Our Commitments to Security

Doximity was created to simplify and support the work of healthcare providers. Our platform is secure, facilitating encrypted, HIPAA-compliant communications with patients.

Doximity maintains the security and privacy requirements of the healthcare industry:

- Requires ongoing HIPAA training for all staff and contractors
- Conducts a risk analysis and access verification quarterly
- Includes a Business Associate Agreement with each member
- Has a Privacy and Security officer
- Offers communication tools only available to healthcare professionals for clinical and patient care purposes
- Requires identity verification upon registration. Please see Doximity Terms of Service for more information
- Utilizes member authentication that adheres to oAuth 2 standards along with MFA

We continuously monitor to improve and adapt:

- Employs multiple logging and monitoring strategies to ensure alerts are raised and resolved promptly (this includes 24/7/365 on-call schedules for team members supporting these systems)
- Utilizes intrusion detection systems to monitor our applications and infrastructure; including but not limited to WAF (Web Application Firewall), RASP (Runtime Application Self-Protection) and brute-force detection (instruction attempts are blocked immediately)
- Disaster recovery plans in place which include an architecture that self-heals during disaster scenarios as well as auto-scaling to manage increased demand
- Conducts ongoing penetration testing using internal testers as well as external firms
- Quarterly white-box testing with security researchers and professionals

We employ industry-leading encryption strategies:

- Passwords are salted and hashed using bcrypt

  Note: *The original password is discarded and never logged or stored*

- Ensures all requests are only made over Secure Sockets Layer (SSL)
- Encrypts video call media on transmission over a DTLS/SRTP connection
- Video call media is never stored permanently; recordings are not allowed
- Encrypts PHI at rest using 256-AES encryption and further encrypts any databases containing it with AWS Key Management Service

The privacy of our members and their work is paramount:

- Patient phone numbers and email addresses are only used to deliver the services connecting doctors to their patients, not for any other commercial purpose
- Doximity does not sell or release the personal contact information of our members, including email addresses and personal device phone numbers

  Note: *The only communications members receive after signing up for Doximity are sent by Doximity regarding Doximity services. All email notifications from Doximity can be categorically turned-off in the communications settings or from the settings link within any email*

- Public patient-facing practice, clinic or hospital contact information may be displayed separately as the CallerID of phone calls or on a member's public profile
- Patients are not required to install an app and access Doximity using trusted and up-to-date web browsers provided by Google, Mozilla, and Apple
- Please see the Doximity Privacy Policy for more information