What about HIPAA?

Planet DDS and our software Denticon helps you comply with HIPAA

Planet DDS is compliant with all the standards included in the HIPAA Security Rule and all the standards of the HIPAA Privacy Rule that apply to Business Associates. In addition, Planet DDS has met the Business Associate requirements of the HITECH Act. Planet DDS undergoes regular assessments with third-party experts to ensure our continued compliance.

Knowing that your vendor meets HIPAA standards lets you focus on your practice and how your team can meet your HIPAA requirements.

Platform Security

Planet DDS invests in security on multiple levels

Planet DDS takes securing your data very seriously. Planet DDS uses state-of-the-art hardware and software firewalls and Intrusion Prevention Systems (IPS) along with continuous Security Information and Event Management (SIEM) to monitor and protect all critical systems. These systems are maintained in a secure data center with limited physical access. Remote access is protected via two-factor authentication and only available to a very limited number of key IT personnel. All systems are updated and patched on a regular basis to ensure any potential vulnerabilities are resolved in a timely manner. Vulnerability scans are performed on a regular basis to ensure the highest level of security.

To further protect you, we continuously replicate data to our Disaster Recovery site. In addition, we send backups off-site both nightly and weekly.

Planet DDS also provides Security Awareness training for all employees to keep them up to date on the latest techniques used by hackers.

Application Security

Denticon offers multiple features to allow you to control what data your users can see and what actions they can take. You can determine a password reset policy for your practice and set the following on a per-user basis:

- User group membership
- Days of week access control
- Time of day access control
- Patient data access control
- Office location access control
- IP access control

Denticon provides a detailed audit history of user actions that is accessible by administrators.