Doximity
Type 2 SOC 3
2020

SOC 3 FOR SERVICE ORGANIZATIONS REPORT

April 1, 2020 To June 30, 2020

Table of Contents

SECTION 1

ASSERTION OF DOXIMITY MANAGEMENT

ASSERTION OF DOXIMITY MANAGEMENT

July 20, 2020

We are responsible for designing, implementing, operating, and maintaining effective controls within Doximity's ('the Company') Healthcare Networking & Communications Platform System throughout the period April 1, 2020 to June 30, 2020, to provide reasonable assurance that Doximity's service commitments and system requirements relevant to Security, Availability and Confidentiality (applicable trust services criteria) were achieved. Our description of the boundaries of the system is presented below in "Doximity's Description of Its Healthcare Networking & Communications Platform System throughout the period April 1, 2020 to June 30, 2020" 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 April 1, 2020 to June 30, 2020, to provide reasonable assurance that Doximity'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, Confidentiality, Processing Integrity and Privacy* (AICPA, *Trust Services Criteria*). Doximity's objectives for the system in applying 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 "Doximity's Description of Its Healthcare Networking & Communications Platform System throughout the period April 1, 2020 to June 30, 2020".

Doximity uses Amazon Web Services ('AWS' or 'subservice organization') 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 Doximity, to achieve Doximity's service commitments and system requirements based on the applicable trust services criteria. The description presents Doximity's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Doximity's controls. The description does not disclose the actual controls at the subservice organization.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary to achieve Doximity'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 Doximity'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 April 1, 2020 to June 30, 2020 to provide reasonable assurance that Doximity's service commitments and system requirements were achieved based on the applicable trust services criteria.

Jey Balachandran

Jey Balachandran
Chief Technology Officer
Doximity

SECTION 2

INDEPENDENT SERVICE AUDITOR'S REPORT

INDEPENDENT SERVICE AUDITOR'S REPORT

To: Doximity

Scope

We have examined Doximity's accompanying description of Healthcare Networking & Communications Platform System titled "Doximity's Description of Its Healthcare Networking & Communications Platform System throughout the period April 1, 2020 to June 30, 2020" (description) based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (AICPA, *Description Criteria*), (description criteria) and the suitability of the design and operating effectiveness of controls stated in the description throughout the period April 1, 2020 to June 30, 2020, to provide reasonable assurance that Doximity'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* (AICPA, *Trust Services Criteria*).

Doximity uses AWS 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 Doximity, to achieve Doximity's service commitments and system requirements based on the applicable trust services criteria. The description presents Doximity's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Doximity's controls. The description does not disclose the actual controls at the subservice organization. Our examination did not include the services provided by the subservice organization, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

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

Doximity 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 Doximity's service commitments and system requirements were achieved. Doximity has provided the accompanying assertion titled "Assertion of Doximity Management" (assertion) about the description and the suitability of design and operating effectiveness of controls stated therein. Doximity is also responsible for preparing the description and assertion, including the completeness, accuracy, and method of presentation of the description and assertion; providing the services covered by the description; selecting the applicable trust services criteria and stating the related controls in the description; and identifying the risks that threaten the achievement of the service organization's service commitments and system requirements.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the description and on the suitability of design and operating effectiveness of controls stated in the description based on our examination. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants.

Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, the description is presented in accordance with the description criteria and the controls stated therein were suitably designed and operated effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

An examination of the description of a service organization's system and the suitability of the design and operating effectiveness of controls involves the following:

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

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

Inherent Limitations

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

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

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements are achieved based on the applicable trust services 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 Doximity's Healthcare Networking & Communications Platform System were suitably designed and operating effectively throughout the period April 1, 2020 to June 30, 2020, to provide reasonable assurance that Doximity's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

The SOC logo for Service Organizations on Doximity'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 Doximity, user entities of Doximity's Healthcare Networking & Communications Platform System during some or all of the period April 1, 2020 to June 30, 2020, business partners of Doximity subject to risks arising from interactions with the Healthcare Networking & Communications Platform System, and those who have sufficient knowledge and understanding of the complementary user entity controls and complementary subservice organization controls and how those controls interact with the controls at the service organization to achieve the service organization's service commitments and system requirements.

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 20, 2020

SECTION 3

DOXIMITY'S DESCRIPTON OF ITS HEALTHCARE NETWORKING & COMMUNICATIONS PLATFORM SYSTEM THROUGHOUT THE PERIOD APRIL 1, 2020 TO JUNE 30, 2020

OVERVIEW OF OPERATIONS

Company Background

Founded in 2011, Doximity is the nation's largest community of verified healthcare professionals with over one million members, including 70% of all doctors and 45% of all nurse practitioners and physician assistants in the US. Doximity's mission is to help providers be more productive, informed and connected. Headquartered in San Francisco, Doximity currently has over 400 full-time employees.

Description of Services Provided

Doximity's mission is to help providers be more productive, informed and connected. Doximity leverages a mobile-first development philosophy to help physicians, nurse practitioners, and physician assistants connect with other healthcare professionals, securely collaborate on patient treatment, grow their practices, and discover new career opportunities.

Doximity allows healthcare professionals to easily stay connected and current through the following features:

- Telehealth - allows healthcare professionals to conduct secure voice and video visits with a customized Caller ID
- Healthcare Provider Directory - allows healthcare professionals to search, find, and reach any other healthcare provider, instantly
- Earn CME/CE - allows healthcare professionals to submit and track credits when ready
- Career Opportunities - allows healthcare professionals to compare salaries and research jobs
- News - allows healthcare professionals to stay up to date on the latest clinical news most relevant to their practice

Principal Service Commitments and System Requirements

Doximity's platform allows healthcare professionals to securely communicate while maintaining compliance with the Health Insurance Portability and Accountability Act of 1996 (HIPAA), as amended by the Health Information Technology for Economic and Clinical Health Act (HITECH). All Doximity employees and contractors who work on the systems that facilitate healthcare communications are required to complete ongoing HIPAA and security training.

Doximity's team of security professionals ensure that the platforms and data are always protected. Doximity conducts a variety of recurring security processes such as risk assessments, penetration testing (using internal testers and external firms), and white-box testing (with security researchers and security professionals).

Doximity employs industry-leading encryption standards to protect all data in transit and at rest. All requests are made over Transport Layer Security (TLS) technology. Video call media is encrypted on transmission over a Datagram Transport Layer Security/Secure Real-time Transport Protocol (DTLS/SRTP) connection. Personal Health Information (PHI) is encrypted at rest using 256-advanced encryption standard (AES) and any databases containing PHI are further encrypted.

Components of the System

Infrastructure

Primary infrastructure used to provide Doximity's Healthcare Networking & Communications Platform System includes the following:

Primary Infrastructure		
Hardware	**Type**	**Purpose**
Amazon Elastic Compute Cloud	Varies by workload type	Major types of workload: • Web request service • Workload processing
Amazon Simple Storage Service	Infrastructure as a Service (IaaS)	Storage
Amazon Aurora & RDS	IaaS	Database
Amazon VPC	IaaS	Resource isolation
Elastic Load Balancing	IaaS	Load balancing
AWS Identity and Access Management	IaaS	Security and access
Amazon Elastic MapReduce	IaaS	Data processing and analysis
AWS Key Management Service	IaaS	Cryptographic key creation and management

Software

Primary software used to provide Doximity's Healthcare Networking & Communications Platform System includes the following:

Primary Software		
Software	**Operating System**	**Purpose**
Chef & Terraform	Linux	Manage and deploy configuration management of the production systems and infrastructure services
GitHub	SaaS	Project and change management tool and manages source code versions during development
CircleCI	SaaS	Automated testing and deployment of changes to the system
Sensu	Linux	Monitoring for system availability and capacity
Sumo Logic	SaaS	Monitor and logging

People

Doximity's executive management includes:

- The CEO, who is responsible for leading and overseeing overall company operations, including sales activities and managing the day-to-day operations of Doximity
- The CTO, who is responsible for oversight of IT related hardware, software, configuration, and security
- SVP of Engineering, who is responsible for the design, implementation, and technical components of the application
- CCO, who is responsible for sales, business development, and marketing activities
- CFO, who is responsible for finance
- Director of People Ops, who is responsible for hiring, onboarding, compensation, termination, conflict resolution, and other back office tasks

Doximity has a staff of over 400 employees organized into the following functional areas:

- Sales, Marketing and Account Management: Responsible for communicating with, onboarding and educating clients and users regarding the use of the system
- Operations: Includes customer service representatives who assist users with issues and make configuration changes at the request of individual users. Also includes Information Technology Services representatives responsible for configuring and maintaining internal systems
- Research and Development: Responsible for the development of new features and functionality within Doximity systems. This includes:
    - Development Operations: responsible for systems configuration and infrastructure
    - Engineering: responsible for software development and design
    - Design: responsible for designing user experience and interfaces
    - Quality Assurance: responsible for software testing and quality controls
    - Analysis: responsible for monitoring and analyzing metrics
    - Product: responsible prioritization and project management

Data

All data contained and/or created by and/or for Doximity systems use. Which include but not limited to:

- Error logs
- Access logs
- User Information

Is maintained securely and encrypted where needed with industry standard encryption. Transferred within secure networks and actively managed and confirmed for accuracy. Security and thorough deletion when it is no longer needed for the proper function of Doximity systems.

Processes, Policies and Procedures

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

Boundaries of the System

The scope of this report includes the Healthcare Networking & Communications Platform System performed in the San Francisco, California facilities.

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

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 period.

Incident in the Last 12 Months

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

Criteria Not Applicable to the System

All Common, Availability and Confidentiality criterion were applicable to the Doximity Healthcare Networking & Communications Platform System.

Subservice Organizations

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

Subservice Description of Services

AWS provides a suite of cloud hosting and computing services, including data and application hosting, as well as automated backup services to customers internationally.

Complementary Subservice Organization Controls

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

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 - Amazon Web Services		
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.

Subservice Organization - Amazon Web Services		
Category	**Criteria**	**Control**
		Electronic intrusion detection systems are installed within data server locations to monitor, detect, and automatically alert appropriate personnel of security incidents.
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, Uninterruptible Power Supply (UPS) units, and redundant power supplies.
		AWS performs periodic reviews of colocation service providers to validate adherence with AWS security and operational standards.
		S3-Specific - S3 performs continuous integrity checks of the data at rest. Objects are continuously validated against their checksums to prevent object corruption.
		S3-Specific - When disk corruption or device failure is detected, the system automatically attempts to restore normal levels of object storage redundancy.
		S3-Specific - Objects are stored redundantly across multiple fault-isolated facilities.
		S3-Specific - The design of systems is sufficiently redundant to sustain the loss of a data center facility without interruption to the service.
		RDS-Specific - If enabled by the customer, RDS backs up customer databases, stores backups for user-defined retention periods, and supports point-in-time recovery.
		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.

Subservice Organization - Amazon Web Services		
Category	**Criteria**	**Control**
		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.

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

- Holding periodic discussions with vendors and subservice organization
- Reviewing attestation reports over services provided by vendors and subservice organization

COMPLEMENTARY USER ENTITY CONTROLS

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

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

1. User entities are responsible for understanding and complying with their contractual obligations to Doximity.
2. User entities are responsible for notifying Doximity of changes made to technical or administrative contact information.
3. User entities are responsible for ensuring the supervision, management, and control of the use of Doximity services by their personnel.
4. User entities are responsible for developing their own disaster recovery and business continuity plans that address the inability to access or utilize Doximity services.
5. User entities are responsible for providing Doximity with a list of approvers for security and system configuration changes for data transmission.
6. User entities are responsible for immediately notifying Doximity of any actual or suspected information security breaches, including compromised user accounts.
7. User entities are responsible for understanding and complying with Doximity's Terms of Service and Privacy Policy.