access privileges and segregate access to in-scope systems.	No exceptions noted.
1.153	Administrative access privileges to CI/CD system are restricted to user accounts accessible by authorized IT personnel.	Inspected the CI/CD administrator listings with the assistance of the senior security engineer to determine that administrative access privileges to the CI/CD system was restricted to user accounts accessible by authorized IT personnel.	No exceptions noted.
§164.312(a)(2)(i) **Unique User Identification**: Assign a unique name and/or number for identifying and tracking user identity.			
1.154	The company network domains are configured to authenticate users via a unique user account and minimum password requirements including MFA.	Inspected the company network domains password configurations and user account listings to determine that company network domains were configured to authenticate users via a unique user account and minimum password requirements including MFA.	No exceptions noted.
1.155	Production servers are configured to enforce SSO authentication and inherits the unique user account and minimum password requirements (including MFA) enforced via the company's corporate network domain.	Inspected the production server SSO authentication configurations to determine that production servers were configured to enforce SSO authentication and inherited the unique user account and minimum password requirements (including MFA) enforced via the company's corporate network domain.	No exceptions noted.

#	Description of Service Organization's Controls	Service Auditor's Tests of Controls	Test Results
1.156	Production databases are configured to enforce SSO authentication and inherits the unique user account and minimum password requirements (including MFA) enforced via the company's production network domain.	Inspected the production database SSO authentication configurations to determine that production databases were configured to enforce SSO authentication and inherited the unique user account and minimum password requirements (including MFA) enforced via the company's production network domain.	No exceptions noted.
1.157	VPN users are authenticated via MFA prior to being granted remote access to the system.	Inspected the VPN authentication configurations to determine that VPN users were authenticated via MFA prior to being granted remote access to the system.	No exceptions noted.
§164.312(a)(2)(ii) **Emergency Access Procedure**: Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency.			
1.158	A disaster recovery and business continuity plan is documented to identify and reduce risks, limit the consequences of damaging incidents, and ensure the timely resumption of essential operations.	Inspected the Disaster Recovery and Business Continuity Plan to determine that it was documented to identify and reduce risks, limit the consequences of damaging incidents, and ensure the timely resumption of essential operations.	No exceptions noted.
1.159	The disaster recovery and business continuity plan is updated and approved on an annual basis.	Inspected the Disaster Recovery and Business Continuity Plan to determine that it was updated and reviewed during the review period.	No exceptions noted.
1.160	A disaster recovery failover test that includes data backup restoration is performed on an annual basis.	Inspected the most recently completed disaster recovery test to determine that a disaster recovery failover test that included a data backup restoration was performed during the review period.	No exceptions noted.
§164.312(a)(2)(iii) **Automatic Logoff (Addressable)**: Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.			
1.161	Workstations are configured to terminate inactive sessions after five minutes of inactivity.	Inspected the display lock configuration to determine that workstations were configured to terminate inactive sessions after five minutes of inactivity.	No exceptions noted.
§164.312(a)(2)(iv) **Encryption and Decryption (Addressable)**: Implement a mechanism to encrypt and decrypt electronic protected health information.			
1.162	Production data is encrypted at rest.	Inspected the data encryption configurations to determine that production data was encrypted at rest.	No exceptions noted.
1.163	The organization utilizes Azure Key Vault to securely store encryption keys.	Inspected the Azure Key Vault settings to determine that the organization utilized Azure Key Vault to securely store encryption keys.	No exceptions noted.

#	Description of Service Organization's Controls	Service Auditor's Tests of Controls	Test Results
§164.312(b) **Audit Controls**: Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.			
1.164	Profisee conducts an internal audit of their information security management system and internal controls annually.	Inspected the internal audit report and meeting invite to determine that Profisee conducted an internal audit of their information security management system and internal controls during the review period.	No exceptions noted.
1.165	An IDPS is utilized to monitor network events for possible or actual network security breaches and is configured to notify personnel upon intrusion detection.	Inspected the IDPS alerting dashboard and configurations, and example alert generated during the review period to determine that an IDPS was utilized to monitor network events for possible or actual network security breaches and was configured to notify personnel upon intrusion detection.	No exceptions noted.
1.166	A firewall system is in place to filter unauthorized inbound network traffic from the Internet.	Inspected the firewall system ruleset configurations to determine that a firewall system was in place to filter unauthorized inbound network traffic from the Internet.	No exceptions noted.
1.167	Continuous vulnerability scanning is configured for production machines to identify vulnerabilities.	Inspected Defender for Cloud vulnerability settings to determine that continuous vulnerability scanning was configured for production machines to identify vulnerabilities.	No exceptions noted.
1.168	A third party performs a penetration test at least annually to identify and exploit vulnerabilities for the web application.	Inspected the web application penetration test report to determine that a third party performed a penetration test during the review period to identify and exploit vulnerabilities for the web application.	No exceptions noted.
1.169	A third party performs a penetration test at least annually to identify and exploit vulnerabilities for the internal network.	Inspected the internal network penetration test report to determine that a third party performed a penetration test during the review period to identify and exploit vulnerabilities for the internal network.	No exceptions noted.
§164.312(c)(1) **Integrity**: Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.			
1.170	The ability to recall data backups is restricted to authorized SaaS Operations personnel.	Inspected the listing of users with the ability to recall data backups to determine that the ability to recall data backups was restricted to authorized SaaS Operations personnel.	No exceptions noted.

#	Description of Service Organization's Controls	Service Auditor's Tests of Controls	Test Results
1.171	Full and incremental backups of the SQL databases are performed based on predefined schedules.	Inspected the backup system schedule configuration to determine that full and incremental backups of the SQL databases were performed based on predefined schedules.	No exceptions noted.
1.172	Production data is encrypted at rest.	Inspected the data encryption configurations to determine that production data was encrypted at rest.	No exceptions noted.
§164.312(c)(2) **Mechanism to Authenticate Electronic Protected Health Information (Addressable)**: Implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner.			
1.173	An IDPS is utilized to monitor network events for possible or actual network security breaches and is configured to notify personnel upon intrusion detection.	Inspected the IDPS alerting dashboard and configurations, and example alert generated during the review period to determine that an IDPS was utilized to monitor network events for possible or actual network security breaches and was configured to notify personnel upon intrusion detection.	No exceptions noted.
1.174	Encrypted VPN sessions are utilized for remote connectivity users.	Inspected the VPN encryption settings to determine that encrypted VPN sessions were utilized for remote connectivity users.	No exceptions noted.
1.175	Production web sessions are encrypted to protect the transmission of information over the Internet.	Inspected the TLS encryption configurations to determine that production web sessions were encrypted to protect the transmission of information over the Internet.	No exceptions noted.
1.176	Production data is encrypted at rest.	Inspected the data encryption configurations to determine that production data was encrypted at rest.	No exceptions noted.
§164.312(d) **Person or Entity Authentication**: Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.			
1.177	The company network domains are configured to authenticate users via a unique user account and minimum password requirements including MFA.	Inspected the company network domains password configurations and user account listings to determine that company network domains were configured to authenticate users via a unique user account and minimum password requirements including MFA.	No exceptions noted.
1.178	The company network domains are configured to enforce an account lockout threshold and duration.	Inspected the company network domain lockout configurations to determine that the company network domains were configured to enforce an account lockout threshold and duration.	No exceptions noted.

#	Description of Service Organization's Controls	Service Auditor's Tests of Controls	Test Results
1.179	Production servers are configured to enforce SSO authentication and inherits the unique user account and minimum password requirements (including MFA) enforced via the company's corporate network domain.	Inspected the production server SSO authentication configurations to determine that production servers were configured to enforce SSO authentication and inherited the unique user account and minimum password requirements (including MFA) enforced via the company's corporate network domain.	No exceptions noted.
1.180	Production databases are configured to enforce SSO authentication and inherits the unique user account and minimum password requirements (including MFA) enforced via the company's production network domain.	Inspected the production database SSO authentication configurations to determine that production databases were configured to enforce SSO authentication and inherited the unique user account and minimum password requirements (including MFA) enforced via the company's production network domain.	No exceptions noted.
1.181	VPN users are authenticated via MFA prior to being granted remote access to the system.	Inspected the VPN authentication configurations to determine that VPN users were authenticated via MFA prior to being granted remote access to the system.	No exceptions noted.
1.182	Administrative access privileges to company network domains are restricted to user accounts accessible by authorized IT personnel.	Inspected the company network domains administrator listings with the assistance of the senior security engineer to determine that administrative access privileges to company network domains were restricted to user accounts accessible by authorized IT personnel.	No exceptions noted.
1.183	Administrative access privileges to production servers and databases are restricted to user accounts accessible by authorized IT personnel.	Inspected the production server and database administrator listings with the assistance of the senior security engineer to determine that administrative access privileges to production servers and databases were restricted to user accounts accessible by authorized IT personnel.	No exceptions noted.
1.184	The ability to administer VPN access is restricted to authorized IT personnel.	Inspected the listing of users with the ability to administer the VPN with the assistance of the senior security engineer to determine that the ability to administer VPN access was restricted to authorized IT personnel.	No exceptions noted.

#	Description of Service Organization's Controls	Service Auditor's Tests of Controls	Test Results
1.185	Administrative access privileges to CI/CD system are restricted to user accounts accessible by authorized IT personnel.	Inspected the CI/CD administrator listings with the assistance of the senior security engineer to determine that administrative access privileges to the CI/CD system was restricted to user accounts accessible by authorized IT personnel.	No exceptions noted.
§164.312(e)(1) **Transmission Security**: Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.			
1.186	Encrypted VPN sessions are utilized for remote connectivity users.	Inspected the VPN encryption settings to determine that encrypted VPN sessions were utilized for remote connectivity users.	No exceptions noted.
1.187	Production web sessions are encrypted to protect the transmission of information over the Internet.	Inspected the TLS encryption configurations to determine that production web sessions were encrypted to protect the transmission of information over the Internet.	No exceptions noted.
§164.312(e)(2)(i) **Integrity Controls (Addressable)**: Implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of.			
1.188	Encrypted VPN sessions are utilized for remote connectivity users.	Inspected the VPN encryption settings to determine that encrypted VPN sessions were utilized for remote connectivity users.	No exceptions noted.
1.189	Production web sessions are encrypted to protect the transmission of information over the Internet.	Inspected the TLS encryption configurations to determine that production web sessions were encrypted to protect the transmission of information over the Internet.	No exceptions noted.
§164.312(e)(2)(ii) **Encryption (Addressable)**: Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.			
1.190	Production data is encrypted at rest.	Inspected the data encryption configurations to determine that production data was encrypted at rest.	No exceptions noted.
Organizational Requirements			
§164.314(a)(1) **Business Associate Contracts or Other Arrangements**: The contract or other arrangement between the covered entity and its business associate required by §164.308(b)(3) must meet the requirements of paragraph (a)(2)(i) or (a)(2)(ii) of this section, as applicable.			
1.191	A business associate agreement is in place for subcontractors that may create, receive, maintain, or transmit ePHI.	Inspected the business associate agreements for subcontractors that may create, receive maintain, or transmit ePHI to determine that a business associate agreement was in place.	No exceptions noted.

#	Description of Service Organization's Controls	Service Auditor's Tests of Controls	Test Results
§164.314(a)(2)(i) **Business Associate Contracts**: The contract must provide that the business associate will: (A) Comply with the applicable requirements of this subpart; (B) In accordance with § 164.308(b)(2), ensure that any subcontractors that create, receive, maintain, or transmit electronic protected health information on behalf of the business associate agree to comply with the applicable requirements of this subpart by entering into a contract or other arrangement that complies with this section; and (C) Report to the covered entity any security incident of which it becomes aware, including breaches of unsecured protected health information as required by § 164.410			
1.192	A business associate agreement is in place for subcontractors that may create, receive, maintain, or transmit ePHI.	Inspected the business associate agreements for subcontractors that may create, receive maintain, or transmit ePHI to determine that a business associate agreement was in place.	No exceptions noted.
§164.314(a)(2)(ii) **Other Arrangements**: The covered entity is in compliance with paragraph (a)(1) of this section if it has another arrangement in place that meets the requirements of § 164.504(e)(3).			
	Not Applicable – Profisee is not a covered entity or government entity.		
§164.314(a)(2)(iii) **Business Associate Contracts with Subcontractors**: The requirements of paragraphs (a)(2)(i) and (a)(2)(ii) of this section apply to the contract or other arrangement between a business associate and a subcontractor required by § 164.308(b)(4) in the same manner as such requirements apply to contracts or other arrangements between a covered entity and business associate.			
1.193	A business associate agreement is in place for subcontractors that may create, receive, maintain, or transmit ePHI.	Inspected the business associate agreements for subcontractors that may create, receive maintain, or transmit ePHI to determine that a business associate agreement was in place.	No exceptions noted.
§164.314(a)(b)(1) **Requirements for Group Health Plans**: Except when the only electronic protected health information 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 electronic protected health information created, received, maintained, or transmitted to or by the plan sponsor on behalf of the group health plan..			
	Not Applicable – Profisee is not a group health plan.		
§164.314(b)(2) 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 electronic protected health information 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 to whom it provides this information agrees to implement reasonable and appropriate security measures to protect the information. (iv) Report to the group health plan any security incident of which it becomes aware.			
	Not Applicable – Profisee is not a group health plan.		

#	Description of Service Organization's Controls	Service Auditor's Tests of Controls	Test Results
Policies and Procedures and Documentation Requirements. A covered entity or business associate must, in accordance with § 164.306:			
§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). This standard is not to be construed to permit or excuse an action that violates any other standard, implementation specification, or other requirements of this subpart. A covered entity or business associate may change its policies and procedures at any time, provided that the changes are documented and are implemented in accordance with this subpart.			
1.194	Organizational and information security policies and procedures are documented and made available to personnel through the Profisee's SharePoint site.	Inspected the company SharePoint site to determine that organizational and information security policies and procedures were documented and made available to personnel through the Profisee's SharePoint site.	No exceptions noted.
1.195	A Security Governance Policy has been formally documented to define the oversight, structures, authorities, and responsibilities associated with the organization's information security program.	Inspected the Security Governance Policy to determine that the Security Governance Policy was formally documented and defined the oversight, structures, authorities, and responsibilities associated with the organization's information security program.	No exceptions noted.
1.196	Policies and procedures formally assign responsibility for the development, and performance of internal control to individuals and teams throughout the organization. The ISC is responsible for coordinating the development and implementation of the information security requirements associated with the organization's information security objectives.	Inspected the Security Governance Policy and the Security Objectives Guidelines to determine that policies and procedures formally assigned responsibility for the development, and performance of internal control to individuals and teams throughout the organization and that the ISC was responsible for coordinating the development and implementation of the information security requirements associated with the organization's information security objectives.	No exceptions noted.
1.197	Documented incident response policies and procedures are in place to guide personnel in identifying, reporting, handling, and communicating security incidents.	Inspected the Security Governance Policy and the Incident Response Policy to determine that documented incident response policies and procedures were in place to guide personnel in identifying, reporting, handling, and communicating security incidents.	No exceptions noted.
1.198	Documented incident response policies and procedures define roles, responsibilities, and required activities for analyzing, responding to, and recovering from security incidents.	Inspected the Incident Response Policy to determine that documented incident response policies and procedures defined roles, responsibilities, and required activities for analyzing, responding to, and recovering from security incidents.	No exceptions noted.

#	Description of Service Organization's Controls	Service Auditor's Tests of Controls	Test Results
1.199	Management has defined configuration standards in the information security policies and procedures.	Inspected the Security Governance Policy to determine that management defined configuration standards in the information security policies and procedures.	No exceptions noted.
1.200	Policies and procedures are in place regarding the detection, logging, and monitoring of unknown or unauthorized components into the environment.	Inspected the Security Governance Policy to determine that documented policies and procedures were in place regarding the detection, logging, and monitoring of unknown or unauthorized components in the environment.	No exceptions noted.
1.201	Management reviews policies, procedures, and other control documents on an annual basis.	Inspected the most recent management review to determine that management reviewed policies, procedures, and other control documents during the review period.	No exceptions noted.
§164.316(b)(1) **Documentation**: (i) 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 or the action, activity, or assessment.			
1.202	Organizational and information security policies and procedures are documented and made available to personnel through the Profisee's SharePoint site.	Inspected the company SharePoint site to determine that organizational and information security policies and procedures were documented and made available to personnel through the Profisee's SharePoint site.	No exceptions noted.
1.203	Management reviews policies, procedures, and other control documents on an annual basis.	Inspected the most recent management review to determine that management reviewed policies, procedures, and other control documents during the review period.	No exceptions noted.
§164.316(b)(2)(i) **Time Limit**: Retain the documentation required by paragraph (b)(1) of this section for 6 years from the date of its creation or the date when it last was in effect, whichever is later.			
1.204	Policies and procedural documents are retained for a minimum of six years in accordance with regulatory and business requirements.	Inspected the company document repository retention configuration to determine that policies and procedural documents were retained for a minimum of six years in accordance with regulatory and business requirements.	No exceptions noted.
§164.316(b)(2)(ii) **Availability**: Make documentation available to those persons responsible for implementing the procedures to which the documentation pertains.			
1.205	Organizational and information security policies and procedures are documented and made available to personnel through the Profisee's SharePoint site.	Inspected the company SharePoint site to determine that organizational and information security policies and procedures were documented and made available to personnel through the Profisee's SharePoint site.	No exceptions noted.

#	Description of Service Organization's Controls	Service Auditor's Tests of Controls	Test Results
§164.316(b)(2)(iii) **Updates**: Review documentation periodically, and update as needed, in response to environmental or operational changes affecting the security of the electronic protected health information.			
1.206	Management reviews policies, procedures, and other control documents on an annual basis.	Inspected the most recent management review to determine that management reviewed policies, procedures, and other control documents during the review period.	No exceptions noted.

HITECH Breach Notification Rule

#	Description of Service Organization's Controls	Service Auditor's Tests of Controls	Test Results
Definitions			
§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) Breach excludes: (i) Any unintentional acquisition, access, or use of protected health information by a workforce member or person acting under the authority of a covered entity or a business associate, if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted under subpart E of this part.(ii) Any inadvertent disclosure by a person who is authorized to access protected health information at a covered entity or business associate to another person authorized to access protected health information at the same covered entity or business associate, or organized health care arrangement in which the covered entity participates, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted under subpart E of this part. (iii) A disclosure of protected health information where a covered entity or business associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information. (2) Except as provided in paragraph (1) of this definition, an acquisition, access, use, or disclosure of protected health information in a manner not permitted under subpart E is presumed to be a breach unless the covered entity or business associate, as applicable, demonstrates that there is a low probability that the protected health information has been compromised based on a risk assessment of at least the following factors:(i) The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification;(ii) The unauthorized person who used the protected health information or to whom the disclosure was made;(iii) Whether the protected health information was actually acquired or viewed; and (iv) The extent to which the risk to the protected health information has been mitigated. Unsecured protected health information means protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the Secretary in the guidance issued under section 13402(h)(2) of Public Law 111-5.		
	Note – This section is informational. Requirements are specified in the sections that follow.		
Notification to Individuals			
§164.404(a)(1): **Standard – General rule**. 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 – Profisee is not a covered entity.		
§164.404(a)(2): **Standard – Breaches treated as discovered**. 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 – Profisee is not a covered entity.		
§164.404(b): **Timeliness of Notification**. 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.			
	Not Applicable – Profisee is not a covered entity.		

#	Description of Service Organization's Controls	Service Auditor's Tests of Controls	Test Results
§164.404(c): **Content of Notification**. (1) Elements. 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 shall include a toll-free telephone number, an e-mail address, Web site, or postal address.(2) Plan Language Requirement. The notification required by paragraph (a) of this section shall be written in plain language.			
	Not Applicable – Profisee is not a covered entity.		
§164.404(d): **Methods of Individual Notification**. The notification required by paragraph (a) of this section shall be provided in the following form: (1) Written Notice. (i) 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 information becomes available. (ii) 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 is required. The notification may be provided in one or more mailings as information is available. (2) Substitute notice. In the case in which 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 reasonably 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).(i) In the case in which 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.(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 unsecured protected health information may be included in the breach. Additional notice in urgent situations. (3) Additional notice in urgent situations. 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 – Profisee is not a covered entity.		
Notification to the Media			
§164.406: (a) Standard. 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 as provided in §164.404(a)(2), notify prominent media outlets serving the State or jurisdiction. (b) Timeliness of notification. 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) Content of notification. The content of the notification required by paragraph (a) of this section shall meet the requirements of §164.404(c).			
	Not Applicable – Profisee is not a covered entity.		
Notification to the Secretary			
§164.408: (a) Standard. 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. (b) Breaches involving 500 or more individuals. For breaches of unsecured protected health information involving 500 or more individuals, a covered entity shall, except as provided in § 164.412, provide the notification required by paragraph (a) of this section contemporaneously with the notice required by § 164.404(a) and in the manner specified on the HHS Web site. (c) Breaches involving 500 or less individuals. 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 discovered during the preceding calendar year, in the manner specified on the HHS Web site.			
	Not Applicable – Profisee is not a covered entity.		

#	Description of Service Organization's Controls	Service Auditor's Tests of Controls	Test Results
Notification by a Business Associate			
§164.410: (a) Standard. (1) General Rule. A business associate shall, following the discovery of a breach of unsecured protected health information, notify the covered entity of such breach. (2) Breaches treated as discovered. For purposes of paragraph (a)(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).(b) Timeliness of notification. 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 discovery of a breach. (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 disclosed during the breach. (2) A business associate shall provide the covered entity with any other available information that the covered entity is required to include in 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.			
2.01	Documented incident response policies and procedures define roles, responsibilities, and required activities for analyzing, responding to, communicating, and recovering from security incidents.	Inspected the Incident Response Policy to determine that documented incident response policies and procedures defined roles, responsibilities, and required activities for analyzing, responding to, communicating, and recovering from security incidents.	No exceptions noted.
2.02	Management reviews the company's incident response and escalation procedures annually for effectiveness.	Inspected the most recent annual information security meeting minutes, calendar invite, and meeting transcript to determine that management reviewed the company's incident response and escalation procedures during the review period for effectiveness	No exceptions noted.
2.03	Incidents are documented and tracked in a standardized ticketing system and updated to reflect the planned incident and problem resolution.	Nonoccurrence: Refer to the test results for control activity CC7.3.2.	
2.04	Security incidents resulting in the unauthorized use or disclosure of personal information are communicated to the affected users.	Nonoccurrence: Refer to the test results for control activity CC7.3.2.	

#	Description of Service Organization's Controls	Service Auditor's Tests of Controls	Test Results
Law Enforcement Delay			
§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.			
2.05	Documented incident response policies and procedures define roles, responsibilities, and required activities for analyzing, responding to, communicating, and recovering from security incidents. This includes procedures for considering applicable laws, regulations or statutory requirements that may impact the resolution of an incident.	Inspected the Incident Response Policy to determine that documented incident response policies and procedures defined roles, responsibilities, and required activities for analyzing, responding to, communicating, and recovering from security incidents, and included procedures for considering applicable laws, regulations or statutory requirements that may impact the resolution of an incident.	No exceptions noted.
2.06	Management reviews the company's incident response and escalation procedures annually for effectiveness.	Inspected the most recent annual information security meeting minutes, calendar invite, and meeting transcript to determine that management reviewed the company's incident response and escalation procedures during the review period for effectiveness	No exceptions noted.
2.07	Incidents are documented and tracked in a standardized ticketing system and updated to reflect the planned incident and problem resolution.	Nonoccurrence: Refer to the test results for control activity CC7.3.2.	
2.08	Security incidents resulting in the unauthorized use or disclosure of personal information are communicated to the affected users.	Nonoccurrence: Refer to the test results for control activity CC7.3.2.	
Administrative Requirements and Burden of Proof			
§164.414(a): **Administrative requirements**. A covered entity is required to comply with the administrative requirements of §164.530 (b), (e), (g), (h), (i), and (j) with respect to the requirements of this subpart.			
	Not Applicable – Profisee is not a covered entity.		
§164.414(b): **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 the subpart or that the use or disclosure did not constitute a breach as defined at §164.402.			
2.09	Documented incident response policies and procedures define roles, responsibilities, and required activities for analyzing, responding to, communicating, and recovering from security incidents.	Inspected the Incident Response Policy to determine that documented incident response policies and procedures defined roles, responsibilities, and required activities for analyzing, responding to, communicating, and recovering from security incidents.	No exceptions noted.

#	Description of Service Organization's Controls	Service Auditor's Tests of Controls	Test Results
2.10	Management reviews the company's incident response and escalation procedures annually for effectiveness.	Inspected the most recent annual information security meeting minutes, calendar invite, and meeting transcript to determine that management reviewed the company's incident response and escalation procedures during the review period for effectiveness	No exceptions noted.
2.11	Incidents are documented and tracked in a standardized ticketing system and updated to reflect the planned incident and problem resolution.	Nonoccurrence: Refer to the test results for control activity CC7.3.2.	
2.12	Security incidents resulting in the unauthorized use or disclosure of personal information are communicated to the affected users.	Nonoccurrence: Refer to the test results for control activity CC7.3.2.	
2.13	A security incident analysis is performed for security incidents to determine the root cause and system impact.	Nonoccurrence: Refer to the test results for control activity CC7.3.2.	

SECTION 5

ADDITIONAL INFORMATION PROVIDED BY MANAGEMENT

MANAGEMENT'S RESPONSES TO EXCEPTIONS NOTED

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC9.2.2	Management obtains and reviews compliance reports for vendors on an annual basis to evaluate the effectiveness of controls within the vendors environments.	Inspected the vendor management review documentation for a sample of current vendors to determine that management obtained and reviewed compliance reports during the review period to evaluate the effectiveness of controls within the vendors environments for each vendor sampled.	The test of the control activity disclosed that management did not obtain and review compliance reports during the review period for one of three vendors sampled.
Management's Response:	Profisee has implemented new processes to retain vendor documentation to prevent this result from reoccurring.		