



# PingCAP HIPAA Whitepaper





# Table of Contents

Overview	3
HIPAA/HITECH	3
Definition	3
HIPAA/HITECH Introduction	3
Shared Responsibility Model	4
TiDB Cloud Security Responsibilities	4
Customers Security Responsibilities	4
Privacy Protection Control	5
Data Subject Right Response	5
Compliance Record Retention	5
Security Controls	5
Administrative Safeguard	6
Security Organization and Management	6
Security Awareness Training	6
Security Risk and Vulnerability Management	7
Business Continuity and Disaster Recovery	7
Technology Safeguard	8
Data Encryption	8
Key Management	9
Access Control	9
Log Audit	10
Physical Safeguard	11
Facility Access Control	11
Device and Media Control	11
Cloud Infrastructure Security	11
Incident Management and Breach Notification	11
Business Associate Agreement	12
Security/Privacy Qualification and Regulation Compliance	12
Conclusion	13



# Overview

PingCAP is an enterprise-level open-source distributed database service provider founded in 2015, providing open-source distributed database products, solutions and consulting, technical support, and certification training services. We are committed to providing global customers an open, efficient, secure, reliable, and compatible data service platform to boost productivity and accelerate enterprise digital transformation and upgrade.

Under HIPAA, PingCAP is a Business Associate. This HIPAA Whitepaper (the "Whitepaper") provides an overview of the roles and responsibilities under HIPAA, an introduction to our products' security features and capabilities, and that can support developers and customers who are subject to HIPAA requirements.

The White Paper is suitable for small, medium, and large businesses and individual customers who use PingCAP products. It outlines PingCAP's latest shared responsibility model, privacy protection, and security measures and is subject to regular updates.

## HIPAA/HITECH

### Definition

**Protected Health Information (PHI):** Health information maintained or transmitted by covered entities or business associates in any form or media (including paper or electronic). The identifiable health information created, received, maintained, or transmitted electronically is defined as electronically protected health information (ePHI).

**Covered Entities:** A health plan, health care clearinghouse, or health care provider who transmits any health information electronically in connection with a transaction, such as claiming health care compensation to a health plan.

**Business Associate:** An individual or entity, but other than in the capacity of a member of the workforce of such covered entities, performs a function or activity on behalf of the covered entity, including creating, receiving, maintaining, or transmitting protected health information.

**Business Associate Agreement (BAA):** An agreement between covered entities and business associates or between business associates and their suppliers required by HIPAA to restrict business associates from appropriately protecting PHI and specify under what condition business associates could process and disclose PHI.

### HIPAA/HITECH Introduction

The Health Insurance Portability and Accountability Act (HIPAA) was signed in 1996. It regulates various healthcare industries, including transaction rules, identification of medical service providers, identification of practitioners, medical information security, medical privacy, health plan identification, the first report of injury, illness reporting, and patient identification.

In 2009, the issue of HITECH strengthened HIPAA in several ways, including extending the scope of security rules to the business associates of covered entities. In addition, business associates should also comply with the new privacy rules and breach notification rules.

The Privacy Rule requires appropriate privacy safeguards to protect PHI and strictly limit the unauthorized use and disclosure of patient's identifiable health information. Under the Privacy Rules, patients also have rights, including access to and obtain copies of PHI and requests for corrections.



The Security Rule requires that covered entities or business associates take appropriate security measures to protect PHI created, received, used, or maintained by them. It requires appropriate administrative, physical, and technical safeguards to ensure PHI's confidentiality, integrity, and availability.

The Breach Notification Rule requires covered entities or business associates to notify stakeholders about breaches of PHI in a timely manner.

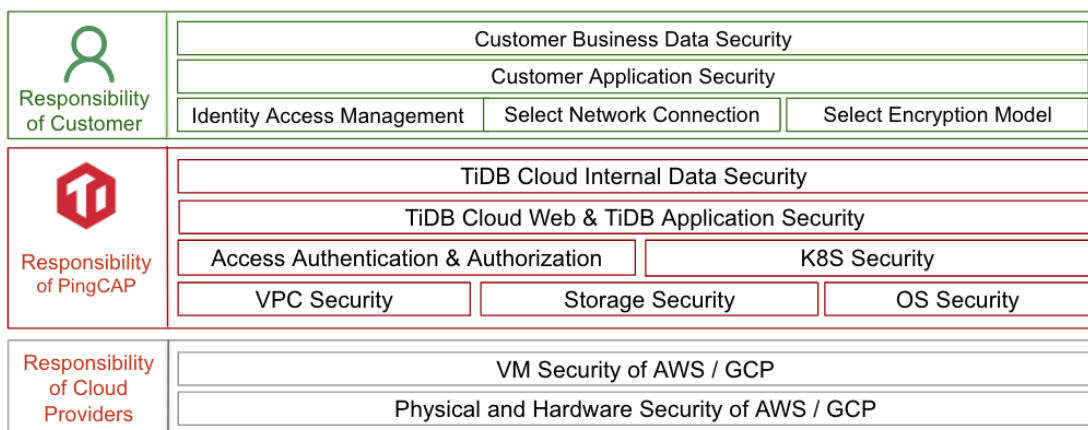
This white paper discussed both HIPAA and HITECH requirements.

## Shared Responsibility Model

PingCAP has created an open-source distributed relational database product called TiDB and a fully managed Database-as-a-Service (DBaaS) called TiDB Cloud. TiDB, as an open-source distributed relational database, can be implemented by customers with PingCAP's assistance. Customers use and maintain the database and take corresponding security responsibilities. In addition, PingCAP provides necessary technical consulting services and support upon customers' request. TiDB Cloud, as a DBaaS product, can be deployed by customers by creating a TiDB Cloud cluster on Google Cloud Platform (GCP) or Amazon Web Services (AWS) to form mission-critical applications quickly. The security responsibility of the database is shared between PingCAP, customers, and cloud service providers (GCP or AWS).

Before customers use TiDB Cloud, they should understand the security responsibility shared between PingCAP and cloud service providers. As the developer of TiDB Cloud, PingCAP is responsible for the product's security and provides database security features to meet customers' needs in different industries. On the other hand, cloud service providers (GCP and AWS) protect the cloud infrastructure; customers are responsible for any data or application stored on or connected to the cloud. A shared security responsibility model helps to reduce customers' operational efforts from multiple perspectives and, in some cases, enhances the default security level.

The following figure shows that TiDB Cloud respects cloud service providers' shared security responsibility model.



In the TiDB Cloud security sharing model, AWS and GCP are responsible for the security of physical infrastructure, computing, storage, network, and virtualization software services provided by the virtualization service layer.

### TiDB Cloud Security Responsibilities

PingCAP is responsible for the security of TiDB Cloud's VPC, Storage, OS, K8S software infrastructure, TiDB and Web platform authentication and authorization. In addition, it provides users with various security features, including optional security



authentication, secure connection, multi-layer data encryption, and operational audits to meet different customers' security control and compliance requirements.

## Customers Security Responsibilities

Customers are responsible for the security of their applications and data. They are also responsible for selecting and configuring secure identity access controls, secure connection methods, and data encryption methods to ensure applications and data are protected with adequate security measures.

## Privacy Protection Control

PingCAP provides high-quality products and services focusing on privacy protection. PingCAP is defined as a business associate under HIPAA and maps the responsibility of privacy protection that applies to a business associate to assist customers in meeting HIPAA requirements. PingCAP has established a comprehensive privacy protection management system according to the ISO 27701:2019 standard and embedded the concept of privacy protection in all aspects of product development lifecycles. PingCAP also designs and customizes privacy protection features to meet local compliance requirements in different regions.

## Data Subject Right Response

HIPAA gives data subjects a wide range of rights regarding their PHI, including the right to access, the right to request a copy, the right to amend, and the right to disclosure.

Customers shall develop and implement procedures for responding to data subject requests under HIPAA to protect data subjects' rights on their PHI.

As a business associate, PingCAP will provide the required responses and support per the Business Associate Agreement (BAA) with customers.

## Compliance Record Retention

HIPAA requires covered entities or business associates to establish policies or procedures to govern internal compliance practices and to maintain records of actions, activities, or assessments performed on PHI in paper or electronic form.

Customers should keep records of PHI processing activities and formulate corresponding protection measures to ensure PHI's confidentiality, availability, and integrity.

PingCAP has established a comprehensive privacy protection system and has formulated related policies and procedures for HIPAA compliance, with a four-tier system from top to bottom, covering the critical contents of data security and privacy protection, including the company's overall strategy, data security, and privacy management, security incident operating procedures, data breach reports. PingCAP continues to monitor changes in laws, regulations, and customer needs to adjust continuously and optimizes internal compliance practices. In addition, for HIPAA required documents, assessment reports, or test results, PingCAP has established a storage mechanism to keep them properly.



# Security Controls

The Security Rule of HIPAA applies to ePHI in electronic form created, received, maintained, or transmitted by covered entities and their business associates, requiring covered entities and business associates to implement reasonable and appropriate administrative, physical, and technical safeguards.

PingCAP has established a comprehensive information security management system per the ISO 27001:2013 standard. Information security is embedded in all aspects of the product life cycle. The security team establishes security control requirements for the company in three areas, including administrative, technical, and physical safeguards, to ensure compliance with the Security Rule of HIPAA.

## Administrative Safeguard

### Security Organization and Management

HIPAA requires covered entities or business associates to designate a security officer, develop and enforce security policies and procedures within organizations, and implement appropriate security controls to ensure security risks are manageable to protect the confidentiality, integrity, and availability of ePHI held by them.

Customers should consider designating an internal security officer, establishing security policies and procedures, implementing disciplinary actions for violations of policies and procedures, and ensuring relevant controls are effectively implemented to meet HIPAA requirements.

For organizational responsibilities, PingCAP has established a top-down security management structure to protect company and customer data, including decision-making, management, execution, and supervision layers, to ensure the effective implementation of organizational security.

- Decision-making Layer: PingCAP has appointed a security officer and formed an information security committee to be responsible for the strategy and decision-making of significant matters for PingCAP security.
- Management Layer: PingCAP has established an information security working group to be responsible for routine information security management.
- Execution Layer: PingCAP appoints leaders of each business line accountable for security risks. Their responsibilities include identifying security risks, formulating management objectives and risk remediation plans, and being responsible for the final effect of implementation.
- Supervision Layer: PingCAP has appointed an independent audit team to verify the security implementation of each business line through annual audits and is responsible for tracking audit findings until they are closed.

PingCAP has established a complete security management system following applicable laws and regulations, industry standards and best practices, including procedures, specifications, process guidelines, and operation manuals, which clearly define the purpose, scope, and requirements of security management and continue to promote effective implementation in the business field.

PingCAP adopts security control measures for pre-employment, employment, and termination of employees, including but not limited to pre-employment background checks, signing confidentiality agreements upon entry, and resignation review. PingCAP also clearly communicates information security control requirements to strengthen internal controls and reduce potential risks brought by personnel to business continuity and security. In addition, PingCAP has established an accountability system for violations of the organization's information security and privacy protection regulations. Accountability is carried out according to the severity, nature, and impact of employee violations.



PingCAP introduced a critical supplier qualification review mechanism for business associate management. For suppliers that may be involved in PHI processing, the IT department and the security department jointly review their security capabilities and HIPAA compliance capabilities and sign Service Level Agreements (SLA), confidentiality agreements, and other business agreements, which stipulate the service scope, service content, service level, security requirements, breach notification and data protection responsibilities of both parties.

## Security Awareness Training

HIPAA requires covered entities and business associates to conduct security awareness training for all employees (including management) regarding PHI protection policies and procedures.

Customers should develop an internal security awareness training program following this requirement to ensure that employees are familiar with corporate security and privacy protection policies to mitigate the risk of security breaches.

PingCAP conducts security awareness training for employees onboarding and on-the-job, as follows:

- New Employee Onboarding Training: When joining the company, employees need to complete integrated security and privacy protection training and assessment, including but not limited to information security incidents and internal company policies.
- On-the-job Security Training: PingCAP conducts targeted security training at different frequencies for employees responsible for various business modules, mainly focusing on product development security, network security awareness, customer data, and privacy protection requirements, and conducts online or offline training regularly according to business needs.

## Security Risk and Vulnerability Management

HIPAA requires an accurate and comprehensive assessment of potential risks and vulnerabilities to the confidentiality, integrity, and availability of PHI held by covered entities or business associates.

Customers shall conduct accurate and comprehensive risk assessments of products and systems that collect or process PHI.

PingCAP identifies the security risks by analyzing the value of assets and potential threats to assets and comprehensively considering the current business characteristics and scale, the protective measures taken, asset vulnerability risks, and other factors according to the ISO 27001:2013 risk assessment method. At the same time, PingCAP formulates corresponding security control measures according to the risk assessment results and re-evaluates them regularly to achieve dynamic risk monitoring and PDCA closed-loop management.

PingCAP has vulnerability identification, risk assessment, vulnerability remediation, and report management mechanisms in place to reduce the likelihood of the vulnerability of information systems and their supporting assets being exploited by external threats. PingCAP actively monitors well-known public vulnerability libraries, open-source communities, security websites, customer reports, and other information sources to find vulnerability information related to PingCAP products timely. PingCAP also regularly reviews products' security and engages third parties to perform vulnerability scanning and penetration tests to strengthen the security of the system. PingCAP evaluates the severity level of identified vulnerabilities, determines the priority based on the risk assessment results and potential impacts of vulnerabilities exploited in products or systems, and formulates vulnerability patching plans. After a vulnerability is patched, a report will be reviewed for lessons learned.



## Business Continuity and Disaster Recovery

HIPAA requires covered entities and business associates to establish disaster recovery plans and emergency operation plans to ensure timely response to emergencies or other incidents (such as fire, vandalism, system failure, and natural disasters) that could damage systems containing PHI.

Following HIPAA business continuity compliance requirements, customers should establish business continuity plans and conduct regular drills to improve emergency response capabilities in the event of business interruption caused by disasters or other events. At the same time, customers can use PingCAP database products or services to archive and backup data involving PHI to ensure that data is secure in the event of an emergency or other events that damage systems that contain PHI.

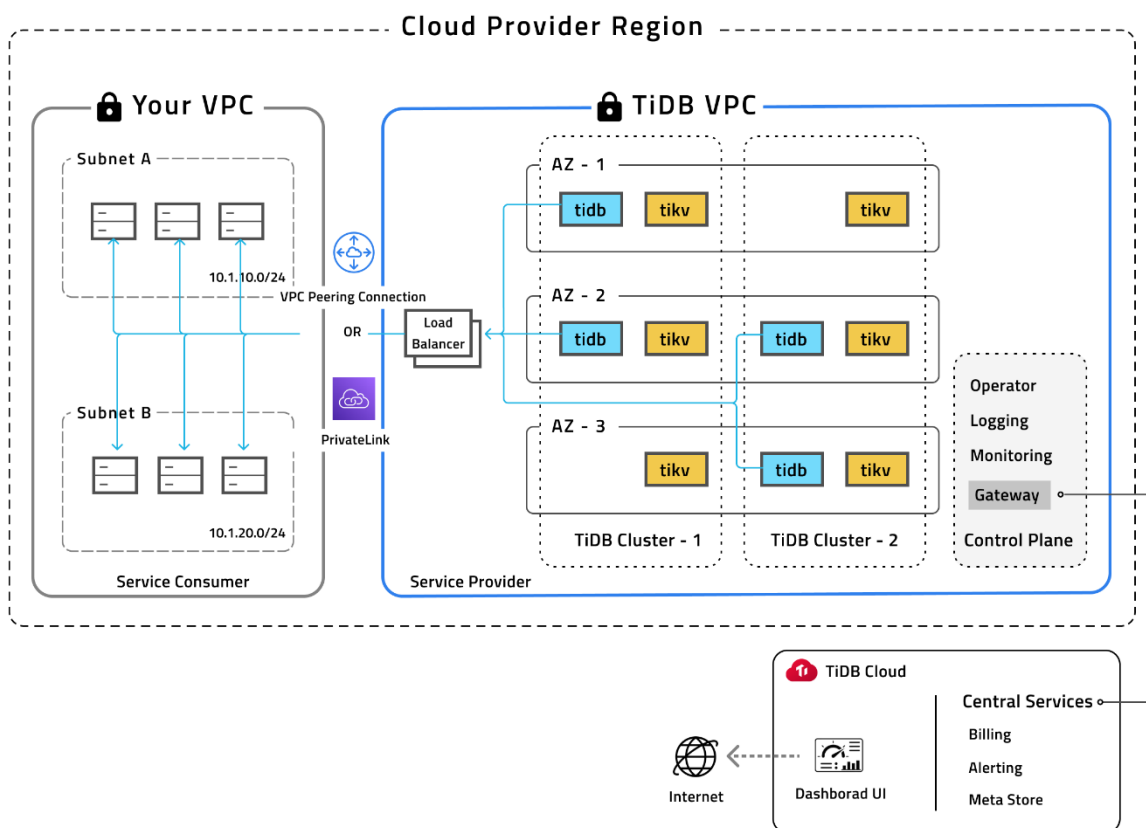
PingCAP has established a comprehensive business continuity and disaster recovery management procedure to ensure our operations and delivery are ready for unexpected events that may cause disruption. PingCAP monitors for updates of industry standards and customer needs to adjust and improve business continuity and disaster recovery management practice.

TiDB cloud, PingCAP's fully managed database as a service (DBaaS) product, is built on AWS and GCP cloud services. Each cloud server node is deployed in three GCP and AWS availability zones to build multi-zone models (as shown in figure 5-1). When one zone fails, the remaining zones can still guarantee the stability of the cluster, service availability, and data integrity. As for data backup, TiDB Cloud product provides options for customers to choose their own data backup strategy, and TiDB Cloud performs automatic full backup every day in the background and keeps backup for a certain period so that it can respond quickly and restore business availability in case of natural or man-made disasters. In addition, TiDB Cloud adopts the deployment of application-level load balancers to ensure maximum service and high availability to meet customer service requests.

PingCAP regularly performs incident drills for critical business systems to verify the resiliency of technology, communication, and personnel, including equipment downtime and network outages.



Figure 5-1, TiDB Cloud Architecture.



## Technology Safeguard

HIPAA requires covered entities and business associates to implement security policies and procedures to prevent alteration or destruction of ePHI in storage and transmission and to implement electronic verification mechanisms to protect data integrity by verifying that ePHI. Customers should consider implementing robust access control and encryption mechanisms in their application system to ensure that the ePHI is protected from unauthorized tampering or destruction and consider using industry-accepted encryption algorithms to protect ePHI.

PingCAP implemented technical measures to ensure only authorized access to data. Any unauthorized access will be discovered and notified immediately during the transmission and storage process to ensure data integrity. PingCAP database products use AES-256, an industrial standard, for application-level encryption and use key management tools to manage encryption keys. PingCAP database products are also equipped with access control functions. Customers can configure account access rights and only allow specific permission accounts to access allowed data tables to reduce the risk of unauthorized access and tampering. In addition, all operations in the database are logged, and customers can choose to enable the log audit function for subsequent review and traceability.

## Data Encryption

HIPAA requires covered entities and business associates to implement mechanisms to encrypt and decrypt PHI and procedures for creating, changing, and protecting passwords.



PingCAP has incorporated data encryption into our daily security management activities as a business associate. TiDB and TiDB Cloud also provide data encryption services, which customers can choose according to their business needs.

#### 1. Encryption in Transit

The TiDB server supports encryption connections based on the TLS (Transport Layer Security) protocol, which is consistent with MySQL encryption connections and can be directly used by existing MySQL clients, including MySQL Shell and MySQL driver. The TLS/SSL protocol versions supported by TiDB are *TLSv1.1*, *TLSv1.2*, and *TLSv1.3*.

TiDB Cloud provides TLS between TiDB Cluster components and one-way TLS services to access TiDB Cluster, which meets customers' database security access requirements and ensures the integrity of the data storage and transfer processes.

#### 2. Encryption at Rest

TiDB supports disk encryption, and customers could enable disk file encryption to prevent attackers from accessing data by reading temporary files. In the TiDB cluster, different encryption methods at rest are used for various components, and customers can choose encryption algorithms such as AES, SM4, and EBS (if the cluster is deployed on AWS) to transparently encrypt data files.

TiDB Cloud supports encryption at rest, that is, transparent encryption of data files. The AWS Key Management Service (KMS) provides a master key for management. TiDB Cloud automatically rotates those keys to encrypt TiDB data and log files.

AWS encryption at rest uses automatic transparent disk encryption and industry-standard AES-256 encryption to protect all volume (disk) data.

GCP encryption at rest uses automatic transparent disk encryption and industry-standard AES-256 encryption to protect all volume (disk) data.

### Key Management

Key Management Service (KMS) is a secure, reliable, easy-to-use key escrow service that helps customers manage and secure keys centrally. When a TiDB Cloud customer creates a TiDB Cloud cluster, the system automatically generates a CMK (TiDB Cloud managed key) in AWS KMS or GCP Service Account Key, and backups the key in the FIPS 140-2 Level 2 hardware security module. At the same time, TiDB Cloud only stores the encryption key, while the plaintext data decryption key only exists in an isolated memory buffer on the running DB instance and will never be persisted or swapped to disk. Customers could refer to TiDB Cloud security white paper for more details about key management and encryption. For more details about key management and encryption, customers could refer to TiDB Cloud security white paper.

### Access Control

HIPAA requires covered entities and business associates to develop and implement technical policies and procedures for electronic information systems with ePHI to constrain the accessibility only to persons or software programs with assessment privileges.

As covered entities, customers shall establish access control policies and procedures for electronic information systems with ePHI. When customers use PingCAP products or services, TiDB and TiDB Cloud products can assist customers in access control management.

PingCAP configured the terminal management system and establishes an account lifecycle management (LCM) procedure to update the identity information status (account ID is a unique identifier) of all employees and third-party personnel, including the process of employee onboarding, transferring, and offboarding, and third-party from joining, sharing, and termination. PingCAP developed separate authentication and network access control policies for employees when accessing highly sensitive resources and business systems. For example, when logging into the cloud infrastructure, employees can log in with enterprise-level Google



accounts and GCP accounts, with two-factor authentication, enabled to authorize permissions within the scope of their responsibilities based on roles. Furthermore, when performing high-risk configuration operations such as modifying network configurations or deleting resources, these operations can only be executed after approval by the management to ensure a higher level of security. Apart from the above, PingCAP determines appropriate access control rules, access rights, and restrictions for specific employee roles, clearly manages identity permissions, defines access policies, and predicts risks so that authorized personnel can access the right resources in different scenarios to protect critical assets from unauthorized access and potential threats.

For products, TiDB supports certificate-based login. In this way, TiDB issues certificates to different users, verifies certificates when users log in, and uses them to encrypt connections when transmitting data. TiDB uses password authentication and X.509 certificates clustering for authentication and supports access control based on users or roles. Customers can grant users permission to view, modify, or delete data objects and data schemas through roles or directly to a specific user.

#### 1. Single Sign-On (SSO)

TiDB Cloud supports Google and GitHub single sign-on, allowing customers to remotely log in to the TiDB Cloud Web Portal and manage user identity information. After logging into the TiDB Cloud, customers' company or personal data will be stored in the Auth0 database, one of the first identity providers in the industry that successfully passed the third-party Level 1 Payment Card Industry (PCI) assessment.

#### 2. Network Connection

TiDB Cloud provides a variety of network connections and access controls, supports custom IP access lists, VPC peering connections, and VPC private connections, and helps customers flexibly manage remote access control and access control between applications and databases. TiDB cluster is deployed in a dedicated AWS or GCP VPC, using authentication and IP access lists to isolate each customer resource interval, only allowing access to user groups that need to access resources, ensuring resource isolation between different customers, and ensuring that different customer resources are independent of each other and the security of the resource processing environment.

- IP Access List

Customers can set that only trusted specified IP addresses can access the database by configuring the IP access list. In contrast, other IP addresses are not allowed access, preventing unauthorized IP addresses or applications from accessing the database, thereby reducing the risk of database attacks.

- VPC Peering

VPC peering allows customers to connect their VPC to TiDB Cloud VPC, privatize routing traffic, and isolate it from the public network. In addition, when customers set up VPC peering, they can enhance the access control using the IP access list.

- VPC PrivateLink

TiDB Cloud PrivateLink can establish a secure and stable private connection between a private network VPC and services on AWS, simplify the entire network architecture, realize private network access to the business network, and avoid security risks that may be caused by accessing the business network through the public network.

## Log Audit

HIPAA requires covered entities and business associates to implement hardware, software, and/or procedural mechanisms to record and inspect activities in information systems that contain or use ePHI.

Customers should consider recording information systems that contain or use ePHI and have procedures in place to periodically audit information system activity records, such as audit logs, access reports, and security event tracking reports.



PingCAP records and regularly reviews user activities, abnormal operations, and fault warnings for business systems for daily development, O&M. At the same time, log information, as one of the key factors of event tracing, is retained in accordance with the requirements of local laws and regulations.

The log records generated by TiDB are managed and stored by customers, and PingCAP will not bring back logs without authorization. TiDB Cloud provides customers with database logging capabilities that can be used to record user access details (such as any SQL statements executed) in logs. TiDB Cloud also provides a database logging auditing function. This feature is disabled by default, and customers must enable the audit logging feature and specify audit filter rules to audit a cluster.

## Physical Safeguard

### Facility Access Control

HIPAA requires covered entities and business associates to develop and implement policies and procedures to restrict physical access to facilities in which electronic information systems are located to protect facilities and equipment from unauthorized physical access, tampering, and theft while ensuring that appropriately authorized access is allowed.

Customers should consider developing physical access control policies and procedures for information systems that contain or use ePHI and the facilities where they are located to prevent unauthorized access, tampering, and theft of facilities in the physical environment.

PingCAP's core business relies mainly on cloud services. Only routers, switches, and other infrastructure are retained in the office to ensure the operation of the internal office network. PingCAP isolates separate areas for storing special information assets or equipment in the office, such as computer rooms. An access control system between each area controls access based on personnel roles to avoid the risk of system interruption, equipment loss or damage, and data theft or tampering due to unauthorized access.

### Device and Media Control

HIPAA requires covered entities and business associates to implement policies and procedures to govern the proper use of and access to devices and electronic media containing ePHI. Covered entities should also have appropriate measures to regulate the receipt, transfer, wipe, and reuse of such devices and electronic media.

Customers should consider establishing appropriate usage and access control policies and procedures for devices and electronic media containing ePHI to manage the receipt, transfer, wipe, and reuse of such devices and electronic media.

PingCAP's current business data is stored on the cloud platform, and corresponding equipment management procedures have been implemented for devices and electronic media involving ePHI to ensure the protection of information assets, devices and electronic media.

## Cloud Infrastructure Security

As a fully managed database as a service (DBaaS), TiDB Cloud introduces the open-source Hybrid Transaction and Analytical Processing (HTAP) database TiDB to the customers' cloud. As a result, customers can create TiDB Cloud clusters to quickly build mission-critical applications on Google Cloud Platform (GCP) and Amazon Web Services (AWS).



Under this business model, public cloud services are one of the key factors supporting the business. Therefore, PingCAP regularly reviews or evaluates audit reports published by third-party cloud service providers to ensure the security and reliability of the cloud services. For the security of cloud service providers, please refer to the following links:

[AWS Compliance](#)

[GCP Compliance](#)

## Incident Management and Breach Notification

PingCAP has information security incident management policies and procedures in place, establishes a management responsibility system, and appoints the PingCAP Information Security and Privacy Protection Committee to be responsible for information security incident response to ensure security incident management policies and procedures are effectively implemented within the company. PingCAP classifies information security incidents according to multiple factors, including the nature of incidents and the impact on the company and customers. Security incidents will be handled according to the internal incident report, incident investigation and handling processes, and corrective action processes to minimize the impact of the incident.

PingCAP records the entire processing in detail while handling information security incidents, reviews and summarizes incidents after completing the processing, and regularly reviews or rehearses these records to avoid repeating the same security problem.

In addition, PingCAP has established a data breach response and notification mechanism that meets the requirements of HIPAA. PingCAP will initiate the security incident response process internally when it discovers and confirms a data breach incident. A dedicated person will be responsible for the breach investigation and material preparation. PingCAP supports customers as appropriate for data breach incidents according to customers' needs.

## Business Associate Agreement

As HIPAA requires, covered entities must enter into Business Associate Agreements (BAAs) with their business associates to ensure that business associates take appropriate steps to protect PHI from unlawful access or disclosure. Signing a BAA is also important to define both partners' responsibilities and clarify PHI's legal use scenarios.

PingCAP is regarded as a Business Associate (BA) under HIPAA and has prepared the Business Associate Agreement (BAA) according to HIPAA requirements. Customers can enter a BAA with PingCAP according to the service engaged.

## Security/Privacy Qualification and Regulation Compliance

PingCAP complies with the requirements of privacy laws and regulations where it operates and actively benchmarks against industry security compliance standards. PingCAP has obtained ISO/IEC 27001, ISO/IEC 27701, SOC 2, and PCI DSS security certification and credentials. In addition, PingCAP also received the ePrivacy seal, an EU privacy certificate verified by an authoritative third party to ensure compliance with EU GDPR requirements.

Certification	Description
ISO/IEC 27001: 2013	Information security management system is a set of security management system standards widely recognized by the industry, which has been regarded as the most authoritative and strict




	information security system certification standard in the world and is accepted worldwide.
ISO/IEC 27701: 2019	Privacy information management system: It is the first privacy information management system standard with a complete operation loop of PDCA. It details the requirements for establishing, implementing, maintaining, and continuously improving a privacy information management system, considering the privacy safeguards required for the processing of personally identifiable information (PII) in addition to information security protections.
SOC2 Audit	SOC 2 (Type II) Report: An independent third-party assurance report that specifically addresses cybersecurity and privacy standards that represent that an organization has achieved its service commitments and system requirements based on the Trust Services Standards for Security, Availability, Confidentiality, and Privacy in Section 100 of the Trust Services Standards developed by the American Institute of Certified Public Accountants.
GDPR ePrivacy GmbH Certification	The authoritative certification of global data security and privacy protection, ePrivacy evaluates through both legal and technical dimensions to ensure that products comply with the requirements of the General Data Protection Regulation (GDPR). This certification has a wide influence in the EU and even the world.
PCI DSS	Payment Card Industry Data Security Standard (PCI DSS): Designed to promote and enhance cardholder data security and facilitate the widespread adoption of global data security measures.

## Conclusion

This whitepaper helps customers to learn more about how PingCAP implements HIPAA requirements as a business associate, ensuring customers use PingCAP database services securely and confidently.

This article is for informational purposes only and has no legal effect or constitute legal advice. Customers should evaluate their use of the database services appropriately and ensure HIPAA requirements are met when using PingCAP products or services.



 <http://www.youtube.com/c/PingCAP>

 <http://linkedin.com/company/pingcap/>

 <http://twitter.com/PingCAP>

 [info@pingcap.com](mailto:info@pingcap.com)