HIPAA Compliant Communications using Doximity

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) was designed to protect electronic data pertaining to patient identification and health, and standardize the process of data interchange. A major component of HIPAA is the "Security Rule", which includes technical safeguards and their implementation. Technical safeguards are defined in 445 CFR Part 164 § 164.304:

> *Technical safeguards means the technology and the policy and procedures for its use that protect electronic protected health information and control access to it.*

The Security Rule's technical safeguards do not mandate a specific technology solution but rather employ the adaptable requirement that an entity use any and as many security measures as are reasonable and appropriate. These security measures are required to meet several standards, as described below. Doximity meets --and in many cases exceeds-- these standards while bringing innovative flexibility and features to physician users.

Access Control

"Access" is defined in § 164.304:

> *Access means the ability or the means necessary to read, write, modify, or communicate data/information or otherwise use any system resource.*

The access control standard § 164.312(a)(1) requires that a covered entity must:

> *Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in §164.308(a)(4).*

Access controls are designed to provide the appropriate privileges to user accessing data, applications and files. The HIPAA Security Rule describes implementation specifications for the access control standard:

> **Unique user identification** § 164.312(a)(2)(i). *Assign a unique name and/or number for identifying and tracking user identity.*

Doximity assigns each user a unique identification number, allowing it to route information appropriately and track user activity. Healthcare provider accounts are associated with a preexisting profile sourced from the National Provider Index (NPI).

> **Automatic logoff** § 164.312(a)(2)(iii). *Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.*

The Doximity website terminates electronic sessions after a period dependent on access-device type. By default, sessions are automatically terminated after 30 minutes of inactivity and a new login required.

> **Encryption and decryption** § 164.312(a)(2)(iv). *Implement a mechanism to encrypt and decrypt electronic protected health information*.

To protect sensitive health information from unauthorized access, all data on the Doximity network is protected using the Secure Sockets Layer (SSL) protocol. In fact, Doximity was the first professional/social network to force the https:// standard for all mobile and web communication features, protecting from unauthorized access over wireless and wired networks. Inbox messages and faxes are additionally encrypted end-to-end using 256-bit Advanced Encryption Standard (AES) encryption with Cipher-Block Chaining (CBC) mode for message headers, content and attachments.

Audit Control

The audit control standard § 164.312(b) requires that a covered entity must:

> *Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.*

Doximity records and examines network activity to protect users, technical infrastructure and electronic health information from security violations. Access logs are stored indefinitely. Logs are maintained every time an inbox (DocMail) or fax (DocFax) record has been accessed or edited. These logs are fully encrypted, easily accessible by Doximity, and can be retrieved at short notice for emergency situations.

Integrity

“Integrity” is defined in § 164.304:

> *Integrity means the property that data or information have not been altered or destroyed in an unauthorized manner.*

The integrity standard § 164.312(c)(1) requires that a covered entity must:

> *Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.*

Doximity protects the integrity of electronic health information via end-to-end encryption and decryption of messages transferred over the SSL protocol. To protect against destruction, Doximity messages are securely archived once per hour, and access to archives is itself logged and archived separately.

Person or Entity Authentication

The person or entity authentication control standard § 164.312(d) requires that a covered entity must:

> *Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.*

During user registration, a new user claiming to be a healthcare provider initiates account registration by entering their name and finding their pre-filled profile, pre-generated by Doximity from the National Provider Index (NPI) of US providers. They then verify they are the person they claim to be by entering their date of birth and work zip code, then passing a challenge-response identity test. Doximity utilizes a third party identification services provider that generates three identity challenge questions based on credit reports and other databases. After passing the identity test, a user creates an account and a personal password, which must be used to subsequently sign-in to the application.

New users that fail to pass the identity quiz, do not find their NPI number, or do not have an NPI number can create an unverified, placeholder Doximity account wherein all communication features are disabled. Users in the unverified state are prompted to enter a manual verification process, wherein proof of identity and provider credentials is established using manually submitted and reviewed copies of identification and employment documents.

Transmission Security

The transmission security standard § 164.312(e)(1) requires that a covered entity must:

> *Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.*

There are two implementation specifications for the transmission security standard:

> **Integrity controls** § 164.312(e)(2)(i). *Implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of.*
>
> **Encryption** § 164.312(e)(2)(ii). *Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.*

Doximity uses the Secure Socket Layer (SSL) Handshake Protocol with a 2048-bit RSA Cryptosystem for all mobile and web data communication, protecting from unauthorized access over wireless and wired networks. Doximity messages are further encrypted using 256-bit AES with CBC mode on message headers, content and attachments.

Mobile Devices

The Doximity mobile application for Android and iOS features secure Inbox messaging and faxing. No PHI is ever stored locally on mobile devices. Rather the data transmitted to mobile devices is erased from the device after access, while the version on Doximity servers remains encrypted at rest. In the event a user has a lost or stolen mobile device, the user or Doximity support can deauthenticate the device remotely.

Summary:

Today's physician faces many of the same communication barriers as their predecessors—they are restricted to outdated, HIPAA approved devices such as pagers and fax machines. Although text messaging is standard practice in other fields, SMS does not meet HIPAA security requirements. That prohibits instant, text-based communication within the medical community.

Doximity provides a HIPAA compliant, digitally encrypted messaging technology that enables physicians to communicate securely and conveniently from web and mobile platforms.

Doximity requires new users to submit personally-identifiable information and pass an identity verification quiz to ensure each member is a verified healthcare professional.

Highlights of Doximity's Security and Compliance Components

* Unique User Identification and Verification
* User Authentication to Confirm the Medical Professional's Identity
* SSL Handshake Protocol with 2048-bit RSA Cryptosystem
* Secure Inbox with End-to-End 256-bit AES Digital Encryption with CBC mode
* Automatic Logoff During Inactivity
* Audit Control to Protect Users from Security Violations
* Backup of All Network Activity

Doximity is a free application that can be utilized on iPhone, Android and the web. HIPAA compliance and data security is a top priority for Doximity's communication platform. We welcome any additional questions, ideas or feedback at support@doximity.com.