Doxy.me complies with all relevant HIPAA rules and regulations.

Covered Entities using our platform are compliant with HIPAA, because doxy.me:

- does not permanently store Protected Health Information.
- operates according to the Privacy and Security Rules.
- conducts risk analysis and management.
- has disaster mitigation plans in place.
- conducts in ongoing HIPAA training for all staff and contractors.
- has a Privacy and Security officer.
- utilizes an IDS (Intrusion Detection System) to monitor our infrastructure; Intrusion attempts are immediately blocked.
- actively employs file integrity monitoring, log monitoring, root checks and process monitoring across our infrastructure.
- performs a nightly scan of our infrastructure to check for malware against signatures that updated daily.
- uses for all servers and images the baseline configurations recommended by industry standard CIS Benchmarks and Security Content Automation Protocol (SCAP).
- automatically encrypts stored data using full volume encryption and 256-bit AES encryption keys and use Amazon Web Services EBS encryption backed by an FIPS 140-2 key management infrastructure.
- conducts regular penetration testing using both internal and third-party testers.
- will sign a Business Associates Agreement acknowledging us as a Business Associate.

Be sure to check with your legal counsel if you have specific questions regarding your compliance responsibilities with HIPAA.

HIPAA Q&A

Does doxy.me have a HIPAA compliance program? Yes, with on-going monthly reviews.

Is doxy.me a typical video service? No, it is built around HIPAA-compliant security and privacy. What does HIPAA compliance mean? Our features are designed and developed with security and privacy in mind to ensure that your telehealth call meets U.S. federal regulations.

Does doxy.me perform annual HIPAA audits and reviews? Yes, with an independent auditor and as related to the Security and Privacy Rules. Our policies and procedures are evaluated as to safeguarding data using industry standard technical and administrative controls.

Does doxy.me provide HIPAA training to its employees? Yes. HIPAA information is regularly disseminated and numerous internal resources are available to each employee.

HIPAA References (highlights)

The sections below are some of the important HIPAA/HITECH requirements and how we fulfill those requirements. More details may be found in the Security Rule (45 C.F.R. Part 164 Subpart C), the Breach Notification Rule (45 C.F.R. Part 164 Subpart D), and the Privacy Rule (45 C.F.R. Part 164 Subpart E).

Have a written set of privacy policies procedures for handling PHI
Even though we don't process PHI, we act like we do. Our internal procedures include who can access the development environment, how to lockdown database servers, and how to handle inquiries and data breaches. (§164.308(a) and its subsections; §164.316(b) (1)(ii))

Establish and test contingency plans that include disaster recovery
Doxy.me has numerous operational policies that provide administrative safeguards to protect all data in the event of an emergency. All data are backed up nightly and replicated in real-time to separate systems. (§164.308 (a)(7)(ii))

Ensure the confidentiality of communications with individuals
All sessions between patient and provider are over a highly-encrypted channel (TLS, also known as HTTPS). Also, the session is never recorded or otherwise stored. It happens in real-time. And any photo or file transferred is automatically and permanently deleted after 15 minutes. (§164.312(e) and its subsections)

Restrict access to data to only those employees who require it to perform their job function
We deploy access controls so only employees with a need to access customer data may do so—with an audit trail. (§164.312(a) and its subsections)

Third-parties we use must comply with HIPAA rules
Our legal agreements with third-parties (those companies that provide extended functionality) state that any data they receive from us will only be used for the purpose intended. In other words, the data must be processed with the same safeguards as used by doxy.me. No data sent to a third-party will ever be sold. ((§164.314(a)(2)(iii))

Implement policies and procedures for authorizing access to PHI and prevent anyone other than the intended recipient from intercepting any data
We run our software and store all data in an ultra-secure Amazon Web Services data center. We track all access to databases whether it's for maintenance or for support. All access to the databases is remote using secure protocols (two-factor authentication and TLS). All databases are highly encrypted, systems are hardened using industry-best methods, and intrusion detection is constantly monitored. Log files are used to record all critical transactions and access. (§164.312 and its subsections)

Data corroboration such as digital signatures, check sums, and message authentication should be used to ensure data integrity and anti-tampering

All communications between patient and provider, as well as data stored in servers, use industry standard protocols to ensure data integrity and anti-tampering. (§164.312(c)(1))

Deploy a high level of authentication to the service
All provider passwords are stored using one-way cryptographic hashing functions so even doxy.me staff and developers can't see or abuse provider passwords. Patients don't have accounts. In addition, the clinic version can use an identity provider with two-factor authentication (such as a code sent to your cell phone). (§164.312(d))

Conduct annual HIPAA risk assessments
Each year, our risk management program requires engaging a trusted third-party auditor to perform an independent HIPAA assessment that evaluates the oxy.me software, environment, and procedures. In addition, we perform periodic penetration testing and vulnerability scans. After an assessment, we review our policies and procedures and adjust as necessary. (§164.308(a)(1)(i) and §164.308(a)(1)(ii))

Have a procedure to respond to data breaches
We have procedures in place to respond to a data breach regardless of what data may have been involved. Any successful unauthorized attempts to access any data, modification or destruction of data, will put into effect emergency steps to mitigate any further disclosure and begin an investigation to the cause and effect. (§ 164.410, HITECH Act §13402(b))

Have a procedure to respond to individual inquiries
If an individual wants to know what data we have collected about them, our policy is to notify and assist the account holder to respond to the request. Doxy.me does not collect information about individuals that would constitute PHI. (§ 164.522 and § 164.404)

In summary

- Doxy.me implements industry best administrative, physical and technical safeguards that reasonably and appropriately protect

the confidentiality, integrity, and availability of all data in accordance with the Security Rule.

- Doxy.me has in place breach notification policies and procedures that comply with the Breach Notification Rule.
- Doxy.me follows policies and procures used to protect an individual's privacy that comply with the Privacy Rule.