A-LIGN

Phreesia, Inc.

Type 2 SOC 3

2023

SOC 3 FOR SERVICE ORGANIZATIONS REPORT

June 1, 2022 to May 31, 2023

Table of Contents

SECTION 1

ASSERTION OF PHREESIA, INC. MANAGEMENT

ASSERTION OF PHREESIA, INC. MANAGEMENT

July 26, 2023

We are responsible for designing, implementing, operating, and maintaining effective controls within Phreesia, Inc.'s ('Phreesia' or 'the Company') Automated Patient Intake Platform Services System throughout the period June 1, 2022 to May 31, 2023, to provide reasonable assurance that Phreesia's service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Availability, and Confidentiality (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*, in AICPA, *Trust Services Criteria*. Our description of the boundaries of the system is presented below in "Phreesia, Inc.'s Description of Its Automated Patient Intake Platform Services System throughout the period June 1, 2022 to May 31, 2023" and identifies the aspects of the system covered by our assertion.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period June 1, 2022 to May 31, 2023, to provide reasonable assurance that Phreesia's service commitments and system requirements were achieved based on the trust services criteria. Phreesia's objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented in "Phreesia, Inc.'s Description of Its Automated Patient Intake Platform Services System throughout the period June 1, 2022 to May 31, 2023".

Phreesia uses Rackspace Technology, Inc. ('Rackspace') and Equinix, Inc. ('Equinix') to provide colocation services, and Amazon Web Services ('AWS'), Google Cloud Platform ('GCP'), and Microsoft Azure ('Azure') to provide cloud hosting services (collectively, the 'subservice organizations'). The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Phreesia, to achieve Phreesia's service commitments and system requirements based on the applicable trust services criteria. The description presents Phreesia's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Phreesia's controls. The description does not disclose the actual controls at the subservice organizations.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary to achieve Phreesia's service commitments and system requirements based on the applicable trust services criteria. The description presents the applicable trust services criteria and the complementary user entity controls assumed in the design of Phreesia's controls.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of these inherent limitations, a service organization may achieve reasonable, but not absolute, assurance that its service commitments and system requirements are achieved.

We assert that the controls within the system were effective throughout the period June 1, 2022 to May 31, 2023 to provide reasonable assurance that Phreesia's service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls and complementary user entity controls assumed in the design of Phreesia's controls operated effectively throughout that period.

Wes Shriner
Senior Director - Audit, Risk, Compliance
Phreesia, Inc.

SECTION 2

INDEPENDENT SERVICE AUDITOR'S REPORT

A-LIGN

INDEPENDENT SERVICE AUDITOR'S REPORT

To Phreesia, Inc.:

Scope

We have examined Phreesia, Inc.'s ('Phreesia' or 'the Company') accompanying assertion titled "Assertion of Phreesia, Inc. Management" (assertion) that the controls within Phreesia's Automated Patient Intake Platform Services System were effective throughout the period June 1, 2022 to May 31, 2023, to provide reasonable assurance that Phreesia's service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Availability, and Confidentiality (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*, in AICPA *Trust Services Criteria*.

Phreesia uses Rackspace and Equinix to provide colocation services, and AWS, GCP, and Azure to provide cloud hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Phreesia, to achieve Phreesia's service commitments and system requirements based on the applicable trust services criteria. The description presents Phreesia's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Phreesia's controls. The description does not disclose the actual controls at the subservice organizations. Our examination did not include the services provided by the subservice organizations, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Phreesia, to achieve Phreesia's service commitments and system requirements based on the applicable trust services criteria. The description presents Phreesia's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of Phreesia's controls. Our examination did not include such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such controls.

Service Organization's Responsibilities

Phreesia is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that Phreesia's service commitments and system requirements were achieved. Phreesia has also provided the accompanying assertion (Phreesia assertion) about the effectiveness of controls within the system. When preparing its assertion, Phreesia is responsible for selecting, and identifying in its assertion, the applicable trust services criteria and for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls within the system.

Service Auditor's Responsibilities

Our responsibility is to express an opinion, based on our examination, on management's assertion that controls within the system were effective throughout the period to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Our examination was conducted in accordance with attestation standards established by the AICPA. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Our examination included:

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

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

Independence and Ethical Responsibilities

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

Inherent Limitations

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

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

Opinion

In our opinion, management's assertion that the controls within Phreesia's Automated Patient Intake Platform Services System were suitably designed and operating effectively throughout the period June 1, 2022 to May 31, 2023, to provide reasonable assurance that Phreesia's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects, if complementary subservice organization controls and complementary user entity controls assumed in the design of Phreesia's controls operated effectively throughout that period.

The SOC logo for Service Organizations on Phreesia's website constitutes a symbolic representation of the contents of this report and is not intended, nor should it be construed, to provide any additional assurance.

Restricted Use

This report, is intended solely for the information and use of Phreesia, user entities of Phreesia's Automated Patient Intake Platform Services System during some or all of the period June 1, 2022 to May 31, 2023, business partners of Phreesia subject to risks arising from interactions with the Automated Patient Intake Platform Services System, and those who have sufficient knowledge and understanding of the complementary subservice organization controls and complementary user entity controls and how those controls interact with the controls at the service organization to achieve the service organization's service commitments and system requirements.

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

A-LIGN ASSURANCE

Tampa, Florida
July 26, 2023

SECTION 3

PHREESIA, INC.'S DESCRIPTION OF ITS AUTOMATED PATIENT INTAKE PLATFORM SERVICES SYSTEM THROUGHOUT THE PERIOD JUNE 1, 2022 TO MAY 31, 2023

OVERVIEW OF OPERATIONS

Company Background

Phreesia gives providers, health plans, life sciences companies, and other organizations tools to help patients take a more active role in their care, improving clinical outcomes, and driving efficiency. Phreesia offers patient-driven digital solutions for intake, outreach, education and more.

Phreesia was founded in 2005 by Chaim Indig and Evan Roberts to transform the healthcare experience by putting innovative technology into the hands of patients to automate check-in and streamline front-office workflow. Phreesia's platform has evolved to include applications in registration, revenue cycle, appointments, eligibility and benefits verification, clinical support, patient activation and analytics, along with integrations with the leading practice management (PM) applications and electronic health record (EHR) systems.

Phreesia is certified by HITRUST Alliance and as a PCI DSS Level 1 Service Provider. Phreesia is a four-time top-ranked Patient Intake Management vendor by the research and insights firm KLAS.

Phreesia realizes how uniquely positioned it is to connect with patients before, during, and after their visit. Phreesia's mission is to help healthcare providers better understand their patients, improve health outcomes and create a better, more engaging healthcare experience for everyone.

Description of Services Provided

The Phreesia platform manages the end-to-end patient intake process and encompasses a comprehensive range of software and services, including:

Phreesia Patient Intake Platform: Software and Services	
Appointment Scheduling	Mobile, virtual visit and in-office registration with self-scheduling, consents, and reminders.
Appointment Accelerator	Automated text message-based solution designed to fill open slots on healthcare organizations' schedules with clinically relevant patients.
Insurance Verification	Automated real-time eligibility and benefits (E&B) checks that help organizations save time and improve collections accuracy.
Health Campaigns	Targeted messages that allow healthcare organizations to engage with patients before, during, and after their visit.
Patient Activation Measure (PAM on Flourish)	Behavioral health model to assess patient's healthcare self-management knowledge, skills, and confidence.
PAM on Flourish Analytics & Reporting	Accurately assess risk and refine care management processes for better patient coaching. Target allocation of staff, resources, and campaigns for improved health outcomes.
Provider Analytics & Reporting	Data and reporting analytics for provider management.
Clinical Support	Collect patient-reported data during intake, screen for relevant conditions, and identify social determinants of health (SDOH).
Connect	Online referral management platform.
POS and Mobile Payments	P2PE and E2EE encrypted transactions through dedicated hardware or user preferred web devices.
Payment Alternatives	Flexible payment options, copayments, and payment plans.

Phreesia Patient Intake Platform: Software and Services	
Automated Collections	Smart payment reminders during digital patient encounters.
Payment Processing and Gateway Services	Full payment processing using either Phreesia or the Client's processor and merchant IDs.
Patient Connect	Provides relevant healthcare messages directly to qualified patients at check-in with follow-up reminders to drive patient activation and improve health outcomes.
Member Connect	Provides relevant healthcare messages directly to qualified members at check-in with follow-up reminders to drive member activation and improve health outcomes.
Patient Insights / Member Insights	Presents customized post-visit health surveys to qualified patients to generate business and clinical insights.
Staff Dashboard	Secure web access to manage patient intake and analytics workflows.
Phreesia Mobile	Secure web access for appointment registration, payment and organization communications using a patient's device.
PadX, PhreesiaPads and Arrivals Stations	Onsite hardware for patient secure web access for appointment registration and payments.

Phreesia's solutions are highly customizable and scalable to healthcare provider organizations of all sizes, from single-specialty practices to multispecialty groups and large health systems.

Information is shared with user entities through secured websites, secured application programming interfaces (APIs), secured purpose-built hardware, and secure electronic exchange (SFTP and e-mail).

Principal Service Commitments and System Requirements

Phreesia designs its processes and procedures to support its service objectives. Those objectives are based on the service commitments that Phreesia makes to user entities, the laws and regulations that govern the provision of Phreesia services, and the financial, operational, compliance, and security requirements that Phreesia has established for the services.

Phreesia's services are subject to the security and privacy requirements of the Health Insurance Portability and Accountability Act (HIPAA) and all relevant regulations. Phreesia is accredited by the Payment Card Industry Data Security Standards (PCI DSS), by HITRUST Alliance, and by the American Institute of Certified Public Accountants (AICPA) SOC2 Type II. Phreesia is subject to all state privacy security laws and regulations in which Phreesia operates.

Security commitments to user entities are documented and communicated in Service-Level Agreements (SLAs), Business Associate Agreements (BAA), and other client agreements, as well as in the description of the service offering provided within Phreesia's Master Services Agreement.

Security concepts of the Phreesia SaaS platform permit system users to access the information they need based on their role in the system while restricting them from accessing information not needed for their role.

Phreesia has implemented the use of encryption technologies to protect client data both at rest and in transit through public networks.

Phreesia establishes operational requirements that support the achievement of security commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in Phreesia's policies and procedures, system design documentation, and contracts with clients.

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 internal business systems and networks are managed, and how employees are hired and trained. In addition to these policies, standard operating procedures have been documented on how to carry out specific manual and automated processes required in the operation and development of the Phreesia SaaS platform and supporting services.

Components of the System

Infrastructure

Primary infrastructure used to provide Phreesia's Automated Patient Intake Platform Services System is available in the full SOC2 report under mutual non-disclosure agreement.

Software

Primary software used to provide Phreesia's Automated Patient Intake Platform Services System is available in the full SOC2 report under mutual non-disclosure agreement.

People

Phreesia is actively growing, with 1,500 full-time employees and 1,200 contractor staff led by the Executive Team:

Chaim Indig, Chief Executive Officer and Board Member

Since co-founding Phreesia in 2005, Chaim Indig has helped revolutionize the patient intake experience. Under his leadership, Phreesia has established a broad national footprint, developed strategic partnerships with some of the world's largest healthcare companies, and earned accolades for its role in making healthcare more efficient and patient centered.

Evan Roberts, Chief Operating Officer

Evan Roberts is a co-founder of Phreesia and the technical visionary responsible for providing Phreesia's transformative patient intake management solutions to healthcare organizations across the country.

Balaji Gandhi, Chief Financial Officer

As Chief Financial Officer, Balaji Gandhi leverages more than 25 years of executive experience to oversee the company's budgeting, forecasting, monthly reporting, financial analysis, internal controls and investor relations.

Dan Nathan, Chief Technology Officer

As Chief Technology Officer, he oversees Phreesia's core and integration platforms, and is responsible for the company's Patient Intake, Data Center Operations, Site Reliability Engineering and Analytics teams.

Allison Hoffman, General Counsel

As Phreesia's General Counsel, Allison manages the company's legal, compliance, risk, and privacy teams. She has more than 25 years of legal and people-management experience.

Organizational Structure

Phreesia is comprised of various departments that work together to achieve the company's mission of creating a better, more engaging healthcare experience for hospitals, health systems, clinics, and specialty groups.

Phreesia partners with its clients to ensure smooth and rapid implementation, provide support across Phreesia's product suite, and improve utilization and retention. Each client is assigned a dedicated implementation team to support the business process integration and technical integration with third-party EHR systems and PM applications. Once onboarded, Phreesia's dedicated account management works continuously with clients to develop solutions that align with their evolving digital strategy and meet their specific needs. Phreesia's product organization is focused on quality delivery, client feedback, and innovative value.

Phreesia's Risk Management and Cyber-Risk Management programs work together to manage and mitigate risk to Phreesia products and services, and within the Phreesia company. Phreesia's Security program is built for product and enterprise security. Continuous monitoring tools, alerting infrastructure, and response capabilities are in place and operating.

Phreesia is compliant with the laws and industry regulations appropriate for its industry and location. Phreesia maintains current certifications for HITRUST and PCI DSS. Phreesia is a publicly traded company and is SOX compliant. Phreesia's Privacy program manages and protects the Personal Health Information (PHI) entrusted to Phreesia.

Data

Data, as defined by Phreesia, constitutes the following:

- PHI and personally identifiable information (PII)
- Payment card data
- Client data
- Internal sensitive information, including secrets, system files, logs, configurations, and output reports

Transaction processing through the Phreesia Patient Intake Platform occurs in the following ways:

- **Phreesia SaaS applications and APIs** - Including Dashboard, Appointments, API, Revenue Cycle, Clinical Support, Patient Activation, Patient Surveys, and Analytics and Reporting functions. On behalf of its clients, Phreesia develops, hosts and supports applications and web services to monitor the intake process, verify eligibility and benefits, process and track payments, and view reporting and analytics. The Testing Summary contains a list of systems involved with these components.
- **Electronic Health Records (EHR) Phreesia Integration Client Software** - Phreesia has built a set of software services that can be installed within an organization's network to integrate information between the organization's EHR system and the Phreesia Dashboard. Once installed and configured to communicate with Phreesia, Phreesia manages updates to the software on the client's behalf. It is the client's responsibility to manage the hosted server and operating environment (network) in which the integration client software resides.
- **Managed Devices** - The PhreesiaPad (tablet) and Arrivals Station (kiosk) allow patients to update their information, take a photo to store in their patient record, capture images of their driver's license and insurance card, sign consent forms, and pay copays and outstanding balances privately and securely from their healthcare provider's waiting room. These devices are managed by Phreesia on behalf of Phreesia's clients and are deployed within healthcare organizations' offices where they are physically secured by the organization's staff.
- **Client-Managed Devices** - Phreesia's iOS mobile application operates on client-owned, managed and secured hardware, and it provides similar functionality to the PhreesiaPad. Phreesia provides a custom iOS application delivered through the application store.

- **Phreesia Mobile** - With Phreesia Mobile, patients can register for their visit from the comfort and privacy of their home computer, tablet, smartphone or other personal device. It also streamlines intake for healthcare staff and alleviates the headache of check-in forms.

Phreesia also offers traditional payment-collection devices, including several form factors of in-office, USB-attached, encrypted card-swipe, and manual key-entry devices. PhreesiaPads, Arrivals Stations and the iOS mobile application are used by patients on site. Phreesia Mobile allows the patient to manage their appointments from anywhere on their own device.

Output reports are available through the Phreesia Dashboard and are delivered through secure transport to verified entities.

Processes, Policies and Procedures

Operational Controls

Formal IT policies and procedures exist that describe physical security, configuration management, systems operations, data communications, systems development life cycle, change control, logical access, availability and monitoring, vulnerability management, backup and disaster recovery standards.

Teams and contractors are expected to adhere to Phreesia policies and procedures that define how services should be delivered. These are located on Phreesia's intranet and can be accessed by any Phreesia team member or contractor.

Physical Security

Phreesia locations:

- Phreesia, Inc. is headquartered at 1521 Concord Pike Suite 301, PMB 221. Wilmington, DE 19803
- One Rackspace data center in Somerset, New Jersey
- Two Equinix data centers in Ashburn, Virginia
- U.S. region instances in MS Azure, Google Cloud (GCP), and Amazon Web Services (AWS)

Phreesia maintains documented Physical Security policies, standards, and procedures to guide personnel in documenting and implementing physical security activities.

Phreesia is a 100% remote-work company. Network, identity, and endpoint security controls are in place to secure Phreesia's 100% remote-work environment. Phreesia staff are trained in physical and operational security concepts as part of their onboarding and annual training. Phreesia users acknowledge acceptance of Acceptable Use Policies, Privacy Policies, Information Security Policies, and Telework Agreements at onboarding and annually thereafter.

Phreesia Offices

Phreesia does not maintain an office facility, workspace, corporate network, or wireless network.

Phreesia Data Centers

Phreesia's SaaS Platform is co-located in locked, secured, single-tenant spaces at Rackspace and Equinix Tier 4 facilities. Phreesia owns and manages equipment hosted in these facilities.

Access to sensitive systems, which are co-located in Phreesia's dedicated data center space, is restricted to key Phreesia personnel and data center staff. Access to points of ingress/egress to Phreesia infrastructure, as well as telecommunications and power connections, are appropriately routed to avoid shared space and designed to prevent unauthorized physical access.

Physical access to data center facilities is under constant video and physical surveillance by data center staff to prevent unauthorized access to Phreesia systems. Rackspace and Equinix maintain data center access request logs for tracking Phreesia entry into co-located data center space. This log is audited against physical access logs periodically to ensure compliance and adherence to established policies and procedures.

Physical access to Phreesia's presence in Azure, GCP, and AWS U.S. regions are not managed by Phreesia. There is no physical access by Phreesia personnel.

Logical Access and Identity Infrastructure

Phreesia maintains documented Logical Access and Identity Infrastructure policies, standards, and procedures to guide personnel in documenting and implementing access activities.

Phreesia uses role-based identity architecture and requires users of the system to be identified and authenticated prior to the use of any system resources. Phreesia applies concepts of least-privileged access, the minimum-necessary rule, and segregation of duties when assigning role-based entitlements.

Resources are protected using authentication systems, such as an identity provider with single sign-on; and multi-factor authentication to authenticate users and authorize user entitlements.

Phreesia resources are data-classified and managed with asset inventory systems. Each asset is assigned a department owner responsible for the system and data. Phreesia's Identity and Access Management (IAM) Program works with asset owners to perform periodic reviews of sensitive access by role.

Employees and approved vendor personnel sign on to the Phreesia network using an Active Directory user ID and password. Users are also required to separately sign onto any systems or applications that do not use the shared sign-on functionality of Active Directory.

Passwords must conform to defined password standards and are enforced through parameter settings in the Active Directory. These settings are part of the configuration standards and force users to change passwords at a defined interval, disable the user ID's ability to access the system and components after a specified number of unsuccessful access attempts, and mask workstation screens, requiring re-entry of the user ID and password after a period of inactivity. Users are authenticated before password changes are completed.

Employees accessing Phreesia resources are required to use two-factor authentication. Employees are issued tokens upon employment and tokens are disabled when an individual departs from Phreesia. Vendor personnel are only permitted access to the network through tightly controlled and approved systems.

Phreesia's Access Management Life Cycle

Upon hire, employees are assigned to a position in the HR management system. Prior to the employee's start date or employment change date, the HR management system creates a report of employee user IDs to be created and access to be granted or removed. The report is used by the service desk to create user IDs and related entitlements. Access rules are predefined based on employment roles.

HR works with IT Security Help Desk to provide timely notification of role changes and terminations. Access change tickets are actioned daily to maintain role-based access.

On a quarterly basis, active employees and system access privileges are reviewed for accuracy and appropriateness as part of the IAM Program. Modifications to access are made based on input from department managers.

On an annual basis, access rules for roles in critical systems and privileged access are reviewed by a working group composed of IAM security, IT, data center, and HR personnel. In evaluating role access, group members consider job description, duties requiring segregation and risks associated with access. If incompatible responsibilities cannot be segregated, Phreesia implements monitoring of one or more of the responsibilities. Monitoring is performed by a superior without responsibility for performing the conflicting activities or by personnel from a separate department. Completed rules are reviewed and approved by the head of information security.

Client Staff Identity Management

Client account configuration standards are client configurable. Phreesia provides clients with a role-based identity architecture and requires users of the system to be identified and authenticated prior to the use of any system resources. Clients are provided documented training and support for managing the logical access of their workforce.

Client employees access the Phreesia Dashboard SaaS application through the Internet using the SSL functionality of their web browser. These client employees must supply a valid user ID and password to gain access to client cloud resources. Passwords must conform to password configuration requirements configured on the account.

Client workforce roles, provisioning, and deprovisioning are managed by the client-assigned superuser account(s) or the client's Single Sign On (SSO) infrastructure.

Networking: Data Connectivity and Communications

Phreesia maintains documented Connectivity and Data Communications policies, standards, and procedures to guide personnel in documenting and implementing data connectivity and communications activities.

Phreesia manages its inbound network boundary through multi-layer firewalls, Web Application Firewalls (WAF), Network based Intrusion Detection (IDS), and load-balanced application pools. Inbound traffic is filtered through content delivery networks to help address DDOS traffic. Remote access is managed through Multi-Factor Authentication (MFA), bastion hosts, and reverse-proxy architecture.

Phreesia manages its lateral and outbound boundaries through web content filtering, access control lists (ACL), firewall monitoring, and multi-zone architecture. Phreesia connections across untrusted networks are encrypted via SSL 1.2 AES-256 2048.

Phreesia applies standard networking controls such as Network Address Translation (NAT), explicit port allocation, ACL, load balancers, firewall clusters, and site-to-site connectivity for redundant connectivity. Administrative access to network infrastructure is restricted to authorized employees from approved source IPs.

Phreesia data connectivity and communications data are classified and managed with an asset inventory system. Each asset is assigned to a department owner responsible for the connectivity and data. Network Operations works with asset owners to perform connectivity and communications operations and maintenance activities.

Software Development Life Cycle (SDLC) and Change Management

Phreesia maintains documented Change Control and Systems Development Life Cycle (SDLC) policies, standards, and procedures to guide personnel in documenting and implementing application and infrastructure change activities.

Change control procedures include change request and initiation processes, documentation requirements, development practices, quality assurance testing requirements, required approval procedures and rollout procedures.

A ticketing system is utilized to document the request and implementation of new changes in the application, operations, and infrastructure. Quality assurance testing and User Acceptance Testing results are documented and maintained with the associated change request. Development and testing are performed in an environment that is logically separated from the production environment. Management approves changes prior to migration to the production environment and documents those approvals within the ticketing system.

Version control software is utilized to maintain source code versions and migrate source code through the development process to the production environment. The version control software maintains a history of code changes to support rollback capabilities and tracks changes to developers.

Computer Operations - Backups

Systems Operations and Maintenance

Phreesia maintains documented Systems Operations policies, standards, and procedures to guide personnel in documenting and implementing systems operations activities.

Phreesia's technical operations teams manage and maintain internal systems to support operations, performance, and resiliency requirements. Phreesia's operational core competencies include:

- Configuration Management
- Data Connectivity and Communications
- Change Control and Systems Development Life Cycle (SDLC)
- Logical Access and Identity Infrastructure
- Computer Operations Availability and Monitoring
- Vulnerability Management
- Computer Operations Backups & Disaster Recovery

Phreesia maintains documented Systems Operations policies, standards, and procedures to guide personnel in documenting and implementing systems operations activities. Phreesia system resources are data classified and managed with an asset inventory system. Each asset is assigned to a department owner responsible for the system and data. Systems Operations works with asset owners to perform system operation and maintenance activities.

Computer Operations - Availability

System Availability and Monitoring

Phreesia maintains documented Availability and Monitoring policies, standards, and procedures to guide personnel in documenting and implementing availability and monitoring activities.

Phreesia monitors the capacity utilization of physical and computing infrastructure both internally and for clients to ensure that service delivery matches service-level agreements. Phreesia evaluates the need for additional infrastructure capacity in response to growth of existing clients and/or the addition of new clients. Infrastructure capacity monitoring includes, but is not limited to, the following infrastructure:

- Data center physical space
- Disk storage
- Network bandwidth
- Compute utilization

Phreesia uses an Endpoint Detection and Response provider for Managed Security Services (MSSP) support for monitoring laptop endpoints.

Phreesia ships operational logs to a centralized log aggregator where events are identified, correlated, and enriched for alerting notification and response teams. Logs are retained for 13 or more months as required. Phreesia has staffed a 24-hour security operations center (SOC) function.

All Phreesia users are trained annually through Phreesia's Privacy and Security training on how to recognize and report possible security and availability events. Incident response policies and procedures are in place to guide personnel to identify, report, and act upon cyber-incidents based upon job role. Response team investigation procedures are in place to triage and respond to security events. Incident Response operations are tested and trained regularly through tabletops and job-specific training.

System Configuration Management

Phreesia maintains documented Configuration Management policies, standards and procedures to guide personnel in documenting and implementing configuration management activities.

Phreesia maintains a standard baseline image for OS builds. This image is reviewed and refreshed regularly. Phreesia manages configuration as code and through documented deployment steps. Phreesia enforces configuration through group policy (GPO) and through Microsoft Intune for laptops. Phreesia's asset inventory is managed through a centralized asset inventory with tagging for application association, data classification and compliance scope.

Resiliency is built into the infrastructure supporting the data center services to help ensure that there is no single point of failure that includes firewalls, routers, servers, and connectivity. If a primary system fails, the secondary hardware is already configured to take its place.

System Vulnerability Management

Phreesia maintains documented Vulnerability Management policies, standards, and procedures to guide personnel in documenting and implementing vulnerability management activities.

Vulnerability scanning is performed by Phreesia on at least a monthly basis using industry leading vulnerability scanning tools from internal and external scanning sources. These technologies are customized to test the organization's infrastructure and software in an efficient manner while minimizing the potential risks associated with active scanning. Retests and on-demand scans are performed on an as-needed basis. Scanning tools that require installation in the Phreesia system are implemented through standard build templates. Scanning is performed with approved scanning templates and with bandwidth-throttling options enabled.

Penetration testing is conducted to measure the security posture of a target system or environment. Phreesia leverages internal staff and third-party vendors that use an accepted industry standard penetration testing methodology. Testing approach begins with a vulnerability analysis of the target system to determine what vulnerabilities exist on the system that can be exploited via a penetration test, simulating a disgruntled/disaffected insider or an attacker that has obtained internal access to the network. Once vulnerabilities are identified, attempts are made to exploit the vulnerabilities to determine whether unauthorized access or other malicious activity is possible. Penetration testing includes network- and application-layer testing, as well as testing of controls and processes around the networks and applications, and it occurs from both outside (external testing) and inside the network.

Phreesia has implemented a patch-management process to ensure contracted client and infrastructure systems are patched in accordance with vendor-recommended operating system patches. Phreesia system owners review proposed operating system patches to determine whether the patches are applied. Phreesia is responsible for determining the risk of applying or not applying patches based upon the security and availability impact of those systems and any critical applications hosted on them. Phreesia periodically scans the environment for vulnerabilities. Phreesia staff validate that patches have been installed and if applicable that reboots have been completed.

The Phreesia software operated at client sites is patched by Phreesia while the client operating systems are patch-managed by the client owner.

System Business Continuity & Disaster Recovery

Phreesia maintains documented Backup and Disaster Recovery policies, standards, and procedures to guide personnel in documenting and implementing backup and disaster recovery activities.

Client data is backed up and monitored by operations personnel for completion and exceptions. In the event of an exception, operations personnel perform troubleshooting to identify the root cause and then re-run the backup job immediately or as part of the next scheduled backup job, depending on client-indicated preference within the documented work instructions.

Backup data is physically secured within geographically separated Phreesia managed data centers and is encrypted at rest. The backup infrastructure is logically secured from other networks.

Phreesia backups are managed separately from the domain. They are stored offline and encrypted between the data centers. Phreesia restore capabilities are tested regularly.

Phreesia's business continuity and disaster recovery (BC/DR) plan is governed by Phreesia's Policies and Standards. Phreesia conducts annual BC/DR exercises, training, and tabletop scenarios throughout organizational management.

Boundaries of the System

The scope of this report includes Phreesia's Automated Patient Intake Platform Services System performed at various locations in the United States, Canada and India by personnel working remotely.

Phreesia is a 100% remote work company with employees in the US and Canada. Network, identity, and endpoint security controls are in place to secure the 100% remote work environment.

Phreesia leverages Rayden Design, a contractor with employees in Pune, India, to assist back-office and client support functions. Access to Phreesia is managed by Phreesia. A secured virtual desktop infrastructure (VDI) hosted in the US is required for access.

Phreesia leverages global code development partners. Code is reviewed, tested, and promoted by Phreesia. Global development partners do not have access to client data.

Phreesia's full workforce, including employees and authorized contractors, is subject to Phreesia's policies, procedures, technical controls, annual training, and ethical standards.

This report does not include the colocation services provided by Rackspace at the Somerset, New Jersey facility and by Equinix at the Ashburn, Virginia facility. This report also does not include the cloud hosting services provided by AWS, GCP, and Azure at various US facilities.

Changes to the System Since the Last Review

Phreesia is a product-led healthcare technology company. Phreesia is continuously improving its infrastructure, operations, and offerings. Some of those changes this year include:

- Launched automated Appointment Reminders to help reduce no-shows and get patients the care they need
- Debuted Phreesia PadX application that lets clients turn any iPad into a PhreesiaPad, giving them more flexibility and giving patients an easy, familiar way to check in for their appointments
- Upgraded the mobile payment workflows to support Apple Pay® and Google Pay™ transactions, which gives patients more convenient options to pay for their care
- Migrated to a next-generation data center that will keep Phreesia's platform reliable, adaptable, and scalable for the long term
- Worked with Phreesia's Latinx Employee Resource Group to prioritize patients' access to care and multi-language needs

Incidents Since the Last Review

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

Criteria Not Applicable to the System

All Common/Security, Availability and Confidentiality criterion were applicable to the Phreesia Automated Patient Intake Platform Services System.

Subservice Organizations

This report does not include the colocation services provided by Rackspace at the Somerset, New Jersey facility and by Equinix at the Ashburn, Virginia facility. This report also does not include the cloud hosting services provided by AWS, GCP, and Azure at various US facilities.

Subservice Description of Services

Rackspace and Equinix provide data center hosting services to Phreesia. AWS, GCP and Azure provide cloud hosting services to Phreesia. The services provided by Rackspace, Equinix, AWS, GCP and Azure include implementing physical security controls to protect the in-scope systems.

Complementary Subservice Organization Controls

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

The following subservice organization controls should be implemented by Rackspace to provide additional assurance that the trust services criteria described within this report are met:

Subservice Organization - Rackspace		
Category	**Criteria**	**Control**
Common Criteria/ Security	CC6.4	On an annual basis, Rackspace performs formal risk assessments over its Data Center services systems.
		Security guards are present at Rackspace data center facilities to monitor physical activity and to respond to security incidents.
		Rackspace data center facilities have an alarm system at exit and entry points to alert security personnel if a door is forced open or left open. Alerts are delivered to the Physical Security Team who follow up and document actions taken.
		Visitors at Rackspace facilities must check in with reception/security before being granted access to Rackspace facilities. Personnel and visitors are required to display their identity badges when onsite at Rackspace data center facilities. Unescorted visitors are not allowed in sensitive areas.
		Two factor authentication is used to gain access to the data center.
		Closed circuit video surveillance (CCTV) is monitored by authorized personnel 24X7. CCTV retention period is at least 90 days for data centers.
		Physical access (badge access/biometric access) events are logged and monitored in real time and alerts are generated and acted upon as appropriate. A Monthly review is conducted to identify unusual patterns. Action is taken to address any patterns discovered.
		Proximity cards are used at Rackspace data center facilities to restrict access to only authorized personnel.
		Physical safeguards are in place to restrict access to the server room within the data center.
		The visitor log is compiled and retained for 12 months. The log is reviewed in the case of incident or emergency situations.
		Appropriateness of physical access to Rackspace data center facilities is reviewed on a periodic basis.
		Physical access is disabled within the timeframe specified by the User Access Standard.
		At least annually Rackspace reviews third-party assurance reports or performs a physical security and environmental controls onsite audit for each leased data center location.
Availability	A1.2	On an annual basis, Rackspace performs formal risk assessments over its Data Center services systems.

Subservice Organization - Rackspace		
Category	**Criteria**	**Control**
		The data center facilities are equipped with redundant heating, ventilation, and air conditioning (HVAC) units to maintain consistent temperature and humidity levels.
		Redundant lines of communication exist to telecommunication providers.
		Data center facilities are equipped with uninterruptible power supplies (UPS) to mitigate the risk of short-term utility power failures and fluctuations.
		Data center facilities are equipped with diesel generators to mitigate the risk of long-term utility power failures and fluctuations.
		Rackspace utilizes fully redundant routing and switching equipment for its core network infrastructure.
		Data centers are equipped with sensors to detect environmental hazards, including smoke detectors where chilled water systems are used as coolant.
		The data center facilities are equipped with raised flooring.
		Data center facilities are equipped with fire detection and suppression systems.
		Fire detection systems, sprinkler systems, and chemical fire extinguishers are inspected at least annually.
		The UPS systems are inspected and/or serviced at least annually.
		Generators are tested at least every 120 days and serviced at least annually.
		A Data Center business continuity plan (BCP) exists and provides the global business continuity plan for Rackspace data centers to manage significant disruptions to its operations and infrastructure.
		Backups are scheduled and performed for customers who have subscribed to the managed backup service based on the backup frequency configured in the backup utility software.
		Customers subscribed to offsite retention have media sent to an offsite storage facility in a locked container.
		Backup tapes are securely destroyed when their useful life expires.
		Rackspace performs weekly monitoring of retention services.
		At least annually Rackspace reviews third-party assurance reports or performs a physical security and environmental controls onsite audit for each leased data center location.

The following subservice organization controls should be implemented by Equinix to provide additional assurance that the trust services criteria described within this report are met:

Subservice Organization - Equinix		
Category	**Criteria**	**Control**
Common Criteria/Security	CC6.4	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 datacenter facility is monitored 24x7 by security personnel.
Availability	A1.2	Datacenter Management team maintains datacenter-managed environmental equipment within the facility according to documented policy and maintenance procedures.
		Environmental controls have been implemented to protect systems inside datacenter facilities, including temperature and heating, ventilation, and air conditioning (HVAC) controls, fire detection and suppression systems, and power management systems.
		Datacenter physical security management reviews and approves the incident response procedures on a yearly basis. The incident security response procedures detail the appropriate steps to be taken in the event of a security incident and the methods to report security weaknesses.
		Critical Equinix components have been designed with redundancy to sustain isolated faults and minimize disruptions to customer services.
		Backup restoration procedures are defined and backup data integrity checks are performed through standard restoration activities.

The following subservice organization controls should be implemented by AWS to provide additional assurance that the trust services criteria described within this report are met:

Subservice Organization - AWS		
Category	**Criteria**	**Control**
Common Criteria / Security	CC6.4	Physical access to data centers is approved by an authorized individual.
		Physical access is revoked within 24 hours of the employee or vendor record being deactivated.
		Physical access to data centers is reviewed on a quarterly basis by appropriate personnel.
		Physical access points to server locations are recorded by closed circuit television camera (CCTV). Images are retained for 90 days, unless limited by legal or contractual obligations.
		Physical access points to server locations are managed by electronic access control devices.
Availability	A1.2	Amazon-owned data centers are protected by fire detection and suppression systems.
		Amazon-owned data centers are air conditioned to maintain appropriate atmospheric conditions. Personnel and systems monitor and control air temperature and humidity at appropriate levels.
		Uninterruptible power supply (UPS) units provide backup power in the event of an electrical failure in Amazon-owned data centers.
		Amazon-owned data centers have generators to provide backup power in case of electrical failure.
		Contracts are in place with third-party colocation service providers which include provisions to provide fire suppression systems, air conditioning to maintain appropriate atmospheric conditions, UPS units, and redundant power supplies.
		AWS performs periodic reviews of colocation service providers to validate adherence with AWS security and operational standards.
		Monitoring and alarming are configured by Service Owners to identify and notify operational and management personnel of incidents when early warning thresholds are crossed on key operational metrics.
		Incidents are logged within a ticketing system, assigned severity rating and tracked to resolution.
		Critical AWS system components are replicated across multiple Availability Zones and backups are maintained.
		Backups of critical AWS system components are monitored for successful replication across multiple Availability Zones.

The following subservice organization controls should be implemented by GCP to provide additional assurance that the trust services criteria described within this report are met:

Subservice Organization - GCP		
Category	**Criteria**	**Control**
Common Criteria / Security	CC6.4	Data center server floors network rooms and security systems are physically isolated from public spaces and/or delivery areas.
		Access to sensitive data center zones requires approval form authorized personnel and is controlled via badge access readers, biometric identification mechanism, and/or physical locks.
		Data center perimeters are defined and secured via physical barriers.
		Access lists to high security areas in data centers are reviewed on a periodic basis and inappropriate access is removed in a timely manner.
		Visitors to data center facilities must gain approval from authorized personnel, have their identity verified at the perimeter, and remain with an escort for the duration of the visit.
		Security measures utilized in data centers are assessed annually and the results are reviewed by executive management.
		Data centers are continuously staffed and monitored by security personnel through the use of real time video surveillance and/or alerts generated by security systems.
Availability	A1.2	Critical power and telecommunications equipment in data centers is physically protected from destruction and damage.
		Data centers are equipped with fire detection alarms and protection equipment.
		Redundant power is utilized to support the continued operation of critical data center equipment in the event of a loss of the primary power source(s).
		The organization conducts disaster recovery testing on an ongoing basis (and at least annually) to enable infrastructure and application teams to test communication plans, fail-over scenarios, operational transition, and other emergency responses. Participating teams create testing plans and document the results and lessons learned from the tests.

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

Subservice Organization - Azure		
Category	**Criteria**	**Control**
Common Criteria / Security	CC6.4	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 datacenter facility is monitored 24x7 by security personnel.
Availability	A1.2	Datacenter Management team maintains datacenter-managed environmental equipment within the facility according to documented policy and maintenance procedures.
		Environmental controls have been implemented to protect systems inside datacenter facilities, including temperature and heating, ventilation, and air conditioning (HVAC) controls, fire detection and suppression systems, and power management systems.
		Datacenter physical security management reviews and approves the incident response procedures on a yearly basis. The incident security response procedures detail the appropriate steps to be taken in the event of a security incident and the methods to report security weaknesses.
		Backups of key Azure service components and secrets are performed regularly and stored in fault tolerant (isolated) facilities.
		Critical Azure components have been designed with redundancy to sustain isolated faults and minimize disruptions to customer services.
		Customer data is automatically replicated within Azure to minimize isolated faults.
		Data Protection Services (DPS) backs up data for properties based on a defined schedule and upon request of the properties. Data is retained according to the data type identified by the property. DPS investigates backup errors and skipped files and follows up appropriately.

Subservice Organization - Azure		
Category	**Criteria**	**Control**
		Backup restoration procedures are defined and backup data integrity checks are performed through standard restoration activities.
		Offsite backups are tracked and managed to maintain accuracy of the inventory information.
		Production data is encrypted on backup media.
		Azure services are configured to automatically restore customer services upon detection of hardware and system failures.

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

- Requesting and approving Phreesia service ticket requests
- Holding periodic discussions with vendors and subservice organizations
- Reviewing attestation reports over services provided by vendors and subservice organizations
- Monitoring external communications, such as customer complaints relevant to the services by the subservice organization

COMPLEMENTARY USER ENTITY CONTROLS

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

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

1. User entities are responsible for physical security of Phreesia devices and components deployed to user entity managed locations.
2. User entities are responsible for ensuring the supervision, management, and control of the use of Phreesia services by their personnel.
3. User entities should establish controls to ensure that access to user organization' systems and applications is adequately restricted to authorized personnel.
4. User entities are responsible for immediately notifying Phreesia of any actual or suspected information security breaches that may impact Phreesia services or data stored within Phreesia, including compromised user accounts and accounts used for integrations and secure file transfers.
5. User entities are responsible for notifying Phreesia of changes made to technical or administrative contact information.
6. User entities are responsible for maintaining their own system(s) of record, and to establish controls that ensure all data transmitted by the user entity to Phreesia is complete, accurate, timely, and protected.

7. Controls should be established to ensure that output data generated by Phreesia is reviewed by the user entity for accuracy.
8. Controls should be established to ensure that transactions are appropriately authorized, complete, and accurate.
9. User entities are responsible for developing their own disaster recovery and business continuity plans that address the inability to access or utilize Phreesia services.
10. User entities are responsible for providing Phreesia with a list of approvers for security and system configuration changes for data transmission.
11. User entities are responsible for establishing controls to ensure that all changes to client contracts and policy changes are appropriately authorized, accurate, and communicated to Phreesia in a timely manner.
12. User entities are responsible for understanding and complying with their contractual obligations to Phreesia.