DATASHEET

HIPAA Compliance

Healthcare-ready telecommunications

Most Dialpad products, including Dialpad Meetings, can be used compliantly by healthcare industry customers once a Business Associate Agreement (BAA) is signed.

Dialpad's BAA does not cover the use of Dialpad fax for PHI or the use of SMS for communicating patient information to non-Dialpad users. To request a BAA, contact legal@dialpad.com.

Note: Dialpad's BAA conforms to the Google Cloud Platform BAA and cannot be revised by Dialpad

How Dialpad keeps communications HIPAA compliant

Rigorous security risk assessment

Dialpad is SOC2 Type 2 certified and has completed the Cloud Security Alliance's Consensus Assessment Initiative Questionnaire which address the controls listed in the HIPAA Security and Privacy Rule and meets the needs of the HIPAA Security Risk Assessment.

You can view the results and learn more about Dialpad's security features at dialpad.com/trust.

Business Associate Agreements (BAA)

Dialpad, as a Business Associate, provides contractual assurance to implement HIPAA safeguards protecting ePHI. This also ensures that any subcontractors partnered with Dialpad will also follow these safeguards. Dialpad's BAA include a custom 30-day retention policy to ensure data protection, we provide:

- Data encryption at rest and in transit
- Access limitation based on minimum necessary privileges
- Reviewing and maintaining our vendors' security and privacy

To ensure data privacy, we provide:

- Access to personal data upon request
- Ability to amend/delete data upon request
- Notification if data breach occurs

Additional security practices at Dialpad

Google Cloud Platform

Dialpad websites, web apps, smartphone back-end, and customer sensitive data is processed and stored using Google Cloud Platform services.

Failovers and backups

Automatic backups are built into our system. Every aspect of our system has been designed with redundancy in mind so that in the event of a failure, there's always an alternative to take its place immediately.

24/7 emergency response

Dialpad's team is available 24/7/365 and employs a "follow the sun" support model so that no matter where you are, Dialpad is available when you need us.

Identity and authentication

User authorization of Dialpad services are communicated over HTTPs and are secured under the administrators choice of OAuth2.0, SAML 2.0, or by email and password combination that is stored and encrypted using a secure cryptographic one-way hash function of the salted password.

Proactive logs and monitoring

We monitor log access to sensitive information and systems and have event monitoring in place, complete with staff who are trained to proactively identify unusual activity.