# Delta Health Technologies' Security Statement for AppointMate®

## Security Statement

The AppointMate application utilizes SSL encryption along with having your account/data protected by a mandatory user ID and password. Any password-protected areas of AppointMate can be accessed only with a valid password. Each password owner is responsible for keeping the password secret and confidential, and for notifying AppointMate if the password may have been stolen or might otherwise be misused.

## Cookies

We use "cookies" as a fundamental part of our interaction with your internet browser. The only information saved is the login name which is used for the username in the login field

## Monthly Vulnerability scanning

Delta Health Technologies® takes security very seriously and ensure that we are doing everything possible to protect our customer's sensitive information. Delta Health Technologies uses a Third Party application to perform security scanning and vulnerability testing based on several industry standard frameworks. Any identified threats are analyzed in light of the value of the asset(s) in question, pervasiveness, effectiveness, existing controls, likelihood of exploitation, and potential impact to the organization if the threat is acted upon. This risk analysis, using an internal risk scoring methodology based on NIST 800-30 Rev.1 results in a risk score that describes the actual risk being incurred due to the existence of the threat or vulnerability and produces comparable and reproducible results in accordance with ISO 27001. The Common Vulnerability Scoring System (CVSS) is an open industry standard for assessing the severity of computer system security vulnerabilities. CVSS attempts to assign severity scores to vulnerabilities, allowing responders to prioritize responses and resources according to threat.

Additionally, Delta Health Technologies requires all development staff to annually participate and attend Open Web Application Security Project (OWASP) training to focus on educating and developing secure coding practices within the AppointMate applications

## Data storage

Our servers are securely located in a state-of-the-art facility that is managed by a premier provider of managed hosting and advance connectivity solutions.  Delta selected their hosting provider because of their reputation for quality service and support as well as their unparalleled reputation.

## Datacenter Certification

Delta Health Technologies partners only with premier service providers and co-location facilities which offers SSAE 16 certified colocation and data center services.

Delta Confidential

## Statement on Auditing Standards SSAE-16 Compliance

SSAE 16 is the new auditing standard put forth by the Auditing Standards Board (ASB) of the American Institute of Certified Public Accountants (AICPA). Replacing the Statement on Auditing Standards no. 70, otherwise known as SAS 70, SSAE-16 Compliance is used for evaluating service provider organization control objectives and activities so that the information can be shared with other parties in a uniform reporting format that is generally accepted by the audit community.

The issuance of the opinion report prepared by Expedient's independent accounting and auditing firm in accordance with SSAE-16 is a reliable indicator that our control objectives and activities have been examined and were found to meet the standards set forth by the AICPA.

**SSAE-16 Compliance Reports:**

- **SOC 1 Report (Type II)**
  Report on Controls at a Service Organization Relevant to User Entities' Internal Control over Financial Reporting (SSAE-16) – This report is used by customers undergoing financial statement audits and those who require compliance with the Sarbanes-Oxley Act or similar regulation. It reports on the effectiveness of controls in achieving stated objectives throughout a specified period and was formerly known as SAS 70. Receipt of this report requires execution of a mutual non-disclosure agreement and is available from an account manager.

- **SOC 2 Report (Type II)**
  Report on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality or Privacy – This report is used by customers who require confidence in the critical business processes and procedures to complement compliance with the Health Information Portability and Accountability Act (HIPAA), Payment Card Industry Digital Security Standard (PCI-DSS), and other industry or government regulations with relevant requirements. Receipt of this report requires execution of a mutual non-disclosure agreement and is available from an account manager.

- **SOC 3 Report**
  Trust Service Report for Organizations – This report is used by prospective and current customers as a general overview of controls related to certain processes and procedures. Receipt of this report requires acceptance of our terms and conditions and is available for download.

## People and access

Delta Health Technologies Operation Support maintains an account on all hosted AppointMate systems and applications for the purpose of maintenance and support. Only employees with the highest clearance have access to application data. Application data is only accessible with appropriate credentials, ensuring that there are no possibilities of one customer having access to another customer's data without the explicit knowledge of their login information.

## Backups

Application database backups are performed daily for all AppointMate hosted services and transaction log backups of databases occur every 15 minutes. The backups are maintained for 14 days.  In addition, the Appointmate database servers are "mirrored" to an off-site remote datacenter.

## Privacy

Delta Health Technologies adheres to a strict policy for ensuring the privacy of your Protected Health Information - PHI (such as full name, address, email address and/or other identifiable information). We will never share PHI information with CCD's, third parties or other mediums outside of AppointMate unless customer gives express permission for us to do so, or unless we are required to do so under applicable law.

*Updated by Jason Spahr on June 25, 2020*