WHITE PAPER

Security Infrastructure and HIPAA

ThoughtSpot Analytics Cloud

ThoughtSpot®

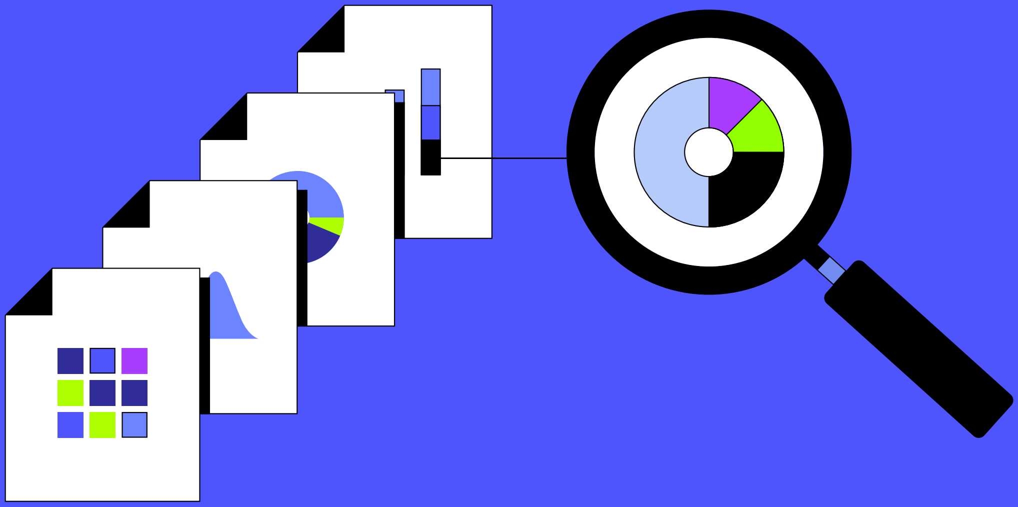


Table of contents

Disclosure

This white paper is provided for informational purposes only; it is provided "as-is" and does not constitute any explicit or implicit warranties, contractual commitments, conditions or assurances. Capitalized terms not otherwise defined herein will have the meanings ascribed in the Health Insurance Portability and Accountability Act of 1996.

Information and views expressed in this white paper, including URL and other Internet website references, may change without notice. This white paper does not provide any legal rights to any intellectual property in any ThoughtSpot product. This white paper is designed to be a broad overview of available security measures and product features, and is not legal advice; please consult with your own counsel to familiarize yourself with the HIPAA requirements applicable to your business.

The content contained herein is current as of December 2023 and represents the status quo as of the time it was written. See the ThoughtSpot Trust Center for the latest information.

Introduction

ThoughtSpot safeguards all customer data with rigorous measures regardless of its type or sensitivity. This white paper is intended to help ThoughtSpot customers understand the security controls available within ThoughtSpot Analytics Cloud to address the security and privacy requirements of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and related laws and regulations. For ease of reference, the terms "Covered Entity" and "Business Associate" used herein will have the meanings ascribed to each in HIPAA.

The information in this document is not intended to serve as an exhaustive attestation of ThoughtSpot's compliance with HIPAA requirements. We recommend Covered Entities reach out to their ThoughtSpot account team to schedule a more detailed discussion with ThoughtSpot's security team about our security infrastructure and available controls within the platform.

01

What is ThoughtSpot Analytics Cloud?

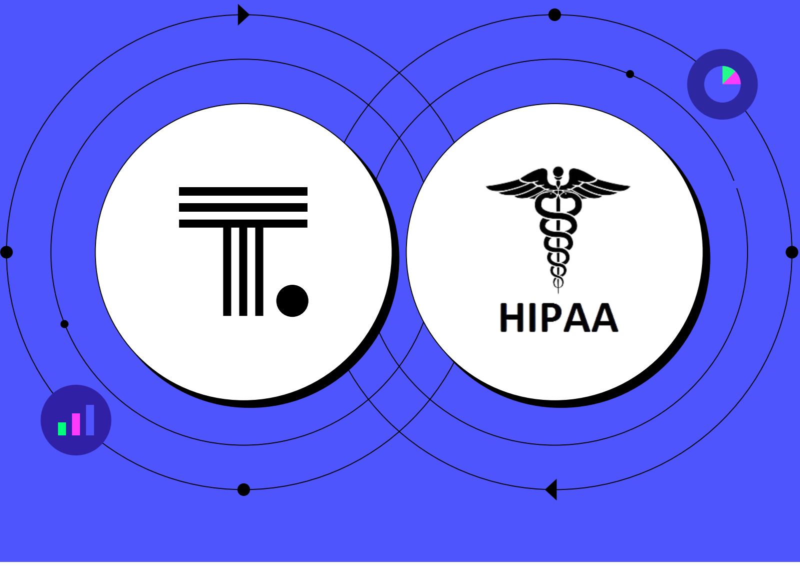
ThoughtSpot empowers everyone to create, consume, and operationalize data-driven insights. Our consumer-grade search and AI technology delivers true self-service analytics that anyone can use, while our developer-friendly platform, ThoughtSpot Everywhere, makes it easy to build interactive data apps that integrate with your existing cloud ecosystem.

To understand how ThoughtSpot Analytics Cloud interacts with any potential electronic protected health information ("ePHI"), it is important to understand how it operates and interacts with the connected cloud data warehouse (e.g., Amazon Redshift, Snowflake, or others). Delivered as a cloud-based, fully-managed SaaS experience, users can interactively ask live, ad-hoc questions via a search bar to uncover insights in their data from their cloud data warehouse. Provided on a one-to-many business model, it runs the same operational infrastructure, support organization, security infrastructure, and version, for all of ThoughtSpot's global customers.

ThoughtSpot Analytics Cloud does not extract data from the data warehouse to perform searches, and no data is categorized as sensitive, patient information, personal health information, or any other schema.

Data remains stored in a data warehouse of the customer's choosing, and searches are executed in the data warehouse. Search results, presented as best-fit visualizations, are not stored in ThoughtSpot, but reconstructed in the user's browser when a user clicks to view a visualization. Data available for search is not moved to ThoughtSpot Analytics Cloud.

Each customer has the opportunity to identify what terms it wants to index and tokenize for use as search terms called "query tokens" that are auto-populated in the search bar as the user types. However, query tokens are not necessary for full use of ThoughtSpot Analytics Cloud. Customers have complete control over what terms are indexed as query tokens in their sole discretion, and ThoughtSpot does not review or qualify query tokens at any time.



02

ThoughtSpot and HIPAA

Patients place their trust in the healthcare industry and expect their providers of healthcare and related insurance coverage to be good stewards of their health information, including addressing HIPAA standards to protect the privacy and security of protected health information where applicable.

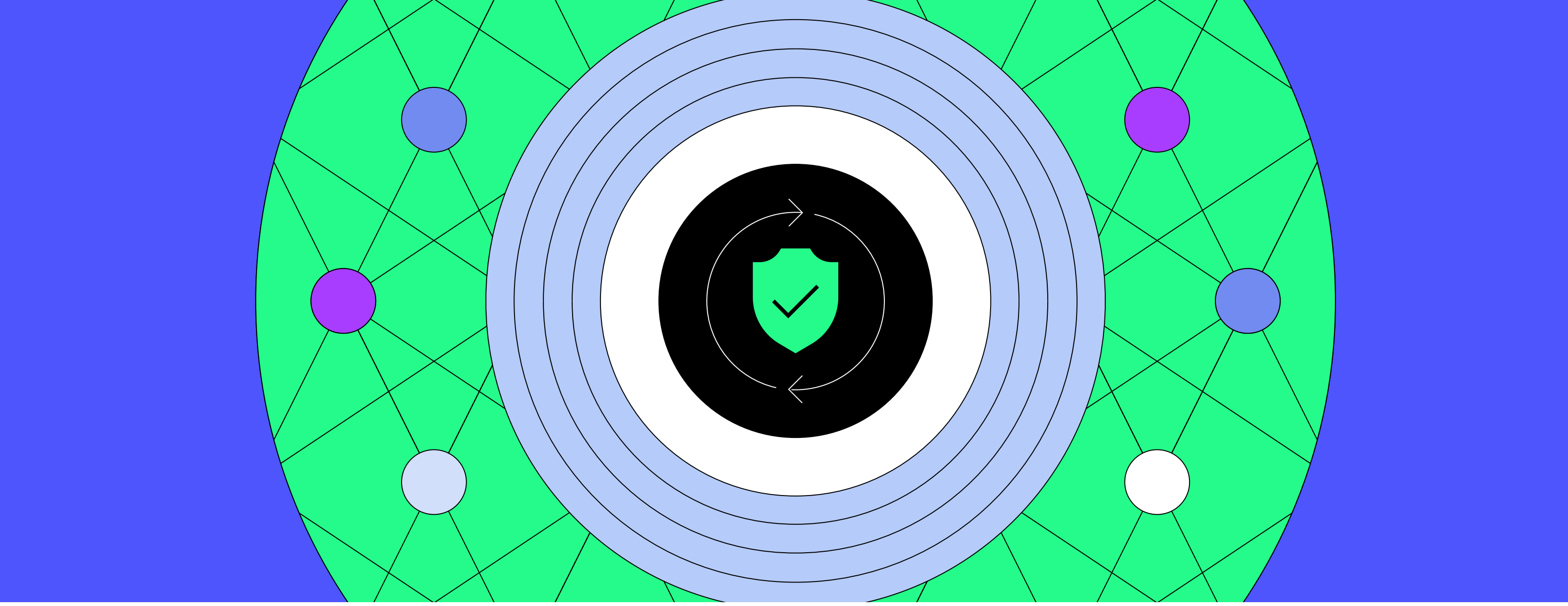
ThoughtSpot recognizes the value and importance of HIPAA to the industry and patients, and so has designed an infrastructure environment that enables it to comply with the provisions of HIPAA applicable to its capacity as a Business Associate. In addition, ThoughtSpot provides customers with customer-controlled security features in ThoughtSpot Analytics Cloud which may help Covered Entities address stringent security requirements.

ThoughtSpot's inherent features, limited data exposure, and infrastructure governance supports a Covered Entity's compliance with HIPAA, but using ThoughtSpot Analytics Cloud does not alone impart compliance to patient data management. A Covered Entity is responsible for ensuring that it has an adequate compliance program and internal processes in place, and that its use of ThoughtSpot Analytics Cloud aligns with HIPAA requirements. ThoughtSpot does not inspect, qualify, or monitor a customer's use, use cases, indexing choices, or types of data.

Recognizing the security and privacy challenges facing Covered Entities, ThoughtSpot developed ThoughtSpot Analytics Cloud to include options and features that enable its healthcare customers to comply with privacy and security requirements stipulated by law.

These requirements include:

- Ensuring the confidentiality, integrity, and availability of ePHI that the organization creates, receives, maintains, or transmits as customer data
- Protecting against any reasonably anticipated threats and hazards to the security or integrity of ePHI.
- Protecting against reasonably anticipated uses or disclosures of such information not permitted by the Privacy Rule.
- Ensuring compliance by the workforce.



03

ThoughtSpot Security Infrastructure and Architecture

Protecting the security and privacy of our customers' data is a top priority for ThoughtSpot.

ThoughtSpot maintains a rigorous, formal, and comprehensive security program that takes into account the state of the art, the nature and purposes of the service, the legal environment, and our customers' need for security and confidentiality. The ThoughtSpot Information Security team monitors, evaluates, and adjusts this security program in light of changing technology and the changing legal and business environments in which it operates. For more information, please visit the ThoughtSpot Trust Center.

Certification and Attestation

ThoughtSpot has made significant investments in technology, processes, and expertise to ensure that ThoughtSpot Analytics Cloud meets the most stringent global standards for performance, scalability, security, privacy, and compliance.

ThoughtSpot has established and maintains sufficient controls to meet the objectives stated in ISO 27001 and SOC 2 Type 2 (or equivalent standards) and, at least once per calendar year, ThoughtSpot utilizes an independent third-party auditor to test against such standards and audit methodologies. You may request the executive summaries of these reports from your ThoughtSpot account team.

Encryption

All data flowing across the global network that interconnects our data centers is automatically encrypted. ThoughtSpot encrypts any data received in transit and at rest to ensure that only authorized users can access it. Encryption keys are encrypted using a secure vault.

Policies and Procedures

It is ThoughtSpot policy to treat all data that is received into ThoughtSpot Analytics Cloud as confidential and treated with the highest sensitivity and in accordance with the controls described herein. To ensure that the data is treated properly, ThoughtSpot's information security team has implemented and enforces a number of policies and procedures designed to ensure the security of your data.

Please see the ThoughtSpot Subscription Service Program Guide for more information, and contact your ThoughtSpot account team to assist you with receiving access to documentation your organization needs to help support internal audit and assessment requirements, prepare for audits, and address regulatory requirements.

Relative to HIPAA compliance, ThoughtSpot keeps ePHI secure in ThoughtSpot Analytics Cloud by implementing administrative, technical, and physical security safeguards that apply to all customers by default such as:

Administrative

- **Data selection**
  Select only relevant source data tables to make available for analysis.
- **Data removal**
  Data no longer needed on an updated liveboard or answer is proactively deleted.
- **Admin access**
  Access privileges of ThoughtSpot employees are based on job requirements using the principle of least privilege access and are revoked upon termination of employment. Entitlements are reviewed semi-annually.
- **Zero trust policies**
  Multiple services monitor, detect, and protect against common attack vectors.
- **Activity audit logs**
  You have access to user login and activity logs that are secured and monitored for anomalies.
- **Account termination**
  All data along with the tenant instance is deleted upon termination or expiration of the agreement or order form.

Technical

- **Privileges**
  Assign users, roles and privileges with differentiated access and available actions. Using a role-based approach provides a highly granular and flexible method for assigning and controlling access.
- **Content sharing**
  Allocate user privileges to share content, with ability to revoke access to previously shared content as needed.
- **Data security rules**
  Set granular object, column, and row-level security rules to control what users are permitted to see.
- **Data encryption**
  Comprehensive support for data encryption at rest and in transit, leveraging AES 256-bit encryption and keys unique to each customer.
- **Data encryption**
  Comprehensive support for data encryption at rest and in transit, leveraging AES 256-bit encryption and keys unique to each customer.
- **Analytics at the source**
  Your data remains stored in the data warehouse of your choice, and queries are performed live, in- database. No data movement required.
- **Authentication**
  ThoughtSpot supports multi-factored authentication, LDAP, and integrates with various identity providers via SAML.
- **Tenant isolation**
  Fully isolated tenants to prevent data leakage and provide protection against unauthorized access.

Physical

- **Facilities**
  ThoughtSpot secures its buildings and workspaces from unauthorized access to protect ThoughtSpot personnel, assets, and data. All ThoughtSpot employees, as well as contractors and third-parties, with a legitimate business need to physically access any ThoughtSpot facilities must comply with the security requirements to ensure maximum security.

- **Personnel**
  ThoughtSpot conducts background checks on all employees in accordance with relevant laws and regulations, and proportional to the business requirements, the sensitivity of the information to be accessed, and the perceived risks in accordance with ThoughtSpot's Background Check Policy.

- **Access**
  All employees who need data center access must first apply for access and provide a valid business justification. These requests are granted based on the principle of least privilege and are reviewed.

04

ThoughtSpot as a Business Associate

A Covered Entity, such as a healthcare provider, health plan, or similar entity that is subject to HIPAA may need to disclose ePHI to a Business Associate that performs functions on the Covered Entity's behalf. HIPAA requires the Covered Entity and Business Associate to enter into a contract, known as a Business Associate agreement ("**BAA**") to ensure that the parties will appropriately safeguard ePHI. The terms of the BAA are prescribed by HIPPA and enforced by the U.S. Department of Health and Human Services. HIPAA requires that a Covered Entity obtain satisfactory assurances from its Business Associate that the Business Associate will appropriately safeguard the ePHI it receives or creates on behalf of the Covered Entity. The satisfactory assurances must be in writing, whether in the form of a contract or other agreement between the Covered Entity and the Business Associate.

ThoughtSpot will enter into a BAA if the Covered Entity customer chooses to index ePHI.

The standard ThoughtSpot BAA attests to the following:

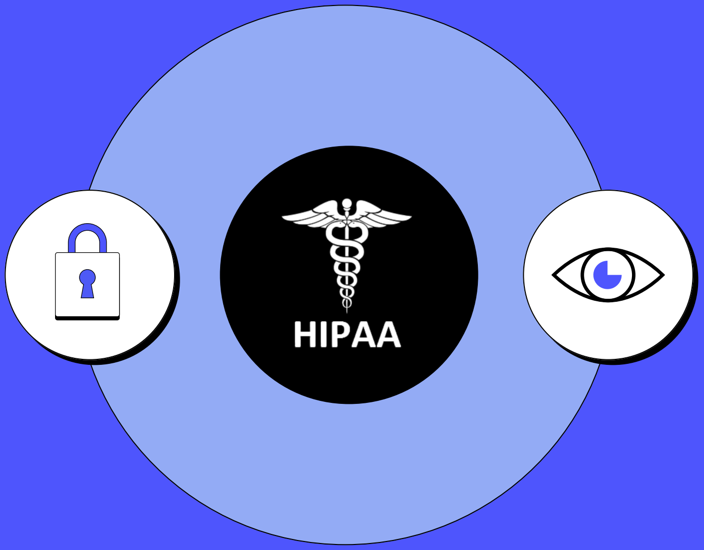
- ThoughtSpot has implemented appropriate safeguards to protect the customer data, including ePHI contained therein.
- ThoughtSpot will comply with provisions applicable to Business Associates, including the Security Rule (45 CFR Part 160 and Subparts A and C of Part 164). In summary, the Security Rule requires appropriate administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of ePHI.
- ThoughtSpot will comply with applicable requirements of the Privacy Rule (45 CFR Part 160 and Subparts A and E of Part 164). In summary, the Rule requires appropriate safeguards to protect the privacy of personal health information and sets limits and conditions on the uses and disclosures that may be made of such information without patient authorization. The Privacy Rule also gives patients control over their health information, including rights to examine and obtain a copy of their health records, and to request corrections.
- ThoughtSpot will comply with applicable requirements of the Breach notification (Subpart D of 45 CFR Part 164). In summary, the Rule requires HIPAA Covered Entities and their Business Associates to provide notification following a breach of unsecured protected health information. The ThoughtSpot BAA sets forth notification requirements that ThoughtSpot follows in the event of any data breach or suspected data breach so that the customer can comply with HIPAA's breach notification requirements.
- ThoughtSpot will have written agreements with any subcontractors who may have access to or will otherwise use or disclose customer data (which may contain ePHI) to ensure compliance with HIPAA.

While ThoughtSpot enters into a BAA with customers that may process ePHI within ThoughtSpot Analytics Cloud, it is important to understand that ThoughtSpot is not a typical Business Associate.

For example, some BAAs require Business Associates to provide an individual access to its ePHI within their "Designated Record Set" and within a prescribed period of time.

However, ThoughtSpot’s customers are able to and are responsible for providing access to individuals who request for access to their ePHI directly by using the connected data warehouse that is the source for such data, which contains all relevant information, and to which ThoughtSpot has no access.

ThoughtSpot will not enter into a BAA that requires ThoughtSpot to carry out the customer's obligations under HIPAA as the Covered Entity.



05

HIPAA Security Standards and Implementation Specifications

One of the goals of HIPAA is to safeguard individuals' ePHI. Per the U.S. Department of Health and Human Services ("**HHS**"), the HIPAA Security Rule sets national standards for protecting the confidentiality, integrity, and availability of electronic protected health information.

The Security Rule requires Covered Entities to maintain reasonable and appropriate administrative, technical, and physical safeguards for protecting ePHI as described in the above section (ThoughtSpot and HIPAA). By following guidelines for administrative, technical, and physical compliance with HIPAA, the Security Rule creates a framework for assessing security. The Security Rule identifies three types of security safeguards required for compliance with HIPAA:

- **Administrative safeguards –** personnel and management processes to train employees who come into contact with ePHI, detect privacy violations, and handle those violations.
- **Physical safeguards –** policies and procedures that govern adding and removing hardware, access to equipment, etc.
- **Technical safeguards** – guidelines for data encryption, data corroboration, and audit logging.

Each safeguard consists of a list of "standards," and each standard consists of "implementation specifications." The standards and implementation specifications are listed in the tables below.

While ThoughtSpot implements and maintains a security program as outlined below, safeguarding ePHI data is a shared responsibility between ThoughtSpot and its customers. Accordingly, customers have an independent obligation to comply with HIPAA and the HITECH Act and are responsible for complying with their responsibilities as Covered Entities by implementing appropriate administrative, technical, and physical safeguards to protect ePHI hosted and processed by ThoughtSpot.

Note: in the tables below (R) = required and (A) = addressable per HIPAA.

Administrative Safeguards

Standards	Sections	Implementation Specifications	ThoughtSpot Analytics Cloud Implementation
Security Management Process	164.308(a)(1)	Risk Analysis (R) Risk Management (R) Sanction Policy (R) Information System Activity Review (R)	ThoughtSpot has a formal Risk Management program based on ISO 27001 that includes an overall risk management program, risk analysis procedures, and system security reviews. Information Security Policies and an Acceptable Use Policy are in place to ensure a sanction policy is applied against workforce members who fail to comply with the security policies and procedures.
Assigned Security Responsibility	164.308(a)(2)	Assigned Security Responsibility (R)	ThoughtSpot's Head of Information Security is responsible for security and key stakeholders oversee the security program.
Workforce Security	164.308(a)(3)	Authorization and/or Supervision (A) Workforce Clearance Procedure (A) Termination Procedures (A)	ThoughtSpot screens all employees and contractors prior to employment. It performs criminal, employment, reference, and financial background checks in accordance with our internal SOPs and as allowable by law. Employee access is determined by the employee's role and function within ThoughtSpot and technical controls are in place to validate access. Access management and authorization to the instance is the responsibility of the customer. ThoughtSpot provides access control list (ACL) rules to restrict access to all database and personalization operations. Customers have the capability within their instance to configure and enforce least privileges to the appropriate personnel only. ThoughtSpot has a termination process that ensures employee and contractor access and entitlements are revoked immediately upon termination of employment.
Information Access Management	164.308(a)(4)	Isolating Health Care Clearinghouse Function (R) Access Authorization (A) Access Establishment and Modification (A)	Although ThoughtSpot does not perform the health care clearinghouse function, all ThoughtSpot customer data is isolated per the ThoughtSpot logically separated single-tenant architecture of the cloud environment on which it was deployed. Access management and authorization to the instance is the responsibility of the customer. The customer's administrator is responsible for the deployment and retirement of user credentials.

			ThoughtSpot has implemented processes and procedures to manage user-level access to systems and applications based on the least-privilege model using role-based access controls. Access is requested through a rigorous change management process and all access requires a secure VPN and multi-factor authentication. The ThoughtSpot compliance team reviews high-risk user authorizations for critical systems on a quarterly basis.
Security Awareness and Training	164.308(a)(5)	Security Reminders (A) Protection from Malicious Software (A) Log-in Monitoring (A) Password Management (A)	ThoughtSpot requires all employees to participate in an annual security awareness training that covers malware, monitoring, password management, data protection, privacy, and general security threats. Additionally, ThoughtSpot developers are specifically trained in secure coding practices (e.g., OWASP). Mandatory security training is assigned for personnel in sensitive roles where appropriate. Periodic reminders in the form of security emails, phishing tests, clean desk/clear screen checks, security policies, and other security topics are shared with employees.
Security Incident Procedures	164.308(a)(6)	Response and Reporting (R)	ThoughtSpot has a formal, documented security incident response policy, process, and workflow. Its incident response process includes event discovery, triage, escalation, notification (including customer notification) remediation, and post-mortem review. If a customer environment or data is impacted, the customer will be notified via their normal support contacts.
Contingency Plan	164.308(a)(7)	Data Backup Plan (R) Disaster Recovery Plan (R) Emergency Mode Operation Plan (R) Testing and Revision Procedure (A) Applications and Data Criticality Analysis (A)	ThoughtSpot has a comprehensive information system contingency plan (ISCP) that considers the criticality of customer data and infrastructure involved with the subscription service, and includes procedures on activation, notification, recovery and reconstitution. The plan applies to the entire ThoughtSpot Analytics Cloud offering. ThoughtSpot Analytics Cloud provides customers with business continuity in the event of an incident or outage with the use of dataless backups. ThoughtSpot backs up customer data in the same region as the ThoughtSpot Cloud Analytics tenant on an hourly, daily, and weekly basis. ThoughtSpot has a target recovery point objective (RPO) of 24 hours and recovery time objective (RTO) of two hours. The Disaster Recovery and Business Continuity Procedure controls are validated on an annual basis to ensure the continuation of critical business processes during the event of an emergency.

Evaluation	164.308(a)(8)	Evaluation (R)	ThoughtSpot performs periodic evaluations of security requirements and controls. Additionally, third-party evaluation of security-related controls is performed on an annual basis (ISO27001, and SOC 2). ThoughtSpot has technical evaluation of its application through its application penetration testing program, which includes major release penetration testing by a third-party vendor contracted by ThoughtSpot and customer penetration testing. Periodic technical and nontechnical evaluations are performed based upon standards implemented and/or in response to environment or operational changes affecting security. However, given the nature of services provided by ThoughtSpot to its customers, all customer data (including potential ePHI stored in ThoughtSpot Analytics Cloud) is treated equally as 'Customer Confidential' data.
Business Associate Contracts and Other Arrangement	164.308(b)(1)	Written Contract or Other Arrangement (R)	Customers potentially storing ePHI in their instance can enter into the ThoughtSpot BAA to ensure compliance with HIPAA, as amended by the Omnibus Rule. Customers have full control over what data is used in their instance. ThoughtSpot treats all customer data equally, and any customer data that is stored or processed by a ThoughtSpot instance is classified internally as 'Customer Confidential' regardless of the data classification determined by the customer. ThoughtSpot Analytics Cloud is hosted in a third-party hosting provider data center facility and ThoughtSpot receives satisfactory assurances as required under HIPAA from such providers. However, ThoughtSpot does not allow third-party vendors to access customer data and so ThoughtSpot does not maintain BAAs with its vendors regarding the services to its customers.

Physical Safeguards

Standards	Sections	Implementation Specifications	ThoughtSpot Analytics Cloud Implementation
Facility Access Controls	164.310(a)	Contingency Operations (A) Facility Security Plan (A) Access Control and Validation Procedures (A) Maintenance Records (A)	The ThoughtSpot Business Continuity Plan considers the criticality of customer data and infrastructure involved with ThoughtSpot Analytics Cloud, and includes procedures on activation, notification, recovery and reconstitution. ThoughtSpot Analytics Cloud is hosted in data center colocation facilities which inherit physical security and environmental controls from third-party hosting providers. Additionally, ThoughtSpot controls and grants access to the dedicated cages in which ThoughtSpot equipment is hosted. Data center access controls are met through a combination of provider-implemented controls and ThoughtSpot-implemented controls. ThoughtSpot reviews independent audit reports, or equivalent certifications, that address physical security and environmental controls implemented at third-party hosting providers. ThoughtSpot stores all customer data in secure data centers that are equipped with 24/7 onsite security of the data center provider, extensive CCTV networks, multiple levels of entry to gain access to the data center halls, visitor control procedures, and biometric access controls. All access- and security-related changes to the physical components of the ThoughtSpot facility within the data center are authorized, monitored, and logged.
Workstation Use	164.310(b)	Workstation Use (R)	ThoughtSpot workstations may incidentally access customer data during support engagements and similar events. They do not otherwise process, transmit, or maintain customer data; customer data always resides within the secure data center environment. ThoughtSpot has policies and technical security controls that ensure its workstations are properly used. These controls include the mandatory use of an isolated and secure access facility when events that may require interaction with customer data are necessary. Employees are not able to access, export or otherwise transfer customer data outside of this facility, and all access is logged and monitored.

Workstation Security	164.310(c)	Workstation security (R)	ThoughtSpot implements technical security controls on all workstations to ensure they are properly secured (e.g., all workstations use full disk encryption and password- based authentication). All workstations are equipped with centrally managed firewall and antivirus technologies as well as always on VPN technology.
Device and Media Controls	164.310(d)(1)	Disposal (R) Media Re-use (R) Accountability (A) Data Backup and Storage (A)	ThoughtSpot has implemented policies and procedures that govern media and device security controls, customer data handling, information security standards, and secure data deletion. ThoughtSpot follows NIST 800-88 recommendations for the proper disposal of hard drives (no tape media is used) and for proper media reuse. ThoughtSpot does not use removable media within its cloud operations environment. Movements of hardware controlled by ThoughtSpot and receiving customer data are authorized, logged, and monitored using the ThoughtSpot configuration management database. Customers can export their data from ThoughtSpot Analytics Cloud at any time. It is their responsibility to protect data once it leaves ThoughtSpot.

Technical Safeguards

Standards	Sections	Implementation Specifications	ThoughtSpot Analytics Cloud Implementation
Access Control	164.312(a)(1)	Unique User Identification (R) Emergency Access Procedure (R) Automatic Logoff (A) Encryption and Decryption (A)	Access management, including authorization, for the instance is the responsibility of the customer. ThoughtSpot utilizes an access control list to restrict access to all database and personalization operations. ThoughtSpot Analytics Cloud provides the ability to view and terminate individual user sessions, lock out users from the system, manage passwords, and inactivate users. The default session timeout on each instance can be adjusted to each customer's own requirements. Customers have the ability to configure and enforce role- based privileges to the appropriate personnel based on business requirements. ThoughtSpot grants systems and applications access based on the requestor's job functions, and on a need-to- know basis. Entitlement reviews of high-risk systems are done on a quarterly basis. All customer data is encrypted at rest with AES256 bit encryption. Access control is a shared responsibility between ThoughtSpot and its customers, as customers have control over the implementation and use of most of the access control features within the service.
Audit Controls	164.312(b)	Audit Controls (R)	System activities are logged both from an infrastructure perspective as well as from within the application. ThoughtSpot monitors all infrastructure logs. ThoughtSpot Analytics Cloud writes detailed log and activity information that is stored in the virtual environment. ThoughtSpot has implemented log management procedures that describe the process of leveraging logs created by devices and applications throughout the ThoughtSpot global infrastructure. These procedures are intended to facilitate security controls, support regulatory requirements, and maintain an accurate event audit trail. ThoughtSpot has established procedures for the security operations team to perform daily, weekly, and other periodic reviews of information system and operational activities and reporting of high-risk issues to security leadership.

Integrity	164.312(c)(1)	Mechanism to Authenticate Electronic Protected Health Information (A)	ThoughtSpot does not perform content monitoring or data loss prevention because the data analyzed remains stored in the customer’s chosen data warehouse. The nature of the ThoughtSpot Analytics Cloud platform makes the determination of alteration or loss of data impossible. As an alternative, customers can elect not to index and tokenize sensitive information at the column, table, or worksheet level. Such information would remain searchable by using chart interface features in ThoughtSpot, but would not auto-populate in the search bar while the user is typing.
Person or Entity Authentication	164.312(d)	Person or entity authentication (R)	Access management for ThoughtSpot Analytics Cloud is the responsibility of the customer. ThoughtSpot supports local authentication, LDAP-based authentication (including Active Directory), and SAML- based and SSO solutions for customer instances. ThoughtSpot access to the production environment is controlled through an IPSec VPN tunnel using two-factor authentication.
Transmission Security	164.312(e)(1)	Integrity Controls (A) Encryption (A)	Customer data is always encrypted using transport-layer security (“TLS”) when traversing public networks. ThoughtSpot also supports TLS encryption for email, FTP/S for file transfers, and secure LDAP for Active Directory and/or LDAP queries. Encryption at rest is applied on all storage devices to include production and backup devices. In addition, user passwords for built-in authentication are stored at rest as hashed values using one-way hashing algorithms.

In addition to the safeguards, there are additional requirements as listed below.

Policies and Procedures Documentation

Standards	Sections	Implementation Specifications	ThoughtSpot Analytics Cloud Implementation
Policies and Procedures	164.316(a)	Policies and procedures (R)	While ThoughtSpot is not directly required to comply with regulatory requirements (other than SOX, SEC (as applicable), and Business Associate requirements under HIPAA), ThoughtSpot provides a cloud-based software solution to its enterprise customers whose regulatory requirements in many cases extend scope to include our application and our business processes. ThoughtSpot documents and reviews changes to the policies and procedures via its managed document program and document control procedures. Thus, ThoughtSpot has implemented reasonable and appropriate policies and procedures to comply with the standards, implementation specifications, or other requirements of this subpart. ThoughtSpot regularly reviews and updates documentation, as needed, with the changing legal and regulatory landscape.
Documentation	164.316(b)	Updates (R) Time limit (R) Availability (R)	While there is no explicit HIPAA policy or procedure implemented to specifically meet compliance with this subpart section of the HIPAA Security Rule, reasonable and appropriate measures have been implemented to maintain a record of any action, activity or assessment, where required by this subpart. These records, actions, activities, or assessments are maintained on an internal ThoughtSpot-managed platform, in the form of control test definitions and activities. Upon contract expiration or exit, all hosted data is deleted, but data will remain available in its location stored in the customer's data warehouse.
General Rule	164.410(a)	Breaches treated as discovered	ThoughtSpot does not perform the function of a Covered Entity. ThoughtSpot reports both incidents and security incidents in accordance with its incident management process and security incident response plan. If a customer instance or customer data is impacted, the customer will be notified via their designated contacts. As the Covered Entity, it is the responsibility of the customer to notify media and/or individuals of breach of unsecured PHI/ePHI, with content as per the requirements on the HHS Website, and within the required timeline. ThoughtSpot will provide its Covered Entity customers with other available information that the Covered Entity customer is required to include in notification to applicable entities (or individuals), to the extent such information is available in the ordinary course of operating the subscription service.

Organization Requirements

Standards	Sections	Implementation Specifications	ThoughtSpot Analytics Cloud Implementation

Business Associate Contracts	164.314(a)
	164.504(e)
		Business associate contracts or other arrangements (R)
		Other requirements for contracts and other arrangements
		Business associate contracts with subcontractors
			ThoughtSpot does not perform the function of a Covered Entity or government entity.
			If ThoughtSpot uses subcontractors that process PHI or ePHI of customers, then it would enter into Business Associate agreements or other contractual commitments that are aligned with the requirement of HIPAA.

Conclusion

ThoughtSpot's operation of ThoughtSpot Analytics Cloud complies with the provisions of HIPAA that are required and applicable to it in its capacity as a Business Associate as described above for customers that are HIPAA-regulated entities and choose to utilize ePHI in ThoughtSpot Analytics Cloud following signature of a BAA with ThoughtSpot.

As discussed in this white paper, ThoughtSpot also offers customer-controlled security features that may be implemented by customers in their respective uses of ThoughtSpot Analytics Cloud.

These features can serve as a set of tools to help its customers address certain security requirements.

Further Reading

- ThoughtSpot Trust Center
- ThoughtSpot Documentation
- ThoughtSpot Business Associate Addendum

  Please request this from your Account Executive
- ThoughtSpot Security documentation

  Please request this from your Account Executive

ThoughtSpot®

About ThoughtSpot

ThoughtSpot is the Modern Analytics Cloud company. With ThoughtSpot, anyone can leverage natural language search and AI to find data insights and tap into the most cutting edge innovations the cloud data ecosystem offers, extend the value of their data to partners and customers, and automate entire business processes.

444 Castro Street, Suite 1000, Mountain View, CA 94041

Every effort has been made to ensure the accuracy of this document. However, ThoughtSpot, Inc., makes no warranties with respect to this document and disclaims any implied warranties of merchantability and fitness for a particular purpose. ThoughtSpot, Inc. shall not be liable for any error or for incidental or consequential damages in connection with the furnishing, performance, or use of this document or examples herein. The information in this document is subject to change without notice.

THOUGHTSPOT.COM