



**A-LIGN**

Doximity

Type 2 SOC 3

2023



# **SOC 3 FOR SERVICE ORGANIZATIONS REPORT**

**August 1, 2023 to October 31, 2023**

## Table of Contents

<b>SECTION 1 ASSERTION OF DOXIMITY MANAGEMENT .....</b>	<b>1</b>
<b>SECTION 2 INDEPENDENT SERVICE AUDITOR’S REPORT .....</b>	<b>3</b>
<b>SECTION 3 DOXIMITY’S DESCRIPTION OF ITS HEALTHCARE COMMUNICATIONS &amp; NETWORKING PLATFORM SERVICES SYSTEM THROUGHOUT THE PERIOD AUGUST 1, 2023 TO OCTOBER 31, 2023 .....</b>	<b>7</b>
OVERVIEW OF OPERATIONS.....	8
Company Background .....	8
Description of Services Provided .....	8
Principal Service Commitments and System Requirements.....	8
Components of the System.....	9
Boundaries of the System.....	13
Changes to the System Since the Last Review.....	13
Incidents Since the Last Review .....	13
Trust Services Criteria and HIPAA/HITECH Requirements Not Applicable to the System ..	14
Subservice Organizations .....	14
COMPLEMENTARY USER ENTITY CONTROLS.....	17

**SECTION 1**

**ASSERTION OF DOXIMITY MANAGEMENT**

## ASSERTION OF DOXIMITY MANAGEMENT

December 12, 2023

We are responsible for designing, implementing, operating, and maintaining effective controls within Doximity's ('the Company') Healthcare Communications & Networking Platform Services System throughout the period August 1, 2023 to October 31, 2023, 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* in AICPA, *Trust Services Criteria*. Our description of the boundaries of the system is presented below in "Doximity's Description of Its Healthcare Communications & Networking Platform Services System throughout the period August 1, 2023 to October 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 August 1, 2023 to October 31, 2023, to provide reasonable assurance that Doximity's service commitments and system requirements were achieved based on the trust services criteria. Doximity'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 "Doximity's Description of Its Healthcare Communications & Networking Platform Services System throughout the period August 1, 2023 to October 31, 2023".

Doximity uses Amazon Web Services, Inc. ('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 August 1, 2023 to October 31, 2023 to provide reasonable assurance that Doximity'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 Doximity's controls operated effectively throughout that period.



---

Alex Schlick  
Sr. Director of Accounting  
Doximity

**SECTION 2**  
**INDEPENDENT SERVICE AUDITOR'S REPORT**



## INDEPENDENT SERVICE AUDITOR'S REPORT

To: Doximity

### *Scope*

We have examined Doximity's accompanying assertion titled "Assertion of Doximity Management" (assertion) that the controls within Doximity's Healthcare Communications & Networking Platform Services System were effective throughout the period August 1, 2023 to October 31, 2023, 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* in 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 also provided the accompanying assertion (Doximity assertion) about the effectiveness of controls within the system. When preparing its assertion, Doximity 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 Doximity's Healthcare Communications & Networking Platform Services System were suitably designed and operating effectively throughout the period August 1, 2023 to October 31, 2023, 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, if complementary subservice organization controls and complementary user entity controls assumed in the design of Doximity's controls operated effectively throughout that period.

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 Communications & Networking Platform Services System during some or all of the period August 1, 2023 to October 31, 2023, business partners of Doximity subject to risks arising from interactions with the Healthcare Communications & Networking 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  
December 12, 2023

### **SECTION 3**

#### **DOXIMITY'S DESCRIPTION OF ITS HEALTHCARE COMMUNICATIONS & NETWORKING PLATFORM SERVICES SYSTEM THROUGHOUT THE PERIOD AUGUST 1, 2023 TO OCTOBER 31, 2023**

## **OVERVIEW OF OPERATIONS**

### **Company Background**

Founded in 2010, Doximity is the nation's largest community of verified healthcare professionals with over 2 million members, including 80% of all doctors and 50% 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 900 full-time employees.

### **Description of Services Provided**

Our mission is to help every clinician be more productive and provide better care for their patients. We are clinicians-first, putting technology to work for doctors instead of the other way around. That guiding principle has enabled Doximity to become an essential and trusted professional platform for clinicians. Our cloud-based platform provides our members with tools specifically built for medical professionals, enabling them to collaborate with their colleagues, securely coordinate patient care, conduct virtual patient visits, stay up-to-date with the latest medical news and research, and manage their careers.

Doximity's cloud-based platform puts modern software tools in the hands of physicians and other medical professionals. Our members have come to rely on us to help them efficiently manage their workday. At the core of our platform is the largest medical professional network in the nation, which creates proximity within our community of doctors and hundreds of thousands of other medical professionals. Our verified member profiles digitize the traditional curriculum vitae, highlighting clinical expertise and reflecting the unique training, certifications, research, and employment affiliations that differentiate medical professionals. Our members can search and connect with colleagues and specialists, which allows them to better coordinate patient care and streamline referrals. In addition, they can discover career opportunities unique to their clinical skill sets.

We support clinicians in an era of information overload, by solving signal-to-noise challenges with our news tools. Our newsfeed addresses the ever-increasing sub-specialization of medical expertise and volume of medical research by delivering news and information that is relevant to each individual clinician's patient population, clinical practice, and professional relationships.

We support clinicians in their day-to-day practice of medicine with mobile-friendly and easy-to-use clinical workflow tools such as voice and video telehealth, secure messaging, digital faxing and a suite of AI-powered tools that help physicians with a range of clinician and administrative tasks. In 2022, we acquired Amion to bring on-call scheduling and communication to the Doximity platform. Our focus on clinician-centric product design and productivity has led to high levels of health professional adoption and endorsement.

### **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). Doximity employees and contractors who work on Doximity systems that facilitate healthcare communications are required to complete ongoing HIPAA and security training.

Doximity's team of security professionals ensure that Doximity 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 data in transit and at rest. Requests are made over Transport Layer Security (TLS) technology. Video call media is encrypted on transmission over a DTLS/SRTP connection. Personal Health Information (PHI) is encrypted at rest using 256-AES encryption and any databases containing PHI are further encrypted.

## Components of the System

### Infrastructure

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

Primary Infrastructure		
Hardware	Type	Purpose
Amazon Aurora	Infrastructure as a Service (IaaS)	Databases leveraged by web applications
Amazon EKS	IaaS	Web application and workload processing services
Amazon S3	IaaS	Storage of assets and logs
Amazon VPC	IaaS	Resource isolation and security
Amazon ELB	IaaS	Load balancing
Amazon IAM	IaaS	Identify and access, management
Amazon EMR	IaaS	Data processing and analysis
Amazon KMS	IaaS	Cryptographic key creation and management
Amazon Shield	IaaS	Managed DDoS protection

### Software

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

Primary Software		
Software	Operating System	Purpose
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
Snowflake	SaaS	Data warehousing and analysis
SumoLogic & Loki	SaaS	Monitor and logging

## *People*

Doximity's executive management includes:

- The CEO, who is responsible for leading and overseeing overall company operations
- The CTO, who is responsible for oversight of IT related hardware, software, configuration, and security
- The CFO, who is responsible for finance
- SVP of Engineering, who is responsible for the design, implementation, and technical component of the application
- SVP of Product, who is responsible for product ideation and delivery
- General Counsel, who is responsible for legal compliance matters
- VP of People Ops, who is responsible for hiring, onboarding, compensation, termination, conflict resolution, and other back-office tasks

Doximity has a staff of over 900 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. 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.

## Physical Security

The in-scope system and supporting infrastructure is hosted by AWS. As such, AWS is responsible for the physical security controls for the in-scope system. Refer to the "Subservice Organizations" section below for the controls in place around physical security.

## Logical Access

Identity and Access Management to systems is managed by Okta. Okta's source of truth for user accounts as well as user-level attributes is Workday, Doximity's Human Resources Information System ('HRIS'). The HR Team is in control of who is an employee/contractor and will receive an Okta account, as well as what team, department, division, and attribute updates.

Accounts are imported/updated hourly from Workday to Okta, and new employee accounts are included in the automated import process and created five days before their start date. The Okta account activation takes place the morning of an employee's start date.

Upon activation, Okta user accounts are required to set a secure 16-digit password and must conform to defined password complexity requirements and age limits that are enforced by Okta. Employees & contractors are also required to activate a multi-factor authentication device (Okta Verify mobile app with push notifications) on their Okta user account. MFA is required to login to Okta and is enforced when authenticating with some of Doximity's more sensitive infrastructure platforms.

All actions taken within Okta are logged and includes behavior detection thresholds that will alert Okta administrators of suspicious activity (new city, country, device, IP, or "impossible location" as compared to previous 20 auth attempts). Okta accounts will automatically lock out a user after 6 incorrect credentials or failed MFA attempts. A locked-out user is required to contact IT support to verify their identity by video call and have an Okta administrator unlock their account and reset their password.

Administrative access to Okta is limited to members of Doximity's IT team and select members of the Infrastructure Security team. Those admins have various levels of administrative capabilities related to their role and responsibilities.

All SaaS platforms are integrated with Okta (for single sign on capability) using SAML 2.0 authentication and are accessed via TLS technology. Role-based access to applications is managed via group memberships within Okta and Okta Group membership is defined by a set of group rules that evaluate each Okta user's attributes to determine what groups they should belong to. When changes are made by the HR team, these rules are re-evaluated upon each hourly import and the group memberships change accordingly, so access to systems and applications change to match an employee's role and responsibility changes within Doximity.

The IT and Infrastructure security teams perform a quarterly audit of accounts, group rules, and access to ensure no orphaned accounts exist and that access restrictions match expectations set by upper management.

As needed, the HR Team will alert members of the IT and Infrastructure Security Teams of any employee departures. When possible, these departures are scheduled ahead of time, but they can also be performed ad-hoc in-emergency situations. At an agreed upon time, a user's Okta account is deactivated. Upon deactivating an employee's Okta account, access to their assigned applications (including e-mail, chat, calendar, etc.) is immediately revoked.

In the case of some of the more advanced application integrations, the associated user accounts in each of the downstream apps are automatically deprovisioned/deactivated. In other cases, the user's account within the SaaS app is manually deactivated and access is revoked by the IT team.

### Computer Operations - Backups

Doximity uses AWS' point-in-time snapshot of data as the backup software. Doximity makes daily snapshots of systems; the snapshots are incremental - the new snapshot saves only the blocks that have changed since the last snapshot.

Doximity policy is to keep data for 14 days. The life cycle of backups is maintained through the AWS policies and security controls. This includes the timing, expiration, encryption & monitoring of the backup process.

Snapshots occur asynchronously; the point-in-time snapshot is created immediately, but the status of the snapshot is pending until the snapshot is complete (when the modified blocks have been transferred to Amazon S3), which can take several hours for large initial snapshots or subsequent snapshots where many blocks have changed. While it is completing, an in-progress snapshot is not affected by ongoing reads and writes to the volume.

Snapshots that are taken of encrypted data (where encryption applies) are automatically encrypted. Restores that are created from encrypted snapshots are also automatically encrypted. The encrypted data volumes and any associated snapshots are protected both at rest and in motion.

### Computer Operations - Availability

Incident response policies and procedures are in place to guide personnel in reporting and responding incidents. Procedures exist to identify, report, and act upon system security breaches and other incidents. Incident response procedures are in place to identify and respond to incidents on the network.

Doximity monitors the capacity utilization of computing infrastructure to ensure that service delivery matches expectations. Doximity evaluates the need for additional infrastructure capacity in response to the growth of system users.

Doximity has a patch management process to ensure infrastructure systems are patched in accordance with vendor recommended operating system patches. Doximity staff validates that patches have been installed and if applicable that reboots have been completed.

### Change Control

Doximity maintains a documented change control policies and procedures to guide personnel in documenting and implementing application and infrastructure changes. This process is built into the Repository controls and the applied rules around the merging of code for release. The change control procedures follow this workflow, a proposed change is created in the repository that controls the infrastructure or application that the change is targeted at. When the person is satisfied with the change it is run through the automated tests and a "Pull Request" requested of the repositories owner group for review. If approved, then it can be merged for Quality assurance testing and further advancement into production.

A tracking system is utilized to document the changes in the application and implementation of new changes. Quality assurance 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.

## Data Communications

Redundancy is built into Doximity's systems from a cloud-first design and the AWS infrastructure. Ensuring that there is no single point of failure that includes Load Balancer, Auto Scale Groups, and multiple Availability Zones. In the event that a primary system fails, the redundant configuration is defined to take its place.

Doximity uses tools such as VPC, Network security groups, Private IP configurations, ingress/egress rules & IAM roles, to provide secure access to Doximity systems after authorization to bastion systems that then allow confirmed users access to production systems.

Penetration testing is conducted to measure the security posture of a target system or environment. The third party vendor uses an accepted industry standard penetration testing methodology specified by Doximity. The third party vendor's 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, the third party vendor attempts 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 occurs from both outside (external testing) and inside the network.

Vulnerability scanning is performed by a third party vendor on an annual basis in accordance with Doximity's policy. The third party vendor uses industry standard scanning technologies and a formal methodology specified by Doximity. 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 annual basis. Internal and external scans are performed during non-peak windows. Tools requiring installation in the Doximity system are implemented through the Change Management process. Scanning is performed with approved scanning templates and with bandwidth-throttling options enabled.

## **Boundaries of the System**

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

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

## **Changes to the System Since the Last Review**

Amion provides on-call scheduling for healthcare professionals and has been a partner to Doximity. As of February 8, 2022, Doximity acquired Amion. Amion has since been integrated into Doximity and its operations, though remnants of the old Amion systems do exist online for legacy clients or those who have not adapted to the new workflow. Legacy Amion systems do remain out of scope of this SOC 2.

## **Incidents Since the Last Review**

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



## Trust Services Criteria and HIPAA/HITECH Requirements Not Applicable to the System

The following trust services criteria and HIPAA/HITECH requirements were not applicable to the system:

Trust Services Criteria and HIPAA/HITECH Requirements Not Applicable to the System		
Category / Safeguard	Criteria / Requirement	Reason
Administrative Safeguard	164.308(a)(4)(ii)(A)	The entity is not a healthcare clearinghouse.
	164.308(b)(1)	The entity is not a covered entity.
	164.308(b)(2)	The entity does not use subcontractors. The organization would not share ePHI if it was in their possession.
Physical Safeguard	164.310(c)	The entity is not a covered entity.
Organizational Safeguard	164.314(a)(2)(ii)	The entity is not a government entity.
	164.314(b)(1), 164.314(b)(2)	The entity is not a plan sponsor.
Breach Notification	164.404(a)(1), 164.404(a)(2), 164.404(b), 164.404(c)(1), 164.404(c)(2), 164.404(d)(1)(i), 164.404(d)(1)(ii), 164.404(d)(2), 164.404(d)(2)(i), 164.404(d)(2)(ii), 164.404(d)(3), 164.406, 164.408(a), 164.408(b), 164.408(c)	The entity is a business associate; its responsibilities for breach notification are limited to its covered entity customers and members.

## 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 the subservice organization. Such controls are called complementary subservice organization controls. It is not feasible for all of the trust services criteria and HIPAA/HITECH requirements related to Doximity's services to be solely achieved by Doximity control procedures. Accordingly, the subservice organization, 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 and HIPAA/HITECH requirements described within this report are met:

Subservice Organization - AWS		
Category / Safeguard	Criteria / Requirement	Control
Common Criteria/Security, Physical Safeguard	CC6.4 164.310(a)(1) 164.310(a)(2)(ii) 164.310(a)(2)(iii) 164.310(a)(2)(iv)	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.
		Electronic intrusion detection systems (IDS) 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, UPS units, and redundant power supplies.

Subservice Organization - AWS		
Category / Safeguard	Criteria / Requirement	Control
		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.
		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 the subservice organization
- Reviewing attestation reports over services provided by vendors and the 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 and HIPAA/HITECH requirements 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 and HIPAA/HITECH requirements 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.