MDaudit
A HAYES TECHNOLOGY

MDaudit Enterprise HIPAA Compliance

The Health Insurance Privacy and Accountability Act (HIPAA) of 1996 contains a Privacy Rule ("Standards for Privacy of Individually Identifiable Health Information") that establishes a set of national standards for the protection of certain health information. The Privacy Rule standards address the use and disclosure of individuals' health information — called "protected health information" (PHI) by organizations subject to the Privacy Rule — called "covered entities," as well as standards for individuals' privacy rights to understand and control how their health information is used.[1]

Hayes is committed to protecting patient data according to the HIPAA Privacy Rule guidelines, and we have instituted the physical, network, and process security precautions in our MDaudit Enterprise software as a service (SaaS) platform to ensure that your protected data is secure.

Secure AWS Cloud Infrastructure

The MDaudit Enterprise platform uses Amazon Web Services (AWS) and its utility-based cloud services to process, store, and transmit PHI. AWS services and data centers have multiple layers of operational and physical security to ensure the integrity and safety of patient data. Our platform uses the following AWS services:

- **EC2** – a scalable, user-configurable compute service that supports multiple methods for encrypting data at rest.
- **S3** – provides server-side and client-side encryptions and several methods of managing keys.
- **Route 53** – a managed DNS service that enables Hayes to register domain names and route and check the health of internet traffic customer domain resources.
- **CloudWatch** – logs, monitors, stores, and provides access to log files, which are encrypted while in transit and at rest.
- **CloudTrail** – enables governance, compliance, operational auditing, and risk auditing of AWS accounts.

[1] HHS.gov, Health Information Privacy, www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html

In addition to the AWS services listed above, we follow these security protocols:

- All storage volumes are encrypted using the AWS Key Management Service with AES-256 Server-Side encryption.
- For internal access to AWS hosted infrastructure, all sessions go through a multi-factor VPN.
- AWS Security Groups are limited to traffic only within the Hayes AWS Virtual Private Cloud, with the exception of traffic to the load balancers and white-listed traffic to our SFTP server.
- For web user access, the Elastic Load Balancer employs TCP pass-through to the EC2 endpoints to enforce HTTPS encryption.

Hayes has a Business Associate Agreement (BAA) contract with AWS. The BAA is required by HIPAA regulations when using a cloud service provider (CSP), and ensures that AWS appropriately safeguards PHI. The contract also clarifies and limits the permissible use and disclosure of PHI by AWS.

Infrastructure Security Measures

- Trend Micro's Deep Security System provides dos and sync flood protection, real-time security incident event management, and real-time Antivirus.
- Geofilters are deployed to reduce global attacks.
- AWS Security groups limit access to our AWS Virtual Private Connection (VPC). Nonpublic facing resources are limited to inter-VPC traffic.
- The Secure File Transfer Protocol (SFTP) server is limited to white-listed IP addresses specified during client onboarding. Load balancers are restricted to port 443 for SSL traffic.
- Audit trails are processed through AWS CloudTrail, and specific application-level logging is captured to record access to PHI within MDaudit Enterprise.

Secure Data Access and Transfer

All domains associated with *mdauditenterprise.com* use an SSL certificate which is issued, managed, and automatically renewed using AWS Certificate Manager. The public key is RSA 2048-bit and signed using SHA256 with RSA.
Hayes uses Secure File Transfer Protocol (SFTP) service to receive data files from clients, which are then transferred to an encrypted volume inside our virtual private cloud (VPC) at AWS. Once the data file is within our VPC, it remains on encrypted volumes with access granted only through a multi-factor VPN, and only where necessary for job functions.

Liability Insurance

As further protection for our client's data, Hayes maintains a $10 million cybersecurity liability insurance policy.

Secure Data Storage

Hayes ensures PHI protection for stored data through the use of data encryption, secured databases, and reliable back-up procedures.

To gain access to MDaudit Enterprise, users must be authenticated using unique, application-specific credentials. The system supports Security Assertion Markup Language (SAML) single-sign-on authentication. All authentication activity is logged within the application. All customer data is encrypted 'at-rest' using Amazon Key Management Service. Customer data is securely transmitted via SFTP through a white-listed, default deny-all firewall.

Data Standards

Hayes supports ANSI ASC X12, developed by the Accredited Standards Committee as a standard format for electronic data interchange (EDI). We support a variety of ANSI ASC X12 transactions including institutional, professional, remittance and claim files (837 I/P and 835s).

Disaster Recovery and Business Continuity

To ensure high-availability of client data, Hayes employs multiple server backups in the US-East 1 and US-East 2 regions. We use redundant backups at the database, volume, and instance levels. In addition, we maintain multiple daily differential backups of our databases, daily backups of all storage volumes, and daily backups of the entire server.

SOC2 Certification

Hayes has successfully completed a System and Organization Control 2 (SOC2) audit to assess potential risks from interactions with the MDaudit Enterprise system. The audit was completed in Q3 2019 and met trust services criteria (TSP 100) for the following:

- Security
- Availability
- Processing Integrity
- Confidentiality
- Privacy

To obtain a copy of the SOC2 audit report, you may enter a request through our Support Center or by contacting your Customer Success Manager or Sales associate. In addition Hayes is also undergoing further security assessment procedures by initiating a HITRUST certification targeted for completion in Q3 2020.

For any additional questions, please contact:
HayesITSecurity@hayesmanagement.com.

70 Walnut Street, Suite 200 | Wellesley, MA 02481
Phone: (617) 559-0404 | Email: info@hayesmanagement.com
www.hayesmanagement.com

A HAYES TECHNOLOGY