proteus®
DIGITAL HEALTH

PROTEUS DIGITAL HEALTH, INC.

INDEPENDENT SERVICE AUDITOR'S SOC 3 REPORT FOR THE DISCOVER AND PMG CLOUD SYSTEMS

FOR THE PERIOD OF AUGUST 1, 2018, TO JANUARY 31, 2019

Attestation and Compliance Services

schellman
Quality, above all.

INDEPENDENT SERVICE AUDITOR'S REPORT

To Proteus Digital Health, Inc.:

Scope

We have examined Proteus Digital Health, Inc.'s ("Proteus") accompanying assertion titled "Assertion of Proteus Digital Health, Inc. Service Organization Management" ("assertion") that the controls within Proteus' Discover and PMG Cloud systems ("system") were effective throughout the period August 1, 2018, to January 31, 2019, to provide reasonable assurance that Proteus' 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 (AICPA, Trust Services Criteria)***.**

Proteus uses a subservice organization for cloud hosting services. The description of the boundaries of the system indicates that complimentary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Proteus, to achieve Proteus' service commitments and system requirements based on the applicable trust services criteria. The description of the boundaries of the system does not disclose the actual controls at the subservice organization. Our examination did not include the services provided by the subservice organization, and we have not evaluated the suitability of the design or operating effectiveness of such complimentary subservice organization controls.

Service Organization's Responsibilities

Proteus 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 Proteus' service commitments and system requirements were achieved. Proteus has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, Proteus 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 whether 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 systems requirements were achieved based on the applicable trust services criteria. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether 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 controls were not effective to achieve Proteus' service commitments and system requirements based on the applicable trust services criteria; and
- Performing procedures to obtain evidence about whether controls within the system were effective to achieve Proteus' 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.

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 Proteus' service commitments and system requirements were achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the 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 Proteus' Discover and PMG Cloud systems were effective throughout the period August 1, 2018, through January 31, 2019, to provide reasonable assurance that Proteus' service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects

Schellman & Company, LLC

Tampa, Florida
March 13, 2019

ASSERTION OF PROTEUS SERVICE ORGANIZATION MANAGEMENT

We are responsible for designing, implementing, operating, and maintaining effective controls within Proteus Digital Health, Inc.'s ("Proteus") Discover and PMG Cloud systems ("system") throughout the period August 1, 2018, to January 31, 2019, to provide reasonable assurance that Proteus' service commitments and system requirements relevant to security, availability, and confidentiality were achieved. Our description of the boundaries of the system is presented below 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 August 1, 2018, to January 31, 2019, to provide reasonable assurance that Proteus' 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 (AICPA, Trust Services Criteria)*. Proteus' objectives for the system in applying the applying the applicable trust services criteria are embodied in its service commitments and systems requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented below.

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 August 1, 2018, to January 31, 2019, to provide reasonable assurance that Proteus' service commitments and systems requirements were achieved based on the applicable trust services criteria.

System Description of the Discover and PMG Cloud Systems

Company Background

Proteus was founded in 2001 and is headquartered in Redwood City, California. Proteus develops digital health products that collect and aggregate behavioral, physiologic, and therapeutic metrics into personal management tools delivered to the mobile devices of consumers.

Armed with more than 400 issued patents, Proteus is in the process of establishing a field called digital medicines – a new category in healthcare that aims to assist physicians and patients in improving treatment outcomes through medication adherence. A digital medicine includes the following features:

- Widely used medicines that have been formulated to trigger alerts when they have been swallowed.
- A wearable patch that detects alerts sent by swallowed medicines and captures physiologic response.
- Mobile applications to support patient self-care and physician decision-making.
- Data analytics to serve the needs of health system managers.

Currently, digital medicines are commercially available in the United States. Data from both randomized clinical trials and real-world use demonstrate that patients have significantly improved outcomes using digital medicines and that these outcomes can be sustained. In conjunction with participation from health systems and pharmaceutical companies, Proteus' digital solution is presented to healthcare providers with a goal of better insight into patient health, optimized therapies, and lower costs.

Description of Services Provided

Discover

Proteus Discover is comprised of ingestible sensors, a small wearable sensor patch, an application on a mobile device, a cloud-based event processing and data storage, and a web-based provider portal. Once activated, Discover unlocks never-before-seen insights into patient health patterns and medication treatment effectiveness, leading to more informed healthcare decisions for everyone involved. Data collected in the smartphone app can be transmitted by the patient to the backend servers, where they are available for analysis and interpretation through the physician portal. The ingestible and wearable components are out of scope since there is no personal health information (PHI) affected by those devices.

Proteus Medical Group (PMG) Cloud

Health system partners transmit aggregated information from Proteus devices to the PMG Cloud. Proteus' PMG Cloud utilizes electronic personal health information (ePHI), PHI, and personal health records (PHR) provided by health system partners. Information is de-identified by PMG Cloud personnel upon receipt from health system partners. The information is subsequently summarized to provide analytics utilized by health system partners to identify and evaluate trends within their patient populations.

System Boundaries

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

[Intentionally Blank]

Principle Service Commitments and System Requirements

Proteus communicates security, availability, and confidentiality commitments to customers in written individualized agreements and statements published on its web portal. Customers are required to sign an agreement prior to using Proteus product offerings.

Proteus maintains its information technology (IT) infrastructure and product offerings through Amazon Web Services, Inc (AWS). Therefore, Proteus relies on AWS service commitments related to file backups, retention, business continuity and disaster recovery planning, and availability requirements. Proteus identifies AWS as a vendor critical to business operations and reviews AWS service agreements and relevant third party assessments on at least annual basis to ensure alignment of AWS commitments to Proteus operational and business objectives.

Proteus develops, maintains, and as necessary in the event of business interruption, executes a business continuity plan. Proteus maintains adequate backup files of customer data and all programs utilized to process customer data in order to execute business continuity plans.

Proteus established confidentiality commitments related to the protection of confidential information from unauthorized access or use, restricted disclosure of confidential information to authorized parties, changes to confidentiality commitments, and data retention. Proteus maintains confidentiality agreements with parties prior to exchange of information classified as confidential. These parties may include, but are not limited to, customers, third parties, employees, and contractors. Further, customer data classified as protected health information (PHI) or personal health records (PHR) are disposed in accordance with documented data retention policy. Per the data retention and disposal policy, Proteus retains and disposes customer data per its regulatory requirements. Those requirements are also communicated through contracts with customers.

In addition, Proteus has put in place a process for sanitizing mobile devices that may contain PHR. When a patient rolls off from the clinic, the clinic collects Proteus-provided devices from the patient and sends to Proteus facility in Hayward, California. Upon receipt of the devices, Proteus sanitizes the devices in accordance with documented data sanitization procedures.

Infrastructure and Software

The production infrastructure is hosted by AWS comprised of managed services. Proteus does not own or maintain any of the hardware located in the AWS data centers, and operates under a shared security responsibility model, where AWS is responsible for the security of the underlying cloud infrastructure including physical infrastructure, geographical regions, availability zones, and edge locations. Proteus is responsible for securing the platform deployed in AWS such as customer data, applications, identity access management, network security group configuration, and network traffic and server-side encryption.

Proteus technology is based on a multi-tenant architecture that applies common, consistent management practices for its customers. The infrastructure has been designed to provide a reliable, scalable, and highly available platform. Proteus has multiple zones set up across regions to ensure the availability of its services. Proteus leverages AWS for data storage and data redundancy.

People

- Executive management and board of directors – responsible for overseeing company-wide activities, establishing business and strategic objectives.
- Human resources (HR) – responsible for establishing employee behavioral policies, acquiring and retaining competent individuals, and monitoring training to maintain and advance skillsets.
- IT – responsible for monitoring and providing service and support to the information resources throughout the enterprise.

- Privacy and security – responsible for establishing privacy and security policies, performing risk assessment, monitoring and addressing security issues and incidents throughout the enterprise.
- Legal – responsible for providing legal counsel and review on matters pertaining to privacy and security, intellectual property, master service agreements (MSAs), nondisclosure agreements (NDAs), and statement of work (SOWs).

Procedures

Access Authentication and Authorization

Proteus employees are required to access the corporate network and in-scope systems through their unique login credentials comprised of a username and password. For all Proteus in-scope systems and applications, passwords have been configured for minimum length and specific character requirements. Administrator privileges to in-scope systems are restricted to limited number of personnel and granted based on job responsibilities. At least on an annual basis, user access reviews are performed to recertify access restrictions.

Access Requests and Access Revocation

Proteus established an enterprise IT security policy that outlines the process for access provisioning, administration, and management. When a new employee is hired and has accepted a position at Proteus, user access provisioning and onboarding requirements are documented using an automated ticketing system. Access requests require approval from the new employee’s manager for processing by IT.

Employee status changes including termination are initiated by the employee’s manager and approved by HR. Upon notification of an employee termination by HR, an automated ticketing system is utilized to initiate and document off-boarding activities.

Change Management

Changes to the applications and infrastructure supporting in-scope applications follow a formal change control policy to ensure that only authorized changes are implemented into the production environment.

Changes are documented and tracked in a ticketing system to ensure review and approval prior to deployment to production and to enable effective coordination and communication between business and developers. Change development activities are completed in a development environment separated from testing and production environments. Once change development activities are completed, the change is pushed to a testing environment for quality assurance review and approval. Proteus utilizes dummy data in the development and testing environment to ensure protection of confidential customer data during the change management process.

A change control board (CCB), comprised of cross-functional members, is established to govern the planned change activities and evaluate the potential impact. Prior to implementing changes into the production environment, change documentation is reviewed by the CCB to validate that testing was performed and potential impact due to code changes has been analyzed. Version control software is in place and utilized if the change implementation results in unintended outcomes or adversely impact the production environment.

Data Backup and Disaster Recovery

Data backup, replication, and recovery policies and procedures are in place to communicate roles and responsibilities to relevant personnel and to ensure systems are replicated in a timely manner and securely stored in order to preserve the integrity of customer files. Proteus utilizes an automated backup system to perform backups of the production databases on a periodic basis. The backup system is configured to notify IT security of backup job failures. In the event of a backup job failure, IT security personnel investigates the alerts and resolves issues as needed.

In addition, Proteus established a disaster recovery plan and it is tested on an annual basis. The disaster recovery plan guides personnel in business continuity plan activation and strategies for restoring critical business functions. IT personnel perform backup restoration testing as part of annual disaster recovery plan exercise to ensure critical backup data are available in the event of business disruption.

Incident Response

Proteus has implemented an incident response policy that is provided to employees. Incident response procedures are established and distributed to operations personnel in charge of carrying out the procedures.

Network operations centers are staffed 24 hours per day to respond to incidents and events. An automated ticketing system and e-mail communications are utilized to document and track resolution of incidents noted.

System Monitoring

Vulnerability assessments and network penetration testing are performed by IT personnel and third-party vendors on at least annual basis. Results of the assessments are reviewed in security meetings with management and remediation plans are proposed and monitored through resolution. In addition, IT personnel review security groups rulesets on a quarterly basis.

Documented system logging and auditing policies and procedures are in place to guide personnel in review of records and information system activities. The in-scope systems are configured to log access related events.

An enterprise monitoring application is utilized to monitor system performance and configured to send automated alerts to IT personnel when predefined thresholds have been exceeded. In addition, an intrusion detection system is utilized to analyze and report network events and to report possible or actual network security breaches to IT personnel. Incidents identified as a result of system monitoring or scanning are documented and tracked through resolution within an automated ticketing system.

Data

The following table describes the information used and supported by the system.

Data Used and Supported by the System		
Data Description	**Data Reporting**	**Classification**
Customer health data	Encrypted storage and limited access; available to customers upon request	Confidential

Subservice Organizations

The cloud hosting services provided by AWS were not included within the scope of this examination. The following table presents the applicable Trust Services criteria that are intended to be met by controls at AWS, alone or in combination with controls at Proteus, and the types of controls expected to be implemented at AWS to meet those criteria.

Control Activity Expected to be Implemented by AWS	Applicable Trust Services Criteria
AWS is responsible for ensuring implemented controls to manage logical access to the underlying network and virtualization management software for their cloud hosting services where production systems reside.	CC6.1 – CC6.3 CC6.5 – CC6.7 CC7.2
AWS is responsible for ensuring implemented controls for restricting physical access to data center facilities, backup media, and other system components including firewalls, routers, virtualization, and storage infrastructure where production systems reside.	CC6.4, CC7.2
AWS is responsible for ensuring the ability to read and recover data from physical assets has been diminished prior to the discontinuation of logical and physical protections.	CC6.5

Control Activity Expected to be Implemented by AWS	Applicable Trust Services Criteria
AWS is responsible for ensuring capacity demand controls are in place to meet Proteus' availability commitments and requirements.	A1.1
AWS is responsible for ensuring environmental protection controls are in place to meet Proteus' availability commitments and requirements.	A1.2