HIPAA, PHI, encryption and data storage standards, and more

Written by Alan Mark. Updated over a week ago

Doxy.me complies with the security and privacy requirements of the healthcare industry.

Protected Health Information Protection

- Doxy.me **does not contain, display, transmit, process, view, or collect Protected Health Information** (PHI).
- Doxy.me **does not record any video or audio calls** or save any chat messages at any time for any reason.
- We utilize the open standard WebRTC **point-to-point NIST-approved AES 128 bit encryption for video & audio communication**.
- Doxy.me uses **full volume encryption and AES 256-bit standard encryption** used on all data stored at rest on file servers with secure backups.
- All access to the doxy.me interface (such as the dashboard, waiting room, and any public webpages) is **secured over TLS 1.2+ (https)**, ensuring the information is encrypted.

Technical and Physical Security Controls

- **All doxy.me data are stored within the highly secure Amazon Web Services (AWS) datacenter infrastructure with their industry standard physical controls.** The doxy.me support system, help center, and public facing website are independent services to ensure uptime and availability across the platforms. For a list of AWS current security accreditations, see the AWS Compliance Programs page.
- **Only a select few senior administrators and developers have access to database servers and code has to be approved by multiple parties and pass automated tests before deployment**. Employees are only allowed access to provider-level data on a need-to-know basis in order to fulfill job function.
- During the provider sign up process, doxy.me will provide immediate feedback on password strength to **require strong passwords**. Any password classified as a 0, 1, or 2 (reflected in the number of dots on the strength indicator) is not allowed.
- All provider **passwords are stored using one-way cryptographic hashing functions** so even doxy.me staff and developers can't see provider passwords. Patients do not have accounts.
- Providers on any subscription plan including the Free plan may use "Log in with Google" or "Log in with Facebook" to implement MFA provided by those

organizations. Providers on the **Clinic subscription plan may use their own LDAP using SAML integration** with doxy.me.

- **Doxy.me does not use proprietary video and audio technology or applications**. Our platform is built on top of the open-source WebRTC standard for real-time communication.

Overall Security Practices

- Doxy.me is browser-based. There is no proprietary or closed-source software to download and install. Patients, clients, and providers all access Doxy.me using **trusted web browsers provided by Microsoft, Google, Mozilla, and Apple** (it is the responsibility of the client to ensure they are using the latest, updated version of their browser). Doxy.me never has direct access or control over a user's physical device or any other application on the device. If your browser is out of date, you will be notified and may be unable to use the system.
- We **only use HIPAA/HITECH compliant servers** with active OSSEC intrusion detection, file integrity monitoring, log monitoring, root check, and process monitoring. We maintain a hardened, patched server OS with frequent security updates. And all workforce members are required to use anti-virus software and full-disk encryption on their devices.
- New vulnerabilities are found every day. Doxy.me has a robust program in place to find and remediate them. We don't comment on specific vulnerabilities.
- Doxy.me conducts **annual HIPAA/HITECH risk assessments** conducted by trusted third-party auditors along with regular penetration testing and vulnerability scans. After the assessment, we regularly review our policies and procedures and adjust them accordingly based on the findings. In the event of any vulnerabilities discovered, we work to address each in a timely manner relative to risk.
- Doxy.me runs a **bug bounty program** to assist in finding and reporting vulnerabilities with our platform. Once a vulnerability has been reported, our team works on implementing fixes as quickly as possible.
- We have **backup and disaster recovery policies and procedures** in place.
- Doxy.me maintains a **cyber insurance policy**.

Third-Party Vendor and Service Provider Security

- We partner with Stripe to manage payments on doxy.me. Stripe is **certified as a PCI Level 1 Service Provider**. Doxy.me does not have access to customers' credit card data.

- **Vendors** that assist in providing the Doxy.me platform **have signed BAAs with doxy.me** specific to the service they provide. Many of these providers operate under Service Level Agreements to help ensure

To comply with HIPAA/HITECH *you* also have some responsibilities while using doxy.me:

- **Sign the Business Associates Agreement** found within your account dashboard.
- Do not share your login email and password with other providers.
- Do not reuse old passwords that may have been compromised and use the provided password strength indicator to ensure your password is strong, complex, and not guessable.
- Keep your browser and operating system up to date to ensure the greatest protection and that the platform works as intended.
- Install and use antivirus and firewall programs suitable for your compliance and security needs.
- Properly authenticate the patients you meet with before you exchange any sensitive information during a call. This may be in the form of requesting the patient to present a form of identification or verifying information you have on file. Doxy.me does not store patient information so the provider is the best individual suited to verify a patient or client.

If you have any questions, please contact our support team.

Learn more at doxy.me.