TREASURE DATA

Treasure Data and the HIPAA Security Rule

White Paper

HIPAA Compliance

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) establishes the standards that protect the confidentiality, integrity, and security of protected health information (PHI). As a Customer Data Platform (CDP) provider, Treasure Data understands and acknowledges the importance of compliance with HIPAA to our customers.

This white paper will define the HIPAA Security Rule's standard for safeguarding electronic protected health information (ePHI), and detail how Treasure Data keeps ePHI protected through documented policies as well as appropriate administrative, physical, and technical safeguards.

The HIPAA Security Rule requires covered entities and business associates to:

1. Ensure the confidentiality, integrity, and availability of all ePHI they create, receive, maintain, or transmit;
2. Identify and protect against reasonably anticipated threats to the security or integrity of the information;
3. Protect against reasonably anticipated impermissible uses or disclosures; and
4. Ensure compliance by their workforce.

As a business associate, Treasure Data is committed to having appropriate administrative, technical, and physical requirements to prevent any unauthorized disclosure or access of ePHI in the Treasure Data environment. The following sections set forth how Treasure Data fulfills HIPAA compliance based on the HIPAA Security Rule.

Policies, Procedures, & Documentation

- Treasure Data's Security Program includes policies, procedures, standards, plans, and guidelines to address HIPAA requirements. All policies are reviewed, approved, and acknowledged at least on an annual basis, or as necessary. In addition to HIPAA, Treasure Data's policies are aligned and mapped to the controls requirements identified in the following frameworks or regulations: Secure Controls Framework (SCF), ISO/IEC 27001, SSAE 18 SOC 2, CCPA, and GDPR.
- Treasure Data's policies, procedures, and plans include the Business Continuity/ Disaster Recovery (BC/DR) Plan and the Security Incident Response Plan (SIRP).
  - » Security Incident Response Plan (SIRP) - includes a multi-step process to define the Security Incident Response Team (SIRT), Incident Response (IR) roles and responsibilities, employee reporting requirements, triage, evidence collection, containment procedures, external communications, remediation, and post-incident review. In the event of a Security Incident which impacts customer ePHI, Treasure Data will notify the customer promptly without undue delay after becoming aware of the confirmed incident.
  - » Business Continuity/Disaster Recovery (BC/DR) Plan - includes a formalized process to identify the consequences of disasters, security failures, loss of service, and service availability gap which may result in a business impact. The BC/DR Plan includes a restoration plan, communication methodologies and responsibilities during an actual emergency, decision-making chains for the development and execution of response to emergencies, and a path from disaster response to re-building the business.

Administrative Safeguards

- Treasure Data undergoes the following annual external audits to ensure compliance with various standards, frameworks, and other customer requirements:
    - ISO/IEC 27001:2013
    - SSAE 18 SOC 2 Type 2
    - HIPAA Type 2
    - PrivacyMark
- The Treasure Data Security Program leverages a unified baseline set of controls by using the Secure Controls Framework (SCF).
- Treasure Data's controls maturity is assessed annually and continuously monitored by using SCF's Security & Privacy Capability Maturity Model (SP-CMM).
- An HIPAA Risk Assessment is performed annually by leveraging SCF's Security & Privacy Risk Management Model (SP-RMM). The risk assessment includes all people, processes, and technology that support the delivery of in-scope HIPAA-related products or services.
- The Risk Management program requires all risks that may compromise the confidentiality, integrity, or availability of ePHI to be reported, analyzed, treated, and monitored. A Risk Register exists within the organization's Governance, Risk, and Compliance (GRC) tools to track and monitor risks.
- A formal Risk Committee has been established and meets on a quarterly basis to ensure identified risks are being treated in a timely manner. The Risk Committee has also established an authority matrix to accept risks that fall below Treasure Data's risk tolerance. Risks that are above Treasure Data's tolerance must be reviewed and approved for acceptance by Executive Management or remediated. Treasure Data's risk tolerance is formally defined by Executive Management annually or as needed.
- Mandatory HIPAA training is required for all Treasure Data employees (full- and part-time) and contractors during the onboarding process. The onboarding process also includes mandatory policy review and acknowledgements within a timely manner.
- Mandatory HIPAA training is also required on an annual basis for all existing employees. The annual training process also includes a mandatory policy review and acknowledgement.
- Treasure Data's HIPAA training and awareness program includes, but is not limited to, handling, disclosure, and confidentiality requirements, breach reporting, data retention, data deletion, breach notification, and other relevant topics.

- Continuous phishing simulations are conducted to ensure employees are properly identifying and reporting phishing attacks that may jeopardize the confidentiality of ePHI.
- The SIRP and BC/DR Plans are both tested annually to ensure the plans are kept relevant, the teams are aware of roles and responsibilities, and lessons learned are identified to help identify improvement opportunities.
- A formal Third-Party Risk Management (TPRM) Program is in place to ensure vendors that may process or store ePHI are adequately assessed and vetted. Treasure Data's TPRM Program includes evaluation of new vendors using a risk-based methodology. New vendors must be vetted and approved by the Security and Legal/Privacy team before commencement of their services.
- High inherent risk vendors must agree to Treasure Data's Supplier Addendum (e.g., confidentiality terms and security controls requirements). Treasure Data is committed to ensure vendors utilized in the delivery of HIPAA-related products or services to customers are able to meet HIPAA requirements, such as the execution of a Business Associates Agreement (BAA).
- The TPRM Program also includes a risk-based approach to performing due diligence assessment continuously on a defined frequency.

Technical Safeguards

Owned by Treasure Data

- Collected ePHI is stored within Amazon Web Service (AWS) Simple Storage Service (S3) buckets. Data stored within S3 is encrypted at-rest using AES-256 via SSE-S3.[1]
- When using the CDP web application, ePHI traffic is encrypted while in-transit to Treasure Data's public endpoints using SSL/TLS.
- When using the CDP's REST APIs, ePHI traffic is encrypted while in-transit to Treasure Data's public endpoints using TLS.
- Treasure Data's encryption policies and standards are mapped to National Institute of Standards (NIST) SP 800-175B.[2]
- Encryption keys are stored within AWS Key Management Service (KMS). Access to the KMS is restricted to authorized Treasure Data personnel only via Identity & Access Management (IAM) roles. Treasure Data utilizes AWS Managed Keys, which are automatically rotated on an annual basis.[3] AWS KMS provides Level 2 FIPS 140-2 Compliance.
- Treasure Data's customer ePHI is logically separated via Account IDs which are stored in AWS Relational Databases Service (RDS). API keys are unique per customer, and furthermore, unique per user. Each user is provided a master-write and read-only key which is associated with their Account ID.
- Treasure Data's access to ePHI stored in S3 is restricted via a centralized Identity Provider (IdP) which requires multi-factor authentication (MFA). Access is restricted by using the least-privilege principle.
- Direct access to production instances or AWS services is only allowed via Treasure Data's Privileged Access Management (PAM) tool. PAM access requires point-in-time approval by an authorized individual (limited number of personnel).
- All activity and corresponding logs conducted via the PAM tool is logged in Treasure Data's Security Incident Event Manager (SIEM) tool. The SIEM is configured to generate alarms for suspicious activity which is monitored 24x7x365 by Treasure Data's Security Operations Center (SOC).
- All logs which track access, use, modifications, or deletions of ePHI are ingested into Treasure Data's SIEM for monitoring. Logs are retained for forensic purposes.
- No human users are given direct access to S3 buckets which store ePHI via the AWS console.

- All in-scope access rights and permissions are reviewed at least annually by IT & Security personnel.
- Treasure Data utilizes various tools to conduct vulnerability scans at least monthly. A formalized Vulnerability Management Program is in place which defines the process of vulnerability analysis and remediation timelines.
- Treasure Data undergoes annual independent penetration testing over the in-scope external network surface, CDP web application, and all CDP APIs. Results of the aforementioned penetration tests are fed into our Vulnerability Management Program and remediated in accordance with our policy timelines.

Owned by Treasure Data Customers

- Role-based access controls and capabilities exist, permitting the Customer's account administrators to restrict access to ePHI or other specific data elements.
- Customers can restrict access to only specific IP addresses. IP whitelisting can be set up at the account (valid for all users) or at the user level.
- Integration with enterprise authentication services is available to securely provide identity federation using SAML protocol.
- At the application level, Treasure Data provides encryption and hashing options for datasets that are confidential or categorized as ePHI data.
- Audit logs are available to view, filter, and query an unlimited number of events for in-platform activity tracking.

Physical Safeguards

- All AWS infrastructure which stores customer ePHI is located within AWS United States regions. Treasure Data utilizes both US East (Northern Virginia) and US West (Oregon). Treasure Data also provides support in non-US regions, but not for the purposes of permanently storing ePHI.
- Treasure Data adheres to the AWS Shared Responsibility model[4] which states that the physical and environmental protection of the CDP environment hosted in AWS is owned by AWS. Therefore, Treasure Data is responsible for ensuring AWS is fulfilling their responsibilities by obtaining their annual SOC 2 Type 2 audit and reviewing all applicable controls for deficiencies.
- Treasure Data is a remote-first company with a variety of office locations globally that provide employees the ability to meet and collaborate with colleagues in-person.[5] Treasure Data's office network is completely segmented from the production network where ePHI is processed and stored.
  - » Treasure Data offices have cameras installed and badge access enabled, and access logs are maintained and periodically reviewed.
- Treasure Data's policies and procedures address the protection of laptops and removable media, regardless of location, including locking unattended laptops, proper destruction or disposal of paper, use of VPN while using public networks, and other relevant topics.
- Treasure Data utilizes a Mobile Device Management (MDM) tool to manage employee laptops and ensure automated controls are implemented, such as a baseline inactivity lockout setting. Personal laptops and/or phones are restricted from accessing systems or services which process or store customer ePHI.

Conclusion

At Treasure Data, reliability and trust is one of our top priorities. As discussed in this white paper, our security practices and safeguards, outlined by the HIPAA Security Rule, ensure that we protect the confidentiality, integrity, and security of ePHI for our healthcare and life sciences customers.

Want to learn more about the Privacy and Breach Notification rules?

Treasure Data understands that HIPAA compliance goes beyond the Security Rule. Refer to Treasure Data's Business Associates Agreement (BAA) for more information regarding our commitment to the Privacy and Breach Notification rules, such as:

1. Scope of use or disclosure of ePHI;
2. Minimum necessary uses and disclosures;
3. Individuals' rights;
4. Safeguards for the protection of ePHI; and
5. Notification of breaches and security incidents.

A copy of the Treasure Data BAA can be provided upon request to your Treasure Data Sales team prior to entering into an agreement.

References

1. Using SSE with AWS SSE-S3
2. NIST - SP 800-175B Rev. 1
3. AWS Managed Keys
4. AWS Shared Responsibility Model
5. Treasure Data Office Locations

TREASURE DATA

Treasure Data helps enterprises use all of their customer data to improve campaign performance, achieve operational efficiency, and drive business value with connected customer experiences. The Treasure Data Customer Data Cloud , our suite of customer data platform solutions integrates customer data, connects identities in unified customer profiles, applies privacy, and makes insights and predictions available for Marketing, Service, Sales, and Operations to drive personalized engagement and improve customer acquisition, sales, and retention. To learn more, visit www.treasuredata.com.

Request a demo today

treasuredata.com | +1 (866) 899-5386