A-LIGN

ContractPod Technologies Ltd

Type 1 Attestation
(AT-C 105, AT-C 205 and AT-C 315)
HIPAA/HITECH

2023

ContractPodAi

Table of Contents

SECTION 1

ASSERTION OF CONTRACTPOD TECHNOLOGIES LTD MANAGEMENT

ASSERTION OF CONTRACTPOD TECHNOLOGIES LTD MANAGEMENT

November 7, 2023

We have prepared the description of ContractPod Technologies Ltd's ('ContractPodAi' or 'the Company') health information security program for the AI Based Company Services System (the "description") for user entities of the system as of September 30, 2023. We confirm, to the best of our knowledge and belief, that:

a. Management's description fairly presents the health information security program for the AI Based Company Services System as of September 30, 2023. The criteria we used in making this assertion were that the description:
   i. fairly presents how the health information security program was designed and implemented to govern the security policies and practices supporting the AI Based Company Services System
   ii. describes the specified controls within the security program designed to achieve the security program's objectives
   iii. does not omit or distort information relevant to the health information security program for the AI Based Company Services System and may not include every aspect that an individual user entity may consider important in its own particular environment

b. The health information security program governing the AI Based Company Services System complied with applicable requirements of HIPAA and HITECH. The criteria we used in making this assertion were that:
   i. management determined the applicable controls (the "controls") included in the health information security program
   ii. the controls documented complied with the standard and implementation guidance for safeguards as defined by the HIPAA Security Rule including the following:
      - Administrative Safeguards
      - Physical Safeguards
      - Technical Safeguards
      - Organizational Requirements
      - Breach Notification
   iii. the controls stated in the description were suitably designed and implemented as of September 30, 2023, to provide reasonable assurance that the applicable HIPAA and HITECH requirements would be met, if its controls operated effectively as of that date and if the user entities applied the complementary controls assumed in the design of ContractPodAi's controls as of that date.

Section 3 of this report includes ContractPodAi's description of the health information security program for the AI Based Company Services System that is covered by this assertion.

Anurag Malik

Anurag Malik
Chief Technology Officer
ContractPod Technologies Ltd

SECTION 2

INDEPENDENT SERVICE AUDITOR'S REPORT

INDEPENDENT SERVICE AUDITOR'S REPORT

To ContractPod Technologies Ltd:

We have examined ContractPodAi description of its health information security program for the ContractPodAi's AI Based Company Services System listed in Section 3 (the "description"), and its health information security program governing the AI Based Company Services System's compliance with applicable requirements of the Health Insurance Portability and Accountability Act Security Rule of 2003 ("HIPAA") and the Health Information Technology for Economic and Clinical Health Act ("HITECH"), enacted as part of the American Recovery and Reinvestment Act of 2009 ("HIPAA/HITECH requirements"). ContractPodAi's management is responsible for its assertion. Our responsibility is to express an opinion about ContractPodAi's compliance with the specified requirements based on our examination.

ContractPodAi uses Microsoft Azure ('Azure' or 'subservice organization') for cloud hosting services. The description indicates that certain applicable HIPAA/HITECH requirements can only be met if controls at the subservice organization are suitably designed. The description presents ContractPodAi's system; its controls relevant to the applicable HIPAA/HITECH requirements; and the types of controls that the service organization expect to be implemented, and suitably designed at the subservice organization to meet certain applicable HIPAA/HITECH requirements. The description does not include any of the controls implemented at the subservice organization. Our examination did not extend to the services provided by the subservice organization.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants and, accordingly, included examining, on a test basis, evidence supporting the fairness of the presentation of the description and the design of ContractPodAi's health information security program for the AI Based Company Services System and performing such other procedures as we considered necessary in the circumstances. Those standards require that we plan and perform the examination to obtain reasonable assurance about whether management's assertion about compliance with the specified requirements is fairly stated, in all material respects. An examination involves performing procedures to obtain evidence about whether management's assertion is fairly stated, in all material respects. The nature, timing, and extent of the procedures selected depend on our judgment, including an assessment of the risks of material misstatement of management's assertion, whether due to fraud or error. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Our examination does not provide a legal determination on ContractPodAi compliance with the specified requirements.

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

A-LIGN ASSURANCE did not perform procedures regarding the operating effectiveness of the controls stated in the description and, accordingly, do not express an opinion thereon. Because of their nature, controls at a service organization may not prevent, or detect and correct, all errors or omissions relevant to meet the applicable HIPAA/HITECH requirements. Also, the projection to the future of any evaluation of the fairness of the presentation of the description or conclusions about the suitability of the design or operating effectiveness of the controls to meet the applicable HIPAA/HITECH requirements is subject to the risks that the system may change or that controls at a service organization may become inadequate or fail.

In our opinion, in all material respects, based on the criteria described in ContractPodAi's assertion in Section 1:

a. The description fairly presents the health information security program for the AI Based Company Services System that was designed and implemented as of September 30, 2023;

b. The health information security program governing the AI Based Company Services System complied with applicable requirements of HIPAA and HITECH; and
c. the controls stated in ContractPodAi's description were suitably designed and implemented as of September 30, 2023, to provide reasonable assurance that the applicable HIPAA and HITECH requirements would be met, if its controls operated effectively as of that date and if the subservice organizations and user entities applied the complementary controls assumed in the design of ContractPodAi's controls as of that date.

This report is intended solely for the information and use of ContractPodAi; user entities of ContractPodAi's AI Based Company Services System as of September 30, 2023; and prospective user entities, independent auditors and practitioners providing services to such user entities, 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, subservice organizations, or other parties
- Internal control and its limitations
- Complementary user-entity controls and complementary subservice organization controls and how they interact with related controls at the service organization to meet the HIPAA/HITECH requirements
- The HIPAA/HITECH requirements
- The risks that may threaten the achievement of the HIPAA/HITECH requirements and how controls address those risks

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

A-LIGN ASSURANCE

Tampa, Florida
November 7, 2023

SECTION 3

CONTRACTPOD TECHNOLOGIES LTD'S DESCRIPTION OF ITS AI BASED COMPANY SERVICES SYSTEM AS OF SEPTEMBER 30, 2023

OVERVIEW OF OPERATIONS

Company Background

ContractPodAi was founded in 2012 with the mission to make the end-to-end contract management system more accessible to corporate in-house legal teams and with the aim of eliminating data entry and paralegal related work for the corporate department.

Laying original claim to the phrase ‘by lawyers for lawyers,’ the platform was created as an affordable, out of the box, end-to-end tool. It features repository, contract generation, and third-party review functionality. Since going live in 2015, the platform has been helping legal departments at large-scale corporations across the globe digitally transform their contract management function.

Description of Services Provided

ContractPodAi provides complete functionality covering the full spectrum of contract management, from creation through to signature and lifecycle management.

This functionality includes:

- Front door requests to the legal team
- Storage in a highly searchable central repository with Optical Character Recognition (OCR) capability
- Detailed reporting and analytics
- Contract creation and assembly
- Access to Leah, an artificially intelligent contract analyst
- E-signature by DocuSign
- Automated workflows and approval process management
- Robust alerts and reminders for key dates and tracking obligations

ContractPodAi provides access to Leah, an artificially intelligent contract analyst. Built on technologies including OpenAI, Zuva AI, International Business Machines (IBM) Watson, and other proprietary AIs, Leah will permanently transform contract creation and automation by reviewing, interpreting and analyzing contracts for key dates and an extensive set of standard key obligations. This information is automatically populated into the contract record, providing substantial savings in manual data entry, as well as the time taken to review contracts.

Electronic Protected Health Information (ePHI) Transmission, Processing & Reporting

ContractPodAi has no internal or external parties who have access to, or process ePHI on ContractPodAi’s behalf. ContractPodAi does not have access to, nor visibility of processed and stored client information. Further, ContractPodAi does not produce or process ePHI of its own in any way.

Principal Service Commitments and System Requirements

ContractPodAi designs its processes and procedures related to its AI Based Contract Management Solutions Services system to meet its objectives for its contract management services. Those objectives are based on the service commitments that ContractPodAi makes to user entities, the laws and regulations that govern the provision of contract management services, and the operational and compliance requirements that ContractPodAi has established for the services. The contract management services of ContractPodAi are subject to regulations, as well as privacy and security laws and regulations in the jurisdictions in which ContractPodAi operates.

Security commitments to user entities are documented and communicated in agreements, as well as in the description of the service offering provided online. Security commitments are standardized and include, but are not limited to, the following:

Security principles within the fundamental designs of the AI Based Contract Management Solutions Services system that are designed to permit users to access the information they need based on their role in the system while restricting them from accessing information not needed for their role.

Use of encryption technologies to protect customer data both at rest and in transit.

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

Components of the System

Infrastructure

Primary infrastructure used to provide ContractPodAi's AI Based Contract Management Solutions Services System includes the following:

Primary Infrastructure		
Hardware	**Type**	**Purpose**
Servers and Infrastructure	Azure	Application hosting and processing
Intrusion Prevention System (IPS)	Azure Intrusion Prevention Threat Scanning	Screens and alerts on network traffic based on "malicious IP addresses and domains" as assessed by feeds from the Microsoft Threat Intelligence service
Firewalls	Windows Firewall Advanced Security	Filters inbound and outbound traffic out of the network
SIEM	Microsoft Sentinel	For monitoring purposes
VPN	Azure VPN	VPN services
SQL Server	Windows	Database

Software

Primary software used to provide ContractPodAi's AI Based Contract Management Solutions Services System includes the following:

Primary Software	
Software	**Purpose**
ContractPodAi®	In-scope application for contract management

Primary Software	
Software	**Purpose**
Microsoft Office 365	Office Productivity
Visual Studio 2019	Development Studio
DocuSign	E-Signature
Azure Cognitive Search	Fluid Search Engine
Aspose PDF	Document Convertor
Aspose Word	Document Convertor
Aspose for DotNet	Document Convertor
Microsoft.NET	Development Framework
C#	Development Language
IBM Watson Ai	Artificial Intelligence
Zuva Ai	Artificial Intelligence
ABBy Fine Reader	OCR Platform Services
Sentry.io	System & Error Logging and View
SharePoint	Document Repository

People

ContractPodAi is organized in the following functional areas:

Senior management staff have overall functional responsibility for commercial, technical, and operational aspects of the business globally. The technical arm is managed out of the Mumbai office.

Finance and Human Resources (HR)/Admin are responsible for the accounts, accounts payable and receivable, and management accounting on a global basis. The team of HR professionals are in three offices, performing HR management, talent acquisition, and payroll/admin functions.

Technology and Development Operations are based largely out of the Mumbai office and involved in platform enhancement, customization, and bug support.

Marketing runs as a global function from the Toronto office and is focused primarily on communications, content, demand, and events.

Sales is globally managed from the NYC and London offices. Both teams consist of leadership, account executives, sales development representatives, and sales engineers.

Transformation is based largely out of London and services the globe. The team consists of implementation managers that run customer implementations from end to end, liaising with the Technology team in Mumbai where necessary. Their entry point on each client project takes place via a handover from the Sales Engineer, at which point the agreement is defined before the point of contract signature. They then own and run the agreement, which defines each client's configuration of the software, and are responsible for client delivery and onboarding.

The Transformation team also features a team of legal engineers, who test and refine the AI review capabilities of the software, feeding back to Technology as appropriate and liaising on the client side to optimize and improve machine learning efficiency on an ongoing basis.

The Customer Success team is based in the New York office and is a global function. The team takes over each customer just after go-live via a handover from the implementation manager. It is their responsibility to act as a single point of contact for the customer on their user journey with the software, with a responsibility to retain and renew the license as appropriate.

Data

- Transaction data: comes from the creation of contracts in the system. This includes metadata of the contracts and the contract file
- Output reports: Reports that are generated from the system for/by the end users of the system
- Audit Trails: Generated by the Contract Lifecycle Management (CLM) solution for user and system actions
- System files/Code Files: Published code files for the ContractPodAi SaaS solutions
- Error logs: Generated by ContractPodAi SaaS product and Windows OS and infrastructure

Health Information Security Program Processes, Policies and Procedures

ContractPodAi has developed a health information security management program to meet the information security and compliance requirements related to AI-Based Contract Management Solutions services and its customer base. The program incorporates the elements of the HIPAA and the HITECH. The description below is a summary of safeguards that ContractPodAi has implemented to adhere to the applicable components of HIPAA Final Security Rule and the breach notification requirements of HITECH.

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

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

Physical Safeguards - Controlling physical access to protected data:

- Documented physical security policies and procedures are in place to guide personnel in physical security administration.
- Physical access procedures are in place to restrict access, log visitors, and terminate access to the office facility.
- Inventory listings are utilized to track and monitor hardware and removable media.
- Data destruction procedures are in place to guide the secure disposal of data and media.

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

- Access to in-scope systems is restricted to authorized personnel based on a valid user account and password.
- Systems are configured to enforce pre-determined thresholds to lock user sessions due to invalid login attempts.

- Security monitoring applications and manual reviews are utilized to monitor and analyze the in-scope systems for possible or actual security breaches.

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

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

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

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

Boundaries of the System

The scope of this report includes the AI Based Contract Management Solutions Services System performed in the Mumbai, India; London, United Kingdom; New York City, New York; and Glasgow, Scotland facilities.

This report does not include the cloud hosting services provided by Azure at multiple facilities.

HIPAA/HITECH REQUIREMENTS AND RELATED CONTROLS

Organizational Structure and Assignment of Authority and Responsibility

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

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

Risk Assessment Process

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

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

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

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

Integration with Risk Assessment

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

Periodic Assessments

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

- *Risk Assessment*: The risk assessment is performed by the risk management personnel. Risk factors associated with the delivery or implementation of services to customers are evaluated considering process owners, dependencies, timelines and quality.
- Health Information Security Risks: Health information security risks are assessed by the CEO and President/CTO. Risk factors associated with the organization are evaluated considering compliance obligations, laws and regulations, policies and procedures, contracts and best practices to which the organization has committed to. Information security assessments carried out by risk management personnel are rolled up to the CEO and President/CTO of the organization.

Periodic Testing and Evaluation

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

- Internal risk assessments
- Corrective action plans
- Management reviews

Information and Communications Systems

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

Various weekly calls are held to discuss operational efficiencies within the applicable functional areas and to disseminate new policies, procedures, controls, and other strategic initiatives within the organization. Additionally, annual meetings are held to provide staff with updates on the firm and key issues affecting the organization and its employees. Senior executives lead the meetings with information gathered from formal automated information systems and informal databases, as well as conversations with various internal and external colleagues. General updates to entity-wide security policies and procedures are usually communicated to the appropriate ContractPodAi personnel via email messages.

Specific information systems used to support ContractPodAi's AI Based Contract Management Solutions Services system are described in the Description of Services section above.

Monitoring Controls

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

On-Going Monitoring

ContractPodAi's management conducts quality assurance monitoring on a regular basis and additional training is provided based upon results of monitoring procedures. This process is accomplished through ongoing monitoring activities, separate evaluations, or a combination of the two.

ContractPodAi has an internal controls matrix for defining different monitoring and audit frequencies. The internal controls matrix ensures the effectiveness of the controls and monitoring of the process flow on a regular basis. The internal controls matrix includes access, security, employee and asset management, quality assurance, and risk assessment related control reviews. A report on these controls is provided to management to inform them of any kind of discrepancy in the processes or potential risk.

Reporting Deficiencies

An internal tracking tool is utilized to document and track the results of on-going monitoring procedures. Escalation procedures are maintained for responding and notifying management of any identified risks. Corrective actions, if necessary, are documented and tracked within the internal tracking tool.

Policies and Procedures

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

Security Awareness Training

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

Incident Response

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

Remediation and Continuous Improvement

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

Changes to the System in the Last 12 Months

No significant changes have occurred to the services provided to user entities in the 12 months preceding the review date.

Incidents in the Last 12 Months

No significant incidents have occurred to the services provided to user entities in the 12 months preceding the review date.

Requirements Not Applicable to the System

The following requirements are not applicable to the system:

Requirements Not Applicable to the System		
Safeguard	**Requirement**	**Reason**
Administrative Safeguards	164.308(a)(4)(ii)(A)	The entity is not a health care clearinghouse.
	164.308(b)(1), 164.308(b)(2), 164.308(b)(3), 164.308(b)(4)	The colocation services provided by the entity does not include sharing information that would require any executed business associate agreements.
Physical Safeguards	164.310(c)	The entity is not a covered entity.
Organizational Safeguards	164.314(a)(1), 164.314(a)(2)(i)	The services provided by the entity does not include sharing information that would require any executed business associate agreements.
	164.314(a)(2)(ii)	The entity is not a government entity.
	164.314(b)(1), 164.314(b)(2)	The entity is not a plan sponsor.
Breach Notification	164.404(a)(1), 164.404(a)(2), 164.404(b), 164.404(c)(1), 164.404(c)(2), 164.404(d)(1)(i), 164.404(d)(1)(ii), 164.404(d)(2), 164.404(d)(2)(i), 164.404(d)(2)(ii), 164.404(d)(3), 164.406, 164.408(a), 164.408(b), 164.408(c)	The entity is a business associate. The entity's responsibilities for breach notification are limited to its' covered entity customers.

Subservice Organizations

This report does not include the cloud hosting services provided by Azure at multiple facilities.

Subservice Description of Services

Azure is a cloud computing service created by Microsoft for building, testing, deploying, and managing applications and services through Microsoft-managed data centers.

Complementary Subservice Organization Controls

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

The following subservice organization controls should be implemented by Azure to provide additional assurance that the safeguards described within this report are met:

Subservice Organization - Azure		
Safeguard	**Requirement**	**Control**
Physical Safeguards	164.310(a)(1), 164.310(a)(2)(ii), 164.310(a)(2)(iii), 164.310(a)(2)(iv), 164.310(d)(1), 164.310(d)(2)(iii)	Procedures have been established to restrict physical access to the datacenter to authorized employees, vendors, contractors, and visitors.
		Security verification and check-in are required for personnel requiring temporary access to the interior datacenter facility including tour groups or visitors.
		Physical access to the datacenter is reviewed quarterly and verified by the Datacenter Management team.
		Physical access mechanisms (e.g., access card readers, biometric devices, man traps / portals, cages, locked cabinets) have been implemented and are administered to restrict access to authorized individuals.
		The data center facility is monitored 24x7 by security personnel.

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

- Holding periodic discussions with the subservice organization
- Reviewing attestation reports over services provided by the subservice organization
- Monitoring external communications, such as customer complaints relevant to the services by the subservice organization

Complementary User Entity Controls

ContractPodAi's services are designed with the assumption that certain controls will be implemented by user entities. Such controls are called complementary user entity controls. It is not feasible for all of the Safeguards related to ContractPodAi's services to be solely achieved by ContractPodAi control procedures. Accordingly, user entities, in conjunction with the services, should establish their own internal controls or procedures to complement those of ContractPodAi's.

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

1. User entities are responsible for reviewing data input and output from the system for completeness and accuracy.
2. User entities are responsible for developing their own disaster recovery and business continuity plans that address the inability to access or utilize ContractPodAi services.
3. User entities are responsible for ensuring the supervision, management, and control of the use of ContractPodAi services by their personnel.
4. User entities are responsible for user access administration, including periodically reviewing access rights for users with access to their production instance of the application.
5. User entities are responsible for immediately notifying ContractPodAi of any actual or suspected information security breaches, including compromised user accounts, including those used for integrations and secure file transfers.
6. User entities are responsible for protecting data sent to ContractPodAi by appropriate methods to ensure confidentiality, integrity, and non-repudiation.
7. User entities are responsible for developing their own disaster recovery and business continuity plans that address the inability to access or utilize ContractPodAi services.

CONTROL ACTIVITIES SPECIFIED BY THE SERVICE ORGANIZATION

ADMINISTRATIVE SAFEGUARDS		
Ref	**Regulation**	**Control Activity Specified by the Service Organization**
164.308 (a)(1)(i)	**Security management process:** Implement policies and procedures to prevent, detect, contain and correct security violations.	Documented incident response and escalation procedures are in place to guide personnel in addressing the threats posed by security incidents. Documented incident response and escalation procedures for reporting security incidents are in place to guide users in identifying, reporting, and mitigating failures, incidents, concerns, and other complaints. Policies and procedures are in place regarding detection, logging, and monitoring of unknown or unauthorized components into the environment. Monitoring software is used to identify and evaluate ongoing system performance, capacity, security threats, changing resource utilization needs and unusual system activity. The monitoring software is configured to alert IT personnel when thresholds have been exceeded. An IPS is utilized to analyze network events and report possible or actual network security breaches. The IPS is configured to notify personnel upon intrusion prevention. FIM software is in place to ensure only authorized changes are deployed into the production environment. The FIM software is configured to notify IT personnel via email alert when a change to the production application code files is detected. A firewall is in place to filter unauthorized inbound network traffic from the Internet. The firewall system is configured to deny any type of network connection that is not explicitly authorized by a firewall system rule. Antivirus software is installed on workstations to detect and prevent the transmission of data or files that contain certain virus signatures recognized by the antivirus software. Internal vulnerability scans are performed on a monthly basis and external vulnerability scans are performed on a monthly basis on the environment to identify control gaps and vulnerabilities.

ADMINISTRATIVE SAFEGUARDS		
Ref	**Regulation**	**Control Activity Specified by the Service Organization**
164.308 (a)(1)(ii)(A)	**Risk analysis:** an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information (ePHI).	A formal risk assessment is performed on at least an annual basis to identify threats that could impair systems vulnerability, security, confidentiality, integrity, and availability of ePHI.
164.308 (a)(1)(ii)(B)	**Risk management:** Ensures the company implements security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with §164.306. Factors identified in §164.306 include: • The size, complexity, capability of the covered entity • The covered entity's technical infrastructure • The costs of security measures • The probability and criticality of potential risks to ePHI	Management develops risk mitigation strategies to address risks identified during the risk assessment process. Internal vulnerability scans are performed on a monthly basis and external vulnerability scans are performed on a monthly basis on the environment to identify control gaps and vulnerabilities.
164.308 (a)(1)(ii)(C)	**Sanction policy:** Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity or business associate.	Sanction policies, which include probation, suspension and termination, are in place for employee misconduct.
	Network (Azure AD)	
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.	Azure AD audit logging settings are in place that include: • Logon events • System events Azure AD audit logs are maintained and reviewed as needed.
	Database (SQL) Azure Managed Sequel	
		Database audit logging settings are in place that include failed logon events. Database audit logs are maintained and reviewed as needed.
	Application (ContractPodAi)	
		Application audit policy settings are in place that include: • Request ID • User ID • Contract ID • Action taken Application audit logs are maintained and reviewed as needed. Resolution of incidents are documented within the ticket and communicated to affected users. Incidents are documented and tracked in a standardized ticketing system and updated to reflect the planned incident and problem resolution.

ADMINISTRATIVE SAFEGUARDS		
Ref	**Regulation**	**Control Activity Specified by the Service Organization**
164.308 (a)(2)	**Assigned security responsibility:** Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the entity.	Responsibility for the development, implementation, and regular maintenance of the policies and procedures that govern the security of protected ePHI is assigned to the Chief Technology Officer (CTO) and General Counsel.
164.308 (a)(3)(i)	**Workforce security:** Policies and procedures are implemented to ensure that all members of the workforce have appropriate access to ePHI, as provided under the Information Access Management standard and to prevent those who do not have appropriate access from obtaining access to ePHI. Policies and procedures should include Authorization and/or Supervision procedures, Workforce Clearance Procedure, and Termination Procedures.	Documented policies and procedures are in place regarding system settings, authentication, access, and security monitoring. Logical access privileges are reviewed on an annual by authorized personnel to help ensure the appropriateness of access credentials and that least privileges required to perform job functions are assigned to user accounts. Logical access to systems is approved and granted to an employee as a component of the hiring process. Logical access to systems is revoked as a component of the termination process.
	Network (Azure Active Directory)	
		Azure AD user access is restricted via role-based security privileges defined within the access control system. Azure AD administrative access is restricted to the following authorized personnel: • Director of Technology • Director of Information Security • Manager of Technology • Infra Support
	Operating System (Windows)	
		Operating system user access is restricted via role-based security privileges defined within the access control system. Operating system administrative access is restricted to the following authorized personnel: • Director of Technology • Senior Director of Technology • Manager of Technology • Senior System Administrator • Senior DevOps Engineer • Infra Support

ADMINISTRATIVE SAFEGUARDS		
Ref	**Regulation**	**Control Activity Specified by the Service Organization**
	Database (SQL) Azure Managed Sequel	
		Database user access is restricted via role-based security privileges defined within the access control system: • Senior Director of Technology • Manager of Technology • DevOps Engineer • Lead DevOps Engineer • Manager of Technology Database administrative access is restricted to the following personnel: • Director of Technology • Senior Director of Technology • Manager of Technology • Senior System Administrator • Senior DevOps Engineer • Infra Support
	Application (ContractPodAi)	
		Application user access is restricted via role-based security privileges defined within the access control system. Application administrative access is appropriately restricted to authorized personnel. Multi-factor authentication (MFA) is required for all users to access the network. An IPS is utilized to analyze network events and report possible or actual network security breaches. The IPS is configured to notify personnel upon intrusion prevention. Azure AD is configured to enforce password requirements that include: • Password history • Password maximum age • Password length • Complexity Application user access is restricted via role-based security privileges defined within the access control system. The entity secures its environment a using multi-layered defense approach that includes firewalls, IPS, antivirus software and a DMZ. VPN and TLS are used for defined points of connectivity. Server certificate-based authentication is used as part of the TLS encryption with a trusted certificate authority.

ADMINISTRATIVE SAFEGUARDS		
Ref	**Regulation**	**Control Activity Specified by the Service Organization**
		Critical data is stored in encrypted format using software supporting the Azure SSE and 256-bit AES. Encryption keys are protected during generation, storage, use, and destruction. Logical access privileges are reviewed on an annual by authorized personnel to help ensure the appropriateness of access credentials and that least privileges required to perform job functions are assigned to user accounts. Backup restoration tests are performed on an annual basis.
164.308 (a)(3)(ii)(A)	**Authorization and/or supervision:** Ensures the authorization and/or supervision of workforce members who work with ePHI or in locations where it might be accessed.	Documented policies and procedures are in place regarding system settings, authentication, access, and security monitoring. Logical access privileges are reviewed on an annual by authorized personnel to help ensure the appropriateness of access credentials and that least privileges required to perform job functions are assigned to user accounts. Logical access to systems is approved and granted to an employee as a component of the hiring process. Logical access to systems is revoked as a component of the termination process.
164.308 (a)(3)(ii)(B)	**Workforce clearance procedure:** Access of a workforce member (employee or computing device) to ePHI is appropriate.	Access control and role-based build procedures are in place to restrict access to systems that maintain ePHI to only authorized personnel. Logical access privileges are reviewed on an annual by authorized personnel to help ensure the appropriateness of access credentials and that least privileges required to perform job functions are assigned to user accounts. Logical access to systems is approved and granted to an employee as a component of the hiring process. Logical access to systems is revoked as a component of the termination process.
164.308 (a)(3)(ii)(C)	**Termination procedures:** Ensure that access to ePHI is terminated as soon as possible when a workforce member's employment ends.	Documented policies and procedures are in place regarding system settings, authentication, access, and security monitoring. Logical access to systems is revoked as a component of the termination process.

ADMINISTRATIVE SAFEGUARDS		
Ref	**Regulation**	**Control Activity Specified by the Service Organization**
164.308 (a)(4)(i)	**Information access management:** Policies and procedures are implemented that ensure authorizing access to ePHI and are consistent with the applicable requirements of the Privacy Rule. Policies and procedures should include: Isolating Health Care Clearinghouse Functions, Access Authorization and Access Establishment and Modification.	Management maintains policies and procedures that ensure the authorization of access to ePHI and are consistent with the applicable requirements of the Privacy Rule.
164.308 (a)(4)(ii)(A)	**Isolating healthcare clearinghouse functions:** If a health care clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the ePHI of the clearinghouse from unauthorized access by the larger organization.	Not applicable. The entity is not a healthcare clearinghouse.
164.308 (a)(4)(ii)(B)	**Access authorization:** Implement policies and procedures for granting access to ePHI, for example, through access to a workstation, transaction, program, process, or other mechanism.	Access control and role-based build procedures are in place to restrict access to systems that maintain ePHI to only authorized personnel. Logical access to systems is approved and granted to an employee as a component of the hiring process.
164.308 (a)(4)(ii)(C)	**Access establishment and modification:** Implement policies and procedures that, based upon the covered entity's or the business associate's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process.	Access control and role-based build procedures are in place to restrict access to systems that maintain ePHI to only authorized personnel. Logical access to systems is approved and granted to an employee as a component of the hiring process. Logical access to systems is revoked as a component of the termination process. Logical access privileges are reviewed on an annual by authorized personnel to help ensure the appropriateness of access credentials and that least privileges required to perform job functions are assigned to user accounts.
164.308 (a)(5)(i)	**Security awareness and training:** Implement a security awareness and training program for all members of the workforce (including management). Component of the Security Awareness and Training program should include Security Reminders, Protection Malicious Software, Log-in Monitoring and Password Management.	Management conducts security awareness training to establish the organization's commitments and requirements for employees. Policies and procedures are in place that outline the performance evaluation process as well as the competency and training requirements for personnel. Upon hire, employees are required to complete information security and awareness training. Upon hire, personnel are required to acknowledge the employee handbook and code of conduct.

ADMINISTRATIVE SAFEGUARDS		
Ref	**Regulation**	**Control Activity Specified by the Service Organization**
		Current employees are required to complete information security and awareness training on an annual basis.
164.308 (a)(5)(ii)(A)	**Security reminders:** Periodic security updates.	Users are made aware of security updates and updates to security policies via survey forms and email notifications.
164.308 (a)(5)(ii)(B)	**Protection from malicious software:** Procedures for guarding against, detecting, and reporting malicious software.	A program of techniques, technologies, and methods to guard against, detect, and report the presence of malicious software is in place. Antivirus software is installed on workstations to detect and prevent the transmission of data or files that contain certain virus signatures recognized by the antivirus software. Monitoring software is in place to monitor and log metrics from resources, applications, performance, resource utilization, and other infrastructure components. Alerts are sent to personnel when certain alarms are triggered. The IPS is configured to notify personnel upon intrusion prevention.
164.308 (a)(5)(ii)(C)	**Log-in monitoring:** Procedures for monitoring log-in attempts and reporting discrepancies.	Regular monitoring and review of log-ins and log-in attempts to the system is in place. Discrepancies and potentially inappropriate or illegal activities are reported to senior management, legal counsel and/or human resources, as appropriate.
	Network (Azure Active Directory)	
		Azure AD audit logging settings are in place that include: • Logon events • System events Azure AD audit logs are maintained and reviewed as needed.
	Database (SQL) Azure Managed Sequel	
		Database audit logging settings are in place that include failed logon events. Database audit logs are maintained and reviewed as needed.
	Application (ContractPodAi)	
		Application audit policy settings are in place that include: • Request ID • User ID • Contract ID • Action taken Application audit logs are maintained and reviewed as needed.

ADMINISTRATIVE SAFEGUARDS		
Ref	**Regulation**	**Control Activity Specified by the Service Organization**
		Resolution of incidents are documented within the ticket and communicated to affected users. Incidents are documented and tracked in a standardized ticketing system and updated to reflect the planned incident and problem resolution.
164.308 (a)(5)(ii)(D)	**Password management:** Procedures for creating, changing, and safeguarding passwords.	Policies are in place to guide personnel in creating, changing, and safeguarding passwords for network devices and servers.
	Network (Azure AD)	
		Azure AD is configured to enforce password requirements that include: • Password history • Password maximum age • Password length • Complexity
	Database (SQL) Azure Managed Sequel	
		Databases are configured to enforce password requirements that include: • Password history • Password maximum age • Password length • Complexity
	Application (ContractPodAi)	
164.308 (a)(6)(i)	**Security incident procedures:** Implement policies and procedures to address security incidents. Policies and procedures should include response reporting.	The application is configured to enforce password requirements that include: • Password history • Password length • Complexity MFA is required for all users to access the network. An IPS is utilized to analyze network events and report possible or actual network security breaches. The IPS is configured to notify personnel upon intrusion prevention. Documented incident response and escalation procedures for reporting security incidents are in place to guide users in identifying, reporting and mitigating failures, incidents, concerns, and other complaints. The incident response and escalation procedures are reviewed at least annually for effectiveness. The incident response policies and procedures define the classification of incidents based on its severity.

ADMINISTRATIVE SAFEGUARDS		
Ref	**Regulation**	**Control Activity Specified by the Service Organization**
164.308 (a)(6)(ii)	**Response and reporting:** Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity or business associate; and document security incidents and their outcomes.	Resolution of incidents are documented within the ticket and communicated to affected users. Incidents are documented and tracked in a standardized ticketing system and updated to reflect the planned incident and problem resolution. Identified incidents are reviewed, monitored, and investigated by an incident response team. Documented incident response and escalation procedures for reporting security incidents are in place to guide users in identifying, reporting, and mitigating failures, incidents, concerns, and other complaints. The incident response and escalation procedures are reviewed at least annually for effectiveness. The incident response policies and procedures define the classification of incidents based on its severity. Resolution of incidents are documented within the ticket and communicated to affected users. Incidents are documented and tracked in a standardized ticketing system and updated to reflect the planned incident and problem resolution. Identified incidents are reviewed, monitored, and investigated by an incident response team.
164.308 (a)(7)(i)	**Contingency plan:** Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain ePHI.	Business continuity and disaster recovery plans are developed and updated on an annual basis. The business continuity plan and disaster recovery procedure are tested on an annual basis. A business continuity plan is documented and in place that outlines the range of disaster scenarios and steps the business will take in a disaster to ensure the timely resumption of critical business operations. The business continuity plan is tested on an annual basis and includes: • Various testing scenarios based on threat likelihood • Identifying the critical systems required for business operations • Assigning roles and responsibilities in the event of a disaster • Assessing and mitigating risks identified as a result of the test disaster

ADMINISTRATIVE SAFEGUARDS		
Ref	**Regulation**	**Control Activity Specified by the Service Organization**
164.308 (a)(7)(ii)(A)	**Data backup plan:** Establish and implement procedures to create and maintain retrievable exact copies of ePHI.	Procedures are in place to provide for complete, accurate, and timely storage of data. Full backups of certain application and database components are performed on a daily basis and incremental backups are performed every four hours.
164.308 (a)(7)(ii)(B)	**Disaster recovery plan:** Establish (and implement as needed) procedures to restore any loss of data.	The business continuity plan and disaster recovery procedures are developed and updated on an annual basis. The business continuity plan and disaster recovery procedures are tested on an annual basis. The disaster recovery plan includes moving the business operations and supporting systems to a hot site. A business continuity plan is documented and in place that outlines the range of disaster scenarios and steps the business will take in a disaster to ensure the timely resumption of critical business operations. The business continuity plan is tested on an annual basis and includes: • Various testing scenarios based on threat likelihood • Identifying the critical systems required for business operations • Assigning roles and responsibilities in the event of a disaster • Assessing and mitigating risks identified as a result of the test disaster Backup restoration tests are performed on an annual basis.
164.308 (a)(7)(ii)(C)	**Emergency Mode Operation Plan:** Establish and implement procedures to enable continuation of critical business processes for protection of the security of ePHI while operating in emergency mode.	The business continuity plan and disaster recovery procedures are developed and updated on an annual basis. The business continuity plan and disaster recovery procedures are tested on an annual basis. The disaster recovery plan includes moving the business operations and supporting systems to a hot site. A business continuity plan is documented and in place that outlines the range of disaster scenarios and steps the business will take in a disaster to ensure the timely resumption of critical business operations.

ADMINISTRATIVE SAFEGUARDS		
Ref	**Regulation**	**Control Activity Specified by the Service Organization**
		The business continuity plan is tested on an annual basis and includes: • Various testing scenarios based on threat likelihood • Identifying the critical systems required for business operations • Assigning roles and responsibilities in the event of a disaster • Assessing and mitigating risks identified as a result of the test disaster Backup restoration tests are performed on an annual basis.
164.308 (a)(7)(ii)(D)	**Testing and revision procedures:** Implement procedures for periodic testing and revision of contingency plans.	The business continuity plan and disaster recovery procedures are developed and updated on an annual basis. The business continuity plan and disaster recovery procedures are tested on an annual basis. The business continuity plan is tested on an annual basis and includes: • Various testing scenarios based on threat likelihood • Identifying the critical systems required for business operations • Assigning roles and responsibilities in the event of a disaster • Assessing and mitigating risks identified as a result of the test disaster
164.308 (a)(7)(ii)(E)	**Applications and data criticality analysis:** Assess the relative criticality of specific applications and data in support of another contingency plan component.	The entity has defined what critical data is processed and how it is processed. Data and information critical to the system is assessed annually for relevance and use. For each critical system, the entity defines and documents what data and information are critical to support the system. The entity has defined the following components of the data critical to supporting the system: • A description of what the critical data is used for • Source of the data • How the data is stored and transmitted

ADMINISTRATIVE SAFEGUARDS		
Ref	**Regulation**	**Control Activity Specified by the Service Organization**
		The entity's risk assessment process includes: • Identifying the relevant information assets that are critical to business operations • Prioritizing the criticality of those relevant information assets • Identifying and assessing the impact of the threats to those information assets • Identifying and assessing the impact of the vulnerabilities associated with the identified threats • Assessing the likelihood of identified threats and vulnerabilities • Determining the risks associated with the information assets • Addressing the associated risks identified for each identified vulnerability
164.308 (a)(8)	**Evaluation:** Perform a periodic technical and nontechnical evaluation based initially upon the standards implemented under this rule and subsequently, in response to environmental or operations changes affecting the security of ePHI that establishes the extent to which an entity's security policies and procedures meet the requirement.	Changes to the regulatory, economic, and physical environment in which the entity operates are considered and evaluated as part of the annual comprehensive risk assessment. Changes to the business structure and operations are considered and evaluated as part of the annual comprehensive risk assessment. Changes in key management and personnel are considered and evaluated as part of the annual comprehensive risk assessment. Changes to the entity's systems, applications, technologies, and tools are considered and evaluated as part of the annual comprehensive risk assessment.
164.308 (b)(1)	**Business associate contracts and other arrangements:** A covered entity, in accordance with 164.306 [The Security Standards: General Rules], may permit a business associate to create, receive, maintain, or transmit ePHI on the covered entity's behalf only if the covered entity obtains satisfactory assurances, in accordance with 164.314 [the Organization Requirements] that the business associate will appropriately safeguard the information.	Not applicable. The services provided by the entity does not include sharing information that would require any executed business associate agreements.
164.308 (b)(2)	A business associate may permit a business that is a subcontractor to create, receive, maintain, or transmit ePHI on its behalf only if the business associate obtains satisfactory assurances, in accordance with §164.314(a), that the subcontractor will appropriately safeguard the information.	Not applicable. The services provided by the entity does not include sharing information that would require any executed business associate agreements.

ADMINISTRATIVE SAFEGUARDS		
Ref	**Regulation**	**Control Activity Specified by the Service Organization**
164.308 (b)(3)	**Written contract or other arrangement:** Document the satisfactory assurances required by paragraph (b)(1) [the Business Associates Contracts and Other Arrangements] of this section through a written or other arrangement with the business associate that meets the applicable requirements of 164.314(a) [the Organizational Requirements].	Not applicable. The services provided by the entity does not include sharing information that would require any executed business associate agreements.
164.308 (b)(4)	**Arrangement:** Document the satisfactory assurances required by paragraph (b)(1) [the Business Associates Contracts and Other Arrangements] of this section through a written or other arrangement with the business associate that meets the applicable requirements of 164.314(a).	Not applicable. The services provided by the entity does not include sharing information that would require any executed business associate agreements.

PHYSICAL SAFEGUARDS		
Ref	**Regulation**	**Control Activity Specified by the Service Organization**
164.310 (a)(1)	**Facility access controls:** Implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.	The controls relating to the regulation are the responsibility of the subservice organization and are monitored by the service organization. Refer to the 'Subservice Organizations' section above for additional details.
164.310 (a)(2)(i)	**Contingency operations:** Establish (and implement as needed) procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency.	The business continuity plan and disaster recovery procedures are developed and updated on an annual basis. The business continuity plan and disaster recovery procedures are tested on an annual basis. The business continuity plan is tested on an annual basis and includes: • Various testing scenarios based on threat likelihood • Identifying the critical systems required for business operations • Assigning roles and responsibilities in the event of a disaster • Assessing and mitigating risks identified as a result of the test disaster
164.310 (a)(2)(ii)	**Facility security plan:** Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.	The controls relating to the regulation are the responsibility of the subservice organization and are monitored by the service organization. Refer to the 'Subservice Organizations' section above for additional details.
164.310 (a)(2)(iii)	**Access control and validation procedures:** Implement procedures to control and validate a person's access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision.	The controls relating to the regulation are the responsibility of the subservice organization and are monitored by the service organization. Refer to the 'Subservice Organizations' section above for additional details.
164.310 (a)(2)(iv)	**Maintenance records:** Implement policies and procedures to document repairs and modifications to the physical components of a facility which are related to security (for example, hardware, walls, doors, and locks).	The controls relating to the regulation are the responsibility of the subservice organization and are monitored by the service organization. Refer to the 'Subservice Organizations' section above for additional details.
164.310 (b)	**Workstation use:** Implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access ePHI.	Procedures that specify the proper functions, processes, and appropriate environments of workstations that access ePHI are in place.
164.310 (c)	**Workstation security:** Covered entities should implement physical safeguards for all workstations that access ePHI, to restrict access to authorized users.	Not applicable. The entity is not a covered entity.

PHYSICAL SAFEGUARDS		
Ref	**Regulation**	**Control Activity Specified by the Service Organization**
164.310 (d)(1)	**Device and media control:** Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain ePHI into and out of a facility, and the movement of these items within the facility.	Removable media is disallowed by policy unless specifically authorized and reviewed by the Information Security team. Part of the controls relating to the regulation are the responsibility of the subservice organization and are monitored by the service organization. Refer to the 'Subservice Organizations' section above for additional details.
164.310 (d)(2)(i)	**Disposal:** Implement policies and procedures to address the final disposition of ePHI, and/or the hardware or electronic media on which it is stored.	Policies and procedures are in place to guide personnel in data, hardware and software disposal and destruction. The entity disposes of data in accordance with the retention periods and disposal procedures defined in the data disposal and destruction policy, legal and contractual obligations, and various statues. An inventory log is maintained of assets with confidential data, and as confidential data meets the retention period, the data is destroyed or purged. Use of removable media is prohibited by policy except when authorized by management.
164.310 (d)(2)(ii)	**Media re-use:** Implement procedures for removal of ePHI from electronic media before the media are made available for re-use. Ensure that ePHI previously stored on electronic media cannot be accessed and reused. Identify removable media and their use. Ensure that ePHI is removed from reusable media before they are used to record new information.	Documented data retention and disposal policy and procedures are in place that include the following: • Defining, identifying and designating information as confidential • Storing confidential information • Protecting confidential information from erasure or destruction • Retaining confidential information for only as long as is required to achieve the purpose for which the data was collected and processed The entity disposes of data in accordance with the retention periods and disposal procedures defined in the data disposal and destruction policy, legal and contractual obligations, and various statues. An inventory log is maintained of assets with confidential data, and as confidential data meets the retention period, the data is destroyed or purged.
164.310 (d)(2)(iii)	**Accountability:** Maintain a record of the movements of hardware and electronic media and any person responsible therefore.	An inventory log is maintained of assets with confidential data. Confidential information is maintained in locations restricted to those authorized to access.

PHYSICAL SAFEGUARDS		
Ref	**Regulation**	**Control Activity Specified by the Service Organization**
164.310 (d)(2)(iv)	**Data backup and storage:** Create a retrievable, exact copy of ePHI, when needed, before movement of equipment.	An inventory log is maintained of assets with confidential data, and as confidential data meets the retention period, the data is destroyed or purged. Use of removable media is prohibited by policy except when authorized by management. Part of the controls relating to the regulation are the responsibility of the subservice organization and are monitored by the service organization. Refer to the 'Subservice Organizations' section above for additional details. Procedures are in place to provide for complete, accurate, and timely storage of data. The ways in which critical data are backed up and stored are documented and reviewed annually. Data backup and restore procedures are in place to guide personnel in performing backup activities. Hourly, weekly, and monthly snapshots are configured for the databases. Backups are automatically disposed of after the retention period is met. When a backup job fails, the backup tool sends an alert to the backup administrators who investigate and resolve the failure. Logical access privileges are reviewed on an annual by authorized personnel to help ensure the appropriateness of access credentials and that least privileges required to perform job functions are assigned to user accounts. Backup restoration tests are performed on an annual basis, as part of the disaster recovery test.

TECHNICAL SAFEGUARDS		
Ref	**Regulation**	**Control Activity Specified by the Service Organization**
164.312 (a)(1)	**Access control:** Implement technical policies and procedures for electronic information systems that maintain ePHI to allow access only to those persons or software programs that have been granted access rights as specified in §164.308(a)(4).	Documented policies and procedures are in place regarding system settings, authentication, access, and security monitoring. Logical access to systems is approved and granted to an employee as a component of the hiring process. Logical access to systems is revoked as a component of the termination process.
164.312 (a)(2)(i)	**Unique user identification:** Assign a unique name and/or number for identifying and tracking user identity. Ensure that system activity can be traced to a specific user. Ensure that the necessary data is available in the system logs to support audit and other related business functions.	Documented policies and procedures are in place regarding system settings, authentication, access, and security monitoring.
	Network (Azure AD)	
		Azure AD user access is restricted via role-based security privileges defined within the access control system. Azure Ad administrative access is restricted to the following authorized personnel: • Senior Director of Technology • Director of Information Security • Manager of Technology • Infra Support Azure AD audit logging settings are in place that include: • Logon events • System events Azure AD audit logs are maintained and reviewed as needed.
	Operating System (Windows)	
		Operating system user access is restricted via role-based security privileges defined within the access control system. Operating system administrative access is restricted to the following authorized personnel • Solution Architect • Director of Technology • Manager of Technology • Developer • Sr. Developer • Security Engineer

TECHNICAL SAFEGUARDS		
Ref	**Regulation**	**Control Activity Specified by the Service Organization**
		Windows audit logging settings are in place that include: • Logon events • System events Windows audit logs are maintained and reviewed as needed.
	Database (SQL) Azure Managed Sequel	
		Database user access is restricted via role-based security privileges defined within the access control system. Database audit logging settings are in place that include failed logon events. Database audit logs are maintained and reviewed as needed.
	Application (ContractPodAi)	
164.312 (a)(2)(ii)	**Emergency access procedure:** Establish (and implement as needed) procedures for obtaining necessary ePHI during an emergency.	Application user access is restricted via role-based security privileges defined within the access control system. Application audit policy settings are in place that include: • Request ID • User ID • Contract ID • Action taken Application audit logs are maintained and reviewed as needed. MFA is required for all users to access the network. An IPS is utilized to analyze network events and report possible or actual network security breaches. The entity secures its environment a using multi-layered defense approach that includes firewalls, an IPS, antivirus software and a DMZ. VPN and TLS are used for defined points of connectivity. Business continuity and disaster recovery plans are developed and updated on an annual basis. The business continuity plan and disaster recovery procedure are tested on an annual basis. A business continuity plan is documented and in place that outlines the range of disaster scenarios and steps the business will take in a disaster to ensure the timely resumption of critical business operations.

TECHNICAL SAFEGUARDS		
Ref	**Regulation**	**Control Activity Specified by the Service Organization**
		The business continuity plan is tested on an annual basis and includes: • Various testing scenarios based on threat likelihood • Identifying the critical systems required for business operations • Assigning roles and responsibilities in the event of a disaster • Assessing and mitigating risks identified as a result of the test disaster The ways in which critical data are backed up and stored are documented and reviewed annually. Data backup and restore procedures are in place to guide personnel in performing backup activities. When a backup job fails, the backup tool sends an alert to the backup administrators who investigate and resolve the failure. Logical access privileges are reviewed on an annual by authorized personnel to help ensure the appropriateness of access credentials and that least privileges required to perform job functions are assigned to user accounts. Backup restoration tests are performed on an annual basis. The business continuity plan and disaster recovery procedures are tested on an annual basis.
164.312 (a)(2)(iii)	**Automatic logoff:** Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.	Documented policies and procedures are in place regarding system settings, authentication, access, and security monitoring.
	Network (Azure AD)	
		Azure AD is configured to enforce password requirements that include: • Password history • Password maximum age • Password length • Complexity
	Operating System (Windows)	
		Operating systems are configured to use Azure AD for single sign-on (SSO).

TECHNICAL SAFEGUARDS		
Ref	**Regulation**	**Control Activity Specified by the Service Organization**
	Database (SQL) Azure Managed Sequel	
		Databases are configured to enforce password requirements that include: • Password history • Password maximum age • Password length • Complexity
	Application (ContractPodAi)	
164.312 (a)(2)(iv)	**Encryption and decryption:** Implement a mechanism to encrypt and decrypt ePHI.	The application is configured to enforce password requirements that include: • Password history • Password length • Complexity Server certificate-based authentication is used as part of the TLS encryption with a trusted certificate authority. Stored passwords are encrypted. Critical data is stored in encrypted format using software supporting the Azure SSE and 256-bit advanced encryption standard (AES). Encryption keys are protected during generation, storage, use, and destruction.
164.312 (b)	**Audit controls:** Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use ePHI.	Regular monitoring and review of log-ins and log-in attempts to the system is in place. Discrepancies and potentially inappropriate or illegal activities are reported to senior management, legal counsel and/or human resources, as appropriate.
	Network (Azure AD)	
		Azure AD audit logging settings are in place that include: • Logon events • System events Azure AD audit logs are maintained and reviewed as needed.
	Operating System (Windows)	
		Windows audit logging settings are in place that include: • Logon events • System events Windows audit logs are maintained and reviewed as needed.
	Database (SQL) Azure Managed Sequel	
		Database audit logging settings are in place that include failed logon events.

TECHNICAL SAFEGUARDS		
Ref	**Regulation**	**Control Activity Specified by the Service Organization**
		Database audit logs are maintained and reviewed as needed.
	Application (ContractPodAi)	
164.312 (c)(1)	**Integrity:** Implement policies and procedures to protect ePHI from improper alteration or destruction.	Application audit policy settings are in place that include: • Request ID • User ID • Contract ID • Action taken Application audit logs are maintained and reviewed as needed. Data that entered into the system, processed by the system and output from the system is protected from unauthorized access. FIM software is in place to ensure only authorized changes are deployed into the production environment. The FIM software is configured to notify IT personnel via email alert when a change to the production application code files is detected.
164.312 (c)(2)	**Mechanisms to authenticate ePHI:** Implement electronic mechanisms to corroborate that ePHI has not been altered or destroyed in an unauthorized manner.	Monitoring software is in place to monitor and log metrics from resources, applications, performance, resource utilization, and other infrastructure components. Alerts are sent to personnel when certain alarms are triggered. An IPS is utilized to analyze network events and report possible or actual network security breaches. The IPS is configured to notify personnel upon intrusion prevention. FIM software is in place to ensure only authorized changes are deployed into the production environment. The FIM software is configured to notify IT personnel via email alert when a change to the production application code files is detected.
164.312 (d)	**Person or entity authentication:** Implement procedures to verify that a person or entity seeking access to ePHI is the one claimed.	Documented policies and procedures are in place regarding system settings, authentication, access, and security monitoring.
	Network (Azure AD)	
		Azure AD user access is restricted via role-based security privileges defined within the access control system.

TECHNICAL SAFEGUARDS		
Ref	**Regulation**	**Control Activity Specified by the Service Organization**
		Azure Ad administrative access is restricted to the following authorized personnel: • Director of Technology • Director of Information Security • Manager of Technology • Infra Support Azure AD is configured to enforce password requirements that include: • Password history • Password maximum age • Password length • Complexity Azure AD account lockout settings are in place that include: • Account lockout duration • Account lockout threshold • Account lockout counter reset Azure AD audit logging settings are in place that include: • Logon events • System events Azure AD audit logs are maintained and reviewed as needed.
	Operating System (Windows)	
		Operating system user access is restricted via role-based security privileges defined within the access control system. Operating system administrative access is restricted to the following authorized personnel: • Senior Director of Technology • Director of Information Security • Senior System Administrator • Senior DevOps Engineer • Manager of Technology • Infra Support Operating systems are configured to use Azure AD for SSO.
	Database (SQL) Azure Managed Sequel	
		Database user access is restricted via role-based security privileges defined within the access control system.

TECHNICAL SAFEGUARDS		
Ref	**Regulation**	**Control Activity Specified by the Service Organization**
		Database administrative access is restricted to the following personnel: • Senior Director of Technology • Director of Information Security • Senior System Administrator • Senior DevOps Engineer • Manager of Technology • Infra Support SQL databases are configured to use mixed mode authentication. Databases are configured to enforce password requirements that include: • Password history • Password maximum age • Password length • Complexity Database users are authenticated via individually assigned user accounts and passwords. Database account lockout settings are in place that include: • Account lockout duration • Account lockout threshold • Account lockout counter reset Database audit logging settings are in place that include failed logon events. Database audit logs are maintained and reviewed as needed.
	Application (ContractPodAi)	
		Application user access is restricted via role-based security privileges defined within the access control system. Application administrative access is appropriately restricted to authorized personnel: • Manager of Technology • Senior Developer • Software Test Lead The application is configured to enforce password requirements that include: • Password history • Password length • Complexity Application users are authenticated via individually assigned user accounts and passwords. Application account lockout settings are in place that include account lockout threshold.

TECHNICAL SAFEGUARDS		
Ref	**Regulation**	**Control Activity Specified by the Service Organization**
		Application audit policy settings are in place that include: • Request ID • User ID • Contract ID • Action Taken Application audit logs are maintained and reviewed as needed. MFA is required for all users to access the network. An IPS is utilized to analyze network events and report possible or actual network security breaches. The entity secures its environment a using multi-layered defense approach that includes firewalls, an IPS, antivirus software and a DMZ.
164.312 (e)(1)	**Transmission security:** Implement technical security measures to guard against unauthorized access to ePHI that is being transmitted over an electronic communications network.	Server certificate-based authentication is used as part of the TLS encryption with a trusted certificate authority. Stored passwords are encrypted. Critical data is stored in encrypted format using software supporting the Azure SSE and 256-bit advanced encryption standard (AES). Encryption keys are protected during generation, storage, use, and destruction.
164.312 (e)(2)(i)	**Integrity controls:** Implement security measures to ensure that electronically transmitted ePHI is not improperly modified without detection until disposed of.	Server certificate-based authentication is used as part of the TLS encryption with a trusted certificate authority. Stored passwords are encrypted. Critical data is stored in encrypted format using software supporting the Azure SSE and 256-bit advanced encryption standard (AES). Encryption keys are protected during generation, storage, use, and destruction. Monitoring software is in place to monitor and log metrics from resources, applications, performance, resource utilization, and other infrastructure components. Alerts are sent to personnel when certain alarms are triggered. An IPS is utilized to analyze network events and report possible or actual network security breaches. The IPS is configured to notify personnel upon intrusion prevention. FIM software is in place to ensure only authorized changes are deployed into the production environment.

TECHNICAL SAFEGUARDS		
Ref	**Regulation**	**Control Activity Specified by the Service Organization**
164.312 (e)(2)(ii)	**Encryption:** Implement a mechanism to encrypt ePHI whenever deemed appropriate.	The FIM software is configured to notify IT personnel via email alert when a change to the production application code files is detected. Server certificate-based authentication is used as part of the TLS encryption with a trusted certificate authority. Stored passwords are encrypted. Critical data is stored in encrypted format using software supporting the Azure SSE and 256-bit AES. Encryption keys are protected during generation, storage, use, and destruction.

ORGANIZATIONAL REQUIREMENTS		
Ref	**Regulation**	**Control Activity Specified by the Service Organization**
164.314 (a)(1)	**Business associate contracts or other arrangements:** A covered entity is not in compliance with the standards in § 164.502(e) if the covered entity knew of a pattern of an activity or practice of the business associate that constituted a material breach or violation of the business associate's obligation under the contract or other arrangement, unless the covered entity took reasonable steps to cure the breach or end the violation, as applicable, and, if such steps were unsuccessful - (A) Terminated the contract or arrangement, if feasible; or (B) If termination is not feasible, reported the problem to the Secretary."	Not applicable. The services provided by the entity does not include sharing information that would require any executed business associate agreements.
164.314 (a)(2)(i)	**Business Associate Contracts:** A business associate contract must provide that the business associate will: "Implement safeguards that protect the confidentiality, integrity, and availability of the electronic protected health…; Report to the covered entity any security incident of which it becomes aware; Authorize termination of the contract, if the covered entity determines that the business associate has violated a material term of the contract."	Not applicable. The services provided by the entity does not include sharing information that would require any executed business associate agreements.
164.314 (a)(2)(ii)	**Other Arrangement:** The Other Arrangements implementation specifications provide that when a covered entity and its business associate are both government entities, the covered entity may comply with the standard in either of two alternative ways.	Not applicable. The entity is not a government entity.
164.314 (b)(1)	**Requirements for Group Health Plans:** Except when the only ePHI disclosed to a plan sponsor is disclosed pursuant to §164.504(f)(1)(ii) or (iii), or as authorized under §164.508, a group health plan must ensure that its plan documents provide that the plan sponsor will reasonably and appropriately safeguard ePHI created, received, maintained, or transmitted to or by the plan sponsor on behalf of the group health plan.	Not applicable. The entity is not a plan sponsor.

ORGANIZATIONAL REQUIREMENTS		
Ref	**Regulation**	**Control Activity Specified by the Service Organization**
164.314 (b)(2)	**Implementation Specifications:** The plan documents of the group health plan must be amended to incorporate provisions to require the plan sponsor to- (i) Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the ePHI that it creates, receives, maintains, or transmits on behalf of the group health plan; (ii) Ensure that the adequate separation required by §164.504(f)(2)(iii) is supported by reasonable and appropriate security measures; (iii) Ensure that any agent, including a subcontractor, to whom it provides this information agrees to implement reasonable and appropriate security measures to protect the information; and (iv) Report to the group health plan any security incident of which it becomes aware.	Not applicable. The entity is not a plan sponsor.
164.316 (a)	**Policies and Procedures:** Implement reasonable and appropriate policies and procedures to comply with the standards, implementation specifications, or other requirements of this subpart, taking into account those factors specified in 164.306(b)(2)(i), (ii), (iii), and (iv) [the Security Standards: General Rules, Flexibility of Approach]. This standard is not to be construed to permit or excuse an action that violates any other standard.	Management reviews policies, procedures and other control documents for accuracy and applicability on an annual basis. Organizational and information security policies and procedures are documented for supporting the functioning of controls and processes and made available to its personnel through the Company's shared drive.
164.316 (b)(1)	**Documentation:** Maintain the policies and procedures implemented to comply with this subpart in written (which may be electronic) form; and (ii) if an action, activity or assessment is required by this subpart to be documented, maintain a written (which may be electronic) record of the action, activity, or assessment.	Management reviews policies, procedures and other control documents for accuracy and applicability on an annual basis. Organizational and information security policies and procedures are documented for supporting the functioning of controls and processes and made available to its personnel through the Company's shared drive.
164.316 (b)(1)(i)	**Time Limit:** Retain the documentation required by paragraph (b) (1) of this section for 6 years for the date of its creation or the date when it last was in effect, whichever is later.	The entity retains all documentation for a minimum period of six (6) years from the date of its creation or modification, or the date when it was last in effect.
164.316 (b)(1)(ii)	**Availability:** Make documentation available to those persons responsible for implementing the procedures to which the documentation pertains.	Organizational and information security policies and procedures are documented for supporting the functioning of controls and processes and made available to its personnel through the Company's shared drive.

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

BREACH NOTIFICATION		
Ref	**Regulation**	**Control Activity Specified by the Service Organization**
164.402	Breach means the acquisition, access, use, or disclosure of protected health information in a manner not permitted under subpart E of this part which compromises the security or privacy of the protected health information. (1)(i) For purposes of this definition, compromises the security or privacy of the protected health information means poses a significant risk of financial, reputational, or other harm to the individual. (ii) A use or disclosure of protected health information that does not include the identifiers listed at §164.514(e)(2), date of birth, and zip code does not compromise the security or privacy of the protected health information.	Breach notification letters or emails are developed and prepared to be used during a breach of ePHI. Notification procedures include: • Notice to parties alerting them to breaches "without unreasonable delay," but no later than 60 days after discovery of the breach • Notice to covered entities when breach is discovered • Notice to the secretary of Human Health Services (HHS) and prominent media outlets about breaches involving more than 500 individual subject's records • Notice to next of kin about breaches involving parties who are deceased • Notices to include what happened, the details of the breached unsecure PHI, steps to help mitigate harm to the party, and the covered entity's response • Annual notice to the secretary of HHS 60 days before the end of the calendar year about unsecure PHI breaches involving fewer than 500 patient records
164.404 (a)(1)	A covered entity shall, following the discovery of a breach of unsecured protected health information, notify each individual whose unsecured protected health information has been, or is reasonably believed by the covered entity to have been, accessed, acquired, used or disclosed as a result of such breach.	Not applicable. The entity is a business associate; its responsibilities for breach notification are limited to its covered entity customers.
164.404 (a)(2)	For purposes of paragraph (a)(1) of this section, §§ 164.406(a), and 164.408(a), a breach shall be treated as discovered by a covered entity as of the first day on which such breach is known to the covered entity, or, by exercising reasonable diligence would have been known to the covered entity. A covered entity shall be deemed to have knowledge of a breach if such breach is known, or by exercising reasonable diligence would have been known, to any person, other than the person committing the breach, who is a workforce member or agent of the covered entity (determined in accordance with the federal common law of agency).	Not applicable. The entity is a business associate; its responsibilities for breach notification are limited to its covered entity customers.
164.404 (b)	Except as provided in §164.412, a covered entity shall provide the notification required by paragraph (a) of this section without unreasonable delay and in no case later than 60 days after discovery of a breach.	Not applicable. The entity is a business associate; its responsibilities for breach notification are limited to its covered entity customers.

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

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

BREACH NOTIFICATION		
Ref	**Regulation**	**Control Activity Specified by the Service Organization**
164.408 (a)	A covered entity shall, following the discovery of a breach of unsecured protected health information as provided in §164.404(a)(2), notify the Secretary.	Not applicable. The entity is a business associate; its responsibilities for breach notification are limited to its covered entity customers.
164.408 (b)	For breaches of unsecured protected health information involving 500 or more individuals, a covered entity shall, expect as provided in §164.412, provide the notification required by paragraph (a) contemporaneously with the notice required by §164.404(a) and in the manner specified on the HHS web site.	Not applicable. The entity is a business associate; its responsibilities for breach notification are limited to its covered entity customers.
164.408 (c)	For breaches of unsecured protected health information involving less than 500 individuals, a covered entity shall maintain a log or other documentation of such breaches and, not later than 60 days after the end of each calendar year, provide the notification required by paragraph (a) of this section for breaches occurring during the preceding calendar year, in a manner specified on the HHS web site.	Not applicable. The entity is a business associate; its responsibilities for breach notification are limited to its covered entity customers.
164.410 (a)(1)	A business associate shall, following the discovery of a breach of unsecured protected health information, notify the covered entity of such breach.	Breach notification letters or emails are developed and prepared to be used during a breach of ePHI. Notification procedures include: • Notice to parties alerting them to breaches “without unreasonable delay,” but no later than 60 days after discovery of the breach • Notice to covered entities when breach is discovered • Notice to the secretary of Human Health Services (HHS) and prominent media outlets about breaches involving more than 500 individual subject’s records • Notice to next of kin about breaches involving parties who are deceased • Notices to include what happened, the details of the breached unsecure PHI, steps to help mitigate harm to the party, and the covered entity’s response • Annual notice to the secretary of HHS 60 days before the end of the calendar year about unsecure PHI breaches involving fewer than 500 patient records

BREACH NOTIFICATION		
Ref	**Regulation**	**Control Activity Specified by the Service Organization**
164.410 (a)(2)	(2) For the purposes of paragraph (1) of this section, a breach shall be treated as discovered by a business associate as of the first day on which such breach is known to the business associate or, by exercising reasonable diligence, would have been known to the business associate. A business associate shall be deemed to have knowledge of a breach if the breach is known, or by exercising reasonable diligence would have been known, to any person, other than the person committing the breach, who is an employee, officer, or other agent of the business associate (determined in accordance with the federal common law of agency).	The entity acknowledges responsibility for notifying affected parties in the event of a breach of unsecured protected health information.
164.410 (b)	Except as provided in §164.412, a business associate shall provide the notification required by paragraph (a) of this section without unreasonable delay and in no case later than 60 calendar days after the discovery of a breach.	The entity notifies affected parties of a breach of ePHI no later than 60 calendar days after the discovery of the breach.
164.410 (c)(1)	The notification required by paragraph (a) of this section shall include, to the extent possible, the identification of each individual whose unsecured protected health information has been, or is reasonably believed by the business associate to have been accessed, acquired, used or disclosure during the breach.	The identification of each individual whose unsecured ePHI has been accessed during the breach is disclosed during notification procedures.
164.410 (c)(2)	A business associate shall provide the covered entity with any other information that the covered entity is required to include in the notification to the individual under §164.404(c) at the time of the notification required by paragraph (a) of this section or promptly thereafter as information becomes available.	Management provides the covered entity with any information that the covered entity is required to include in the notification to the individual at the time of the breach and as soon as it is available.
164.412	If a law enforcement official states to a covered entity or business associate that a notification, notice or posting required under this subpart would impede a criminal investigation or cause damage to national security, a covered entity or business associate shall: (a) If the statement is in writing and specifies the time for which a delay is required, delay such notification, notice, or posting for the time period specified by the official; or (b) If the statement is made orally, document the statement, including the identity of the official making the statement, and delay the notification, notice, or posting temporarily and no longer than 30 days from the date of the oral statement, unless a written statement as described in paragraph (a) of this section is submitted during that time.	The entity refrains from, or delays notifying HHS personnel, the covered entity, or other required persons following the discovery of a breach of unsecured protected health information when required by law.

BREACH NOTIFICATION		
Ref	**Regulation**	**Control Activity Specified by the Service Organization**
164.414	**Administrative requirements and burden of proof**: In the event of a use or disclosure in violation of subpart E, the covered entity or business associate; as applicable, shall have the burden of demonstrating that all notifications were made as required by this subpart or that the use or disclosures did not constitute a breach as defined at §164.402. See §164.530 for definition of breach.	The entity acknowledges responsibility for notifying affected parties in the event of a breach of unsecured protected health information.

SECTION 4

INFORMATION PROVIDED BY THE SERVICE AUDITOR

GUIDANCE REGARDING INFORMATION PROVIDED BY THE SERVICE AUDITOR

A-LIGN ASSURANCE's examination of the controls of ContractPodAi was limited to the HIPAA/HITECH requirements and related control activities specified by the management of ContractPodAi and did not encompass all aspects of ContractPodAi's operations or operations at user entities. Our examination was performed in accordance with American Institute of Certified Public Accountants (AICPA) AT-C 105, AT-C 205 and AT-C 315.

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

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

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

- Understand the aspects of the service organization's controls that may affect the HIPAA/HITECH requirements
- Understand the flow of ePHI through the service organization
- Determine whether the service organization's controls are suitably designed to meet the health information security program of the user entity's and determine whether they have been implemented