HUAWEI CLOUD
Compliance with HIPAA

Version 1.0
Date November 2019

HUAWEI TECHNOLOGIES CO., LTD.

HUAWEI

Notice

The purchased products, services and features are stipulated by the contract made between Huawei and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided without warranties, guarantees or representations of any kind, either express or implied.

The contents of this document may be updated from time to time due to product version upgrades or other reasons. Unless otherwise specified in the contract, this document is provided as a guide only, and all statements, information, and recommendations in this document are not warranties of any kind, express or implied.

Huawei Technologies Co., Ltd.

Address: Huawei Industrial Base
Bantian, Longgang
Shenzhen 518129
People's Republic of China

Website: HUAWEI – https://www.huawei.com/en/

HUAWEI CLOUD – https://intl.huaweicloud.com/en-us/

Email: support@huawei.com

Contents

1. HIPAA Introduction

The Health Insurance Portability and Accountability Act (HIPAA)[1] was promulgated in 1996. The Act covers a range of control requirements for PHI security and privacy to enhance information sharing and improve the efficiency and quality of health care systems.

The control requirements of HIPAA[2] mainly include three parts: security rules, privacy rules and breach notification rules, which are applicable to the covered entities, including healthcare providers, health plans and healthcare clearinghouses. In addition, HIPAA also applies to the business associates of the covered entities.

The demand for digitalization across the worldwide medical industry is increasing. As a result of this digitalization, however, a number of challenges have arisen. The high availability and scalability of cloud computing make it possible for the medical industry to improve efficiency and reduce costs. HUAWEI CLOUD provides cloud services featuring high performance, high reliability, and high security, assisting medical customers to meet the requirements of HIPAA, and enabling them to use HUAWEI CLOUD services safely and with confidence.

2. Definition of Key Terms in HIPAA

- **Covered entities**

Covered entities refer to entities that need to comply with HIPAA requirements, including the following three categories:

(1) Healthcare providers: Any entity that provides medical services and conducts certain financial and administrative transactions electronically for which the United States Department of Health and Human Services (HHS) has adopted a standard.

Examples: Doctors, clinics, pharmacies, etc.

(2) Health plan: An individual or group plan that provides, or pays the cost of, medical care.

Examples: Health insurance companies, company health plans, etc.

(3) Healthcare clearinghouses: Any entity that processes or assists in the processing of health information.

Examples: Billing services, community health management information systems, etc.

- **Business associates**

A "business associate" is a person or entity, other than a member of the workforce of a covered entity, who performs functions or activities on behalf of, or provides certain services to, a covered entity that involves access by the business associate to protected health information. Business associate functions and activities may include: claims processing or administration; data analysis, processing or administration; quality assurance; billing. Business associate services may include:

[1] https://aspe.hhs.gov/report/health-insurance-portability-and-accountability-act-1996
[2] https://www.hhs.gov/hipaa/for-professionals/index.html

legal; actuarial; accounting; consulting; data aggregation; management; administrative; accreditation; and financial.

Examples: An attorney whose legal services to a health plan involve access to protected health information; a CPA firm whose accounting services to a health care provider involve access to protected health information.

- **Protected health information (PHI)**

PHI refers to personal identifiable health information maintained or transmitted by the entity or business associate in any form or medium, including paper or electronic form. Personal identifiable health information is information that identifies the individual or can be used to identify the individual based on a reasonable belief, including:

(1) Information related to the past, present or future physical or mental health of an individual;
(2) Information related to medical services provided to individuals;
(3) Information on past, present or future payment for the provision of healthcare to an individual.

- **Electronic protected health information (ePHI)**

ePHI refers to PHI created, received, maintained or transmitted in electronic form.

- **Business Associate Agreement (BAA)**

The HIPAA Rules generally require that covered entities and business associates enter into contracts with their business associates to ensure that the business associates will appropriately safeguard protected health information. *Note: Subcontractors are also regarded as business associates.*

- **Breach of PHI**

A breach is, generally, an impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of the protected health information. An impermissible use or disclosure of protected health information is presumed to be a breach unless the covered entity or business associate, as applicable, demonstrates that there is a low probability that the protected health information has been compromised based on a risk assessment of at least the following factors:

(1) The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification;
(2) The unauthorized person who used the protected health information or to whom the disclosure was made;
(3) Whether the protected health information was actually acquired or viewed; and
(4) The extent to which the risk to the protected health information has been mitigated.

Examples: Unauthorized access to the hospital's electronic medical records, a hacking in a medical service's network server that results in unlawful disclosure of health-related records, etc.

3. HUAWEI CLOUD Security and Privacy Compliance

HUAWEI CLOUD inherits Huawei's comprehensive management system and leverages its experience in IT system construction and operation, actively managing and continuously improving the development, operation and maintenance of cloud services. To date, HUAWEI CLOUD has received a number of international and industry security compliance certifications[3], ensuring the security and compliance of businesses deployed by cloud service customers.

HUAWEI CLOUD has attained the following certifications:

Certification	Description
ISO 27001:2013	ISO 27001 is a widely used international standard that specifies requirements for information security management systems. This standard provides a method of periodic risk evaluation for assessing systems that manage company and customer information.
Classified Cybersecurity Protection of China's Ministry of Public Security	Classified Cybersecurity Protection issued by China's Ministry of Public Security is used to guide organizations in China through cybersecurity development. Today, it has become the general security standard widely adopted by various industries throughout China. HUAWEI CLOUD has passed the registration and assessment of Classified Cybersecurity Protection Class 3. In addition, key HUAWEI CLOUD regions and nodes have passed the registration and assessment of Classified Cybersecurity Protection Class 4.
ISO 27017:2015	ISO 27017 is an international certification for cloud computing information security. The adoption of ISO 27017 indicates that HUAWEI CLOUD has achieved internationally recognized best practices in information security management.
Singapore MTCS Level 3 Certification	The Multi-Tier Cloud Security (MTCS) specification is a standard developed by the Singapore Information Technology Standards Committee. This standard requires cloud service providers (CSPs) to adopt sound risk management and security practices in cloud computing. HUAWEI CLOUD Singapore has obtained the highest level of MTCS security rating (Level 3).
ISO 20000-1:2011	ISO 20000 is an international recognized information technology service management system (SMS) standard. It specifies requirements for the service provider to plan, establish, implement, operate, monitor, review, maintain and improve an SMS to make sure CSPs can provide effective IT services to meet the requirements of customers and businesses.

[3] https://intl.huaweicloud.com/en-us/securecenter/safetycompliance.html

Certification	Description
SOC audit	The SOC audit report is an independent audit report issued by a third-party auditor based on the relevant guidelines developed by the American Institute of Certified Public Accountants (AICPA) for the system and internal control of outsourced service providers. At present, HUAWEI CLOUD has passed the audit of SOC2 Type 1 Privacy Principle in terms of privacy, which proves that HUAWEI CLOUD has reasonable control measures in terms of cloud management and technology.
ISO 27018:2014	ISO 27018 is the first international code of conduct that focuses on personal data protection in the cloud. This certification indicates that HUAWEI CLOUD has a complete personal data protection management system and is a global leader in the data security management domain.
PCI DSS Certification	Payment Card Industry Data Security Standard (PCI DSS) is the global card industry security standard, jointly established by five major international payment brands: JCB, American Express, Discover, MasterCard and Visa. It is the most authoritative and strict financial institution certification in the world.
ISO 22301:2012	ISO 22301 is an internationally recognized business continuity management system standard that helps organizations avoid potential incidents by identifying, analyzing, and alerting risks, and develops a comprehensive Business Continuity Plan (BCP) to effectively respond to disruptions so that entities can recover rapidly, keep core business running, and minimize loss and recovery costs.
CSA STAR Gold Certification	CSA STAR certification was developed by the Cloud Security Alliance (CSA) and the British Standards Institution (BSI), an authoritative standard development and preparation body as well as a worldwide certification service provider. This certification aims to increase trust and transparency in the cloud computing industry and enables cloud computing service providers to demonstrate their service maturity.
Gold O&M (TRUCS)	The Gold O&M certification is designed to assess the O&M capability of cloud service providers who have passed TRUCS certification. This certification confirms that HUAWEI CLOUD services operate a sound O&M management system that satisfies the cloud service O&M assurance requirements specified in Chinese certification standards.
Certification for the Capability of Protecting Cloud Service User Data (TRUCS)	This certification evaluates a CSP's ability to protect cloud data. Evaluation covers pre-event prevention, in-event protection, and post-event tracking.

Certification	Description
ITSS Cloud Computing Service Capability Evaluation by the Ministry of Industry and Information Technology (MIIT)	ITSS cloud computing service capability evaluation is based on Chinese standards such as the General Requirements for Cloud Computing and Cloud Service Operations. It is the first hierarchical evaluation mechanism in China's cloud service/cloud computing domain. Huawei private and public clouds have obtained cloud computing service capability level-1 (top level) compliance certificates.
TRUCS	Trusted Cloud Service (TRUCS) is one of the most authoritative public domain assessments in China. This assessment confirms that HUAWEI CLOUD complies with the most detailed standard for cloud service data and service assurance in China.
Cloud Service Security Certification - Cyberspace Administration of China (CAC)	This certification is a third-party security review conducted by the Cyberspace Administration of China according to the Security Capability Requirements of Cloud Computing Service. HUAWEI CLOUD e-Government Cloud Service Platform has passed the security review (enhanced level), indicating that Huawei e-Government cloud platform was recognized for its security and controllability by China's top cybersecurity management organization.
International Common Criteria EAL 3+ Certification	Common Criteria (CC) certification is a highly recognized international standard for information technology products and system security. HUAWEI CLOUD FusionSphere passed CC EAL 3+ certification, indicating that the HUAWEI CLOUD software platform is highly recognized worldwide.
ISO 27018:2014	ISO 27018 is an international code of conduct that focuses on the protection of personal data in the cloud. The adoption of ISO 27018 indicates that HUAWEI CLOUD has met the requirements of an internationally complete personal data protection and management system.
ISO 29151:2017	ISO 29151 is an international practical guide to the protection of personal identity information. The adoption of ISO 29151 confirms HUAWEI CLOUD's implementation of internationally recognized management measures for the entire lifecycle of personal data processing.
ISO 27701:2019	ISO 27701 specifies requirements for the establishment, implementation, maintenance and continuous improvement of a privacy-specific management system. The adoption of ISO 27701 demonstrates that HUAWEI CLOUD operates a sound system for personal data protection.

Certification	Description
BS 10012:2017	BS10012 is the personal information data management system standard issued by BSI. The BS10012 certification indicates that HUAWEI CLOUD offers a complete personal data protection system to ensure personal data security.

4. HUAWEI CLOUD Security Responsibility Sharing Model

The primary responsibilities of HUAWEI CLOUD are developing and operating the physical infrastructure of HUAWEI CLOUD data centers; the IaaS, PaaS, and SaaS services provided by HUAWEI CLOUD; and the built-in security functions of a variety of services. Furthermore, HUAWEI CLOUD is also responsible for the secure design, implementation, and O&M of the multi-layered defense-in-depth, which spans the physical, infrastructure, platform, application, and data layers, in addition to the identity and access management (IAM) cross-layer function.

The primary responsibilities of the tenant are customizing the configuration and operating the virtual network, platform, application, data, management, security, and other cloud services to which a tenant subscribes on HUAWEI CLOUD, including its customization of HUAWEI CLOUD services according to its needs as well as the O&M of any platform, application, and IAM services that the tenant deploys on HUAWEI CLOUD. At the same time, the tenant is also responsible for the customization of the security settings at the virtual network layer, the platform layer, the application layer, the data layer, and the cross-layer IAM function, as well as the tenant's own in-cloud O&M security and the effective management of its users and identities.

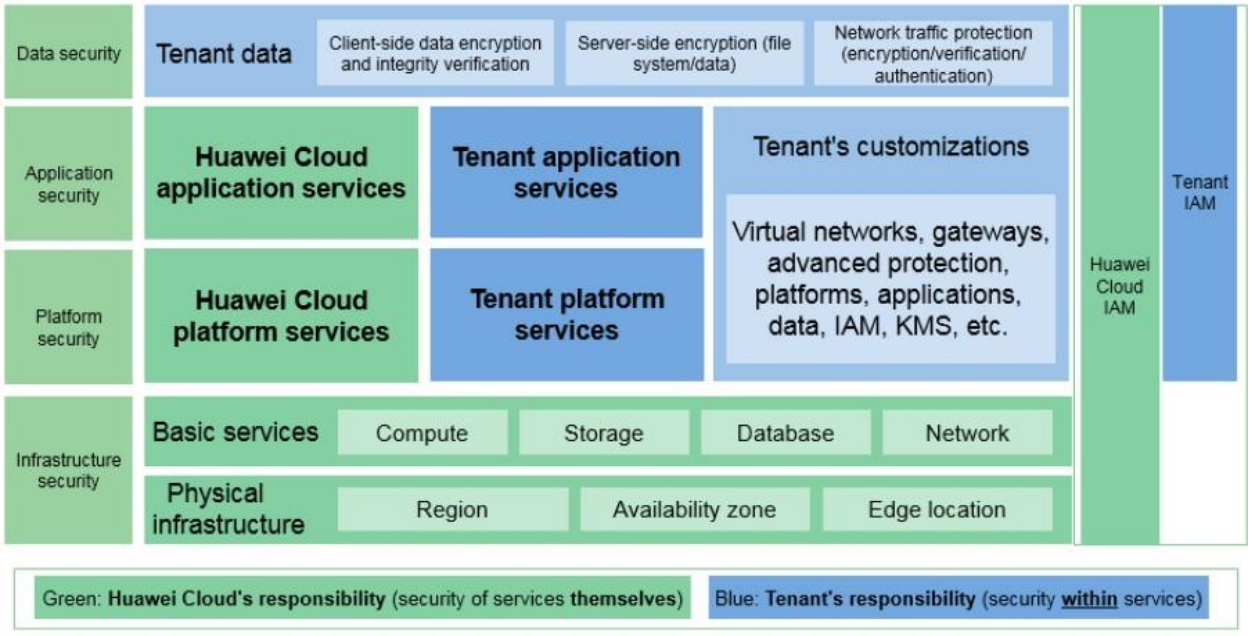

Figure 1: Responsibility Sharing Model

For details on the security responsibilities of both tenants and HUAWEI CLOUD, please refer to the *HUAWEI CLOUD Security White Paper*[4] released by HUAWEI CLOUD.

5. HUAWEI CLOUD Global Infrastructure

HUAWEI CLOUD operates services in many countries and regions around the world. The HUAWEI CLOUD infrastructure is built around Regions and Availability Zones (AZ). Compute instances and data stored in HUAWEI CLOUD can be flexibly exchanged among multiple regions or multiple AZs within the same region. Each AZ is an independent, physically isolated fault maintenance domain, Users can and should take full advantage of all these regions and AZs in their planning for application deployment and operations in HUAWEI CLOUD. Distributed deployment of an application across a number of AZs provides a high degree of assurance for normal application operations and business continuity in most outage scenarios (including natural disasters and system failures). For current information on HUAWEI CLOUD Regions and Availability Zones, please refer to the official website of HUAWEI CLOUD *"Worldwide Infrastructure"*[5].

6. HUAWEI CLOUD Privacy Protection Control

Privacy protection has always been a core element of HUAWEI CLOUD. Operating a professional privacy protection team responsible for establishing and implementing relevant controls and processes, HUAWEI CLOUD integrates its privacy protection practices and experiences into the development lifecycle of cloud services. As a result, each cloud service satisfies privacy protection compliance requirements, and provides privacy protection functions for customers to meet compliance needs. HUAWEI CLOUD's privacy protection efforts have achieved remarkable results, having been recognized by authoritative institutions both at home and abroad. For details on HUAWEI CLOUD's privacy protection and authentication, please refer to the *White Paper for HUAWEI CLOUD Privacy Protection*[6], or visit the Trust Center for more information.

6.1 Data Access

HUAWEI CLOUD deeply understands the importance of customer content data to customers. HUAWEI CLOUD has always adhered to the principle of "not accessing customer data without permission", ensuring that data is owned, used by customers and creates value for customers. In return, HUAWEI CLOUD customers have full control over their content data. They understand the location of content data storage and they can set up appropriate protection measures.

HUAWEI CLOUD adheres to the principle of "not accessing customer content data". HUAWEI CLOUD carries out operations according to customer requirements and authorization. Once a customer no longer wishes to use HUAWEI CLOUD services, HUAWEI CLOUD executes data deletion following an agreed period of time, utilizing a strict data deletion mechanism. For more

[4] https://intl.huaweicloud.com/content/dam/cloudbu-site/archive/hk/en-us/securecenter/security_doc/SecurityWhitepaper_en.pdf
[5] https://intl.huaweicloud.com/en-us/global/
[6] https://intl.huaweicloud.com/content/dam/cloudbu-site/archive/hk/en-us/securecenter/security_doc/PrivacyWhitepaper_en.pdf

information on HUAWEI CLOUD data access, please refer to the *White Paper for HUAWEI CLOUD Data Security*[7].

6.2 Commitments to Safeguarding Individual's Right to Privacy

As customers have full control over their content data, they should take steps to protect the data subject's right to privacy. HUAWEI CLOUD's Identity and Access Management and Log Tank services can enable customers to better protect the rights of data subjects. The HUAWEI CLOUD Security Control chapter of this user guide will provide more details on **Identity and Access Management (IAM)**[8] and **Log Tank Service (LTS)**[9]**.** You can also refer to the IAM and LTS on the official website.

7. HUAWEI CLOUD Security Control

HIPAA security rules establish national standards for the confidentiality, integrity and availability of electronic protected health information (ePHI). According to United States Department of Health and Human Services (HHS)[10], the primary goal of security rules is to protect the privacy of personal health information while allowing the covered entities to adopt new technologies to improve the quality and efficiency of healthcare

Unlike privacy rules, security rules only apply to ePHI in electronic form created, received, maintained or transmitted by the covered entities and its business associates. Security rules require the covered entities and business associates to implement appropriate management, technical and physical safeguards to:

- Ensure confidentiality, integrity and availability of all ePHIs created, received, maintained, or transmitted;
- Identify and defend against reasonably anticipated threats to the security or integrity of information;
- Protect against any impermissible use or disclosure;
- Ensure compliance by their workforce.

The following introduces the administrative, physical, and technical safeguards for protecting ePHI implemented by the covered entities and their business associates, as well as HUAWEI CLOUD's response to HIPAA requirements.

7.1 Administrative Safeguards

Security management process: HIPAA requires the covered entities to designate a security officer responsible for formulating and implementing its security policies and procedures. Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and

[7] https://intl.huaweicloud.com/content/dam/cloudbu-site/archive/hk/en-us/securecenter/security_doc/DataSecurityWhitepaper_en.pdf
[8] https://intl.huaweicloud.com/en-us/product/iam.html
[9] https://intl.huaweicloud.com/en-us/product/lts.html
[10] https://www.hhs.gov/

appropriate level to ensure the confidentiality, integrity, and availability of electronic protected health information. Implement procedures to regularly review records of information system activity. Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity or business associate.

Customers can record operations related to the use of cloud service resources using the **Cloud Trace Service (CTS)**[11] of HUAWEI CLOUD. CTS can record all personnel behavior relating to resource and system configuration changes, all user operations relating to the management interface, and all API operations on HUAWEI CLOUD systematically and in real time. With the help of object-level API events recorded in CTS, users can detect data breach by collecting activity data on OBS objects. As one of HUAWEI CLOUD's management services, CTS security design is built based on HUAWEI CLOUD security architecture. Four aspects are primarily covered: network security, network boundary security, application security and data security, ensuring a secure CTS is provided to tenants.

Huawei regards cyber security as one of the company's important strategies and achieves it through top-down governance structure. Adhering to Huawei's cyber security strategy and norms, HUAWEI CLOUD security team independently plans and manages security work in this field. To achieve the integration of R&D, operation and maintenance of cloud services and cloud security services in an all-round way, the organizational structure tends to be flat in order to adapt to the necessary DevOps/DevSecOps process for cloud services. HUAWEI CLOUD has developed a sound information security risk management mechanism, and regularly conducts internal and third-party penetration tests and security assessments to ensure the security of the cloud environment carrying ePHI data.

Information access management: HIPAA requires the covered entities or business associates to develop policies and procedures for authorizing access to ePHI. They must ensure proper access according to the role of the user or recipient (role-based access).

Customers can access the HUAWEI CLOUD **Identity and Access Management (IAM)** to manage user accounts that use cloud resources. IAM supports not only password authentication but also multi-factor authentication, and customers can choose to enable it. If the tenant has a secure and reliable external identity authentication service provider, the external federated identity authentication users of IAM services can be mapped to temporary HUAWEI CLOUD users and access the tenant's HUAWEI CLOUD resources. IAM supports hierarchical fine-grained authorization, enabling administrators to plan cloud resource permissions based on a user's job responsibilities. They can also set security policies for users to access cloud service systems, such as setting access control lists to restrict malicious access from untrusted networks.

HUAWEI CLOUD will not access ePHI data in principle. If required to assist customers in maintaining the system, HUAWEI CLOUD will only access data after obtaining customer authorization.

[11] https://intl.huaweicloud.com/en-us/product/cts.html

Security awareness and training: HIPAA requires the covered entities to implement a security awareness and training program for all members of its workforce (including management), and impose appropriate sanctions on staff who violate their policies and procedures.

Customers should consider formulating security training programs to educate all employees in their organizations, and should deal with security violations appropriately. In this regard, HUAWEI CLOUD is compliant with this requirement throughout the internal security management.

In order to enhance the awareness of cyber security, avoid the risk of cyber security violations, and ensure normal operation of businesses, HUAWEI CLOUD carries out security awareness education from three aspects: popularization of awareness education, publicity activities, and Huawei's Employee Business Conduct Guidelines (BCG) and the signing of commitments. In addition, HUAWEI CLOUD carries out security awareness training for all staff at least once a year.

Evaluation: HIPAA requires the covered entities to periodically evaluate to what extent their security policies and procedures meet the requirements of security rules.

Customers should consider establishing a security risk assessment or audit mechanism to regularly assess the conformity of their security policies and procedures. HUAWEI CLOUD has also applied this requirement to its own internal security management.

HUAWEI CLOUD has developed a complete information security management system with reference to ISO 27001, and established advanced HUAWEI CLOUD information security policies and procedures. HUAWEI CLOUD regularly evaluates and continuously optimizes the system in accordance with HIPAA security rules to ensure that its security policies and procedures meet the requirements of enterprise security strategy and security compliance requirements.

Emergency plan: HIPAA requires the covered entities to establish (and implement as needed) policies and procedures for responding to an emergency, or any other occurrence that damages systems containing electronic protected health information.

HUAWEI CLOUD provides multi-granularity data backup and archiving services to meet customers' requirements in specific scenarios. Customers can use the versioning function of OBS, Volume Backup Service (VBS), and Cloud Server Backup Service (CSBS) to back up in-cloud documents, disks, and servers. Benefiting from on-demand use, scalability, and high reliability features of cloud services, customers can also use the Backup and Archive Solution, backup and archiving software, and HUAWEI CLOUD infrastructure to back up on-premises data to HUAWEI CLOUD. With the DEW service, customers can encrypt backup data easily and quickly, thereby ensuring data security. To improve the emergency response capability, customers can perform the recovery drill periodically. The Backup and Archive solution allows customers to use backups to restore data in the in-cloud system. After the data is restored, resources can be released, significantly reducing the recovery drill cost.

HUAWEI CLOUD has established an effective business continuity management system and obtained ISO 22301 certification. HUAWEI CLOUD supports replication of user data in multiple data center nodes. If a single node fails, user data will not be lost, and the system can initiate

automatic detection and self-healing. In addition, HUAWEI CLOUD utilizes architecture deployed by multiple regions around the world for disaster recovery and backup of the data center itself. As well as providing high-availability infrastructure, redundant data backup, and disaster preparedness in available areas, HUAWEI CLOUD has also developed business continuity and disaster recovery plans which are regularly tested. Customers can make full use of these regions and available areas to plan the deployment and operation of application systems in the cloud. Distributed deployment of applications based on multiple available zones ensures that the system can run continuously in cases of failure, including natural disasters and system failures.

7.2 Physical Safeguards

Facility access controls: HIPAA requires the covered entities to implement policies and procedures in order to limit physical access to electronic information systems, as well as the facility or facilities in which they are housed so as to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft, while ensuring that properly authorized access is permitted.

Customers should consider strict access control over the physical environment in which the accessible ePHI information systems are located to prevent unauthorized access, tampering and theft of facilities in the physical environment. In this regard, HUAWEI CLOUD has applied this requirement to its own internal security management.

HUAWEI CLOUD has established comprehensive physical security and environmental safety protection measures, strategies, and procedures that comply with Class A standard of GB 50174 Code for *Design of Electronic Information System Room* and T3+ standard of TIA-942 *Telecommunications Infrastructure Standard for Data Centers*. The HUAWEI CLOUD O&M team enforces stringent access control, safety measures, regular monitoring and auditing, and emergency response measures to ensure the physical security and environmental safety of HUAWEI CLOUD data centers. For more details, please refer to the *HUAWEI CLOUD Security White Paper*.

Workstation security: HIPAA requires the covered entities to implement physical safeguards for all workstations that access electronic protected health information, to restrict access to authorized users only.

Customers should consider implementing physical security controls on all workstations accessible to ePHI to prevent unauthorized access to workstations. In this regard, HUAWEI CLOUD has applied this requirement to its own internal security management.

Based on business functions and network security risks, the HUAWEI CLOUD data center network is mapped into different security zones to achieve network isolation using both physical and logical controls, which boosts network immunity and fault tolerance in response to attacks from both external threat actors and malicious insiders. The Operations Management (OM) zone hosts OM components. HUAWEI CLOUD OM personnel must first log onto the Virtual Private Network (VPN) to connect to this security zone, and then log onto managed nodes through bastion hosts. HUAWEI CLOUD administrator-level personnel can access the OM interfaces of all

security zones from this security zone, which does not expose its interfaces to any other security zone. Office endpoints connected to the cloud environment strictly comply with the requirements of office equipment security management. The cloud environment needs to be accessed through bastion hosts so that the operations can be logged.

Device and media controls: HIPAA requires the covered entities to implement policies and procedures to manage the correct use and access of devices and electronic media containing ePHI. Covered entities should also have corresponding measures to manage the reception, transfer, removal and reuse of such devices and electronic media.

Customers should consider standardizing the proper use and access of devices and electronic media that may contain ePHI data. In this regard, HUAWEI CLOUD has applied this requirement to its own internal security management.

HUAWEI CLOUD has set rules for the management of storage media, servers and storage machines that store ePHI data, in order to strengthen the protection of information assets and prevent the loss of physical assets. The rule requires that storage media, servers, and storage machines should be checked and approved by the head of the demand department, and records should be kept. USB disks used in the operation and maintenance process should be checked and approved by the manager of the data center, and records should be kept. If server hard disks (and/or servers as a whole) or storage machines need to be decommissioned, the data should be removed. In addition, the security requirements for this kind of equipment and media are also defined in room migration, return to suppliers, equipment outgoing room, and decommission scenarios. When customers take the initiative to delete data, or if data needs to be deleted due to service expiration, HUAWEI CLOUD will strictly follow data destruction standards and customer agreements. To avoid loss due to microoperation following the destruction of important data and the impossibility of restoration, it is suggested that customers should consider carefully before destroying the data and make a backup of the data to be destroyed (HUAWEI CLOUD provides a data backup service. For more details, please refer to the backup service introduction outlined in the emergency plan of section 7.1 "Administrative Safeguards").

7.3 Technical Safeguards

Access control: HIPAA requires the covered entities to implement technical policies and procedures for electronic information systems that maintain ePHI to allow access only to authorized personnel.

Customers should consider enforcing strict access control over ePHI in the application system. In addition, customers can access the HUAWEI CLOUD Console to create accounts and grant privileges for those accessing Huawei's cloud resources through **Identity and Access Management (IAM)**. Each HUAWEI CLOUD customer has a unique user ID, and can configure a variety of user authentication mechanisms including account password and multi-factor authentication. IAM allows customer security administrators to set password strategies and change password cycles of different intensities according to their needs. This prevents users from setting low-strength passwords or using fixed passwords for extended periods, leading to account breach.

In addition, IAM also allows customer security administrators to set up user security groups to manage resource access rights for employees with different roles within the organization.

HUAWEI CLOUD employees do not have access to customer data unless authorized by customers. However, further cooperation with customers to meet the requirements of HIPAA require HUAWEI CLOUD Operations and Maintenance (O&M) personnel to configure management permissions in accordance with the principle of "least privilege". When accessing HUAWEI CLOUD Management Network for centralized management of the system, HUAWEI CLOUD O&M personnel must use unique employee identity accounts. User accounts are equipped with strong password security policies, and passwords are changed regularly to prevent brute force attacks. In addition, two-factor authentication involving USB keys and Smart Cards is used to authenticate O&M personnel.

Audit controls: HIPAA requires the covered entities to implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use ePHI.

Customers should consider implementing the recording of ePHI access or operation in application systems. In addition, customers can access ePHI activity records through HUAWEI CLOUD Log Tank Service (LTS) for real-time queries and activity logs dumps. Customers can also perform real-time decision analysis using log services without any development activity. In addition, LTS can be combined with **Virtual Private Cloud (VPC)**[12] and **Cloud Trace Service (CTS)**, enabling customers to manage operational records of cloud service resources through CTS, including queries, audits, and tracing of user ePHI access and operation.

Integrity control: HIPAA requires the covered entities to implement policies and procedures to protect electronic protected health information from improper alteration or destruction. Electronic mechanisms should also be implemented to confirm that electronic protected health information has not been altered or destroyed in an unauthorized manner.

Customers should consider implementing strong access control and encryption mechanisms in the application system, to ensure that ePHI is protected from unauthorized tampering or destruction. They should also consider utilizing industry-recognized encryption algorithms to protect ePHI data.

Customers can manage access control of cloud resources through HUAWEI CLOUD IAM. In addition, HUAWEI CLOUD also provides cloud resources such as the **Data Encryption Workshop (DEW)**[13] wherein the complex data encryption and decryption and key management logic are encapsulated. Customers can choose cloud hard disk EVS, object storage OBS, mirror service IMS, and cloud database (MySQL, PostgreSQL, SQL Server) with data encryption function to configure the encryption. HUAWEI CLOUD data encryption function also adopts high-strength algorithms (support RSA, DSA, ECDSA and other common asymmetric and symmetric algorithms) to store data. The encryption key can be centralized and managed by DEW throughout the life cycle. Without authorization, others cannot obtain keys to decrypt data, which ensures data security on the cloud, which ensures the security of customer’s ePHI data on the cloud.

[12] https://intl.huaweicloud.com/en-us/product/vpc.html
[13] https://intl.huaweicloud.com/en-us/product/dew.html

DEW adopts the layered key management mechanism. Specifically, after association configuration on DEW Console or using APIs, customer's master key stored in DEW encrypts the encryption keys of each storage service, while the master key is encrypted by the root key stored in HSM. In this way, a complete, secure and reliable key chain is formed. HSM is certified by international security organizations and can prevent intrusion and tampering. Even Huawei O&M personnel cannot obtain the root key.

Transmission security: HIPAA requires the covered entities to implement technical security measures to protect against unauthorized access to electronic protected health information transmitted over an electronic communications network.

Customers should consider implementing industry recognized transmission encryption mechanism (such as TLS) at the application system layer to protect ePHI in network transmission from unauthorized access. Customers can also use HUAWEI CLOUD Data Encryption Workshop (DEW) when implementing ePHI data transmission encryption. DEW provides two encryption key management options. By default, it provides a fully managed encryption key service to manage the encryption key of the server for customers. DEW also provides another option for customers and in this way they can upload their own keys. Customers can manage its own encryption key in an all-round way.

In addition, customers can choose HUAWEI CLOUD **Direct Connect (DC)**[14] and **Virtual Private Network (VPN)**[15] to ensure the security of ePHI in transmission. DC is used to construct a high-speed, low-latency, stable and secure dedicated connection channel between a customer's local data center and HUAWEI CLOUD VPC. While making full use of HUAWEI CLOUD service advantages, it continues to use existing IT facilities to achieve a flexible and scalable hybrid cloud computing environment. Meanwhile, VPN is used to build a convenient, flexible, and ready-to-use IPsec encryption connection channel between a local data center and HUAWEI CLOUD VPC.

Customers can also use HUAWEI CLOUD Virtual Private Cloud (VPC) service to apply for an isolated, private virtual network environment in HUAWEI CLOUD. Customers can freely configure IP address segment, subnet, security group and other sub services in VPC, and can also apply for elastic bandwidth and elastic IP to build a business system, so as to realize complete isolation between different tenants in the three-tier network. Tenants can fully control their own virtual network construction and configuration, and through configuring network access control strategy (ACL) and security group rules, they can strictly control the network traffic in and out of subnets and virtual machines to meet the needs of more fine-grained network isolation.

In addition, HUAWEI CLOUD service products and components have planned and implemented the isolation mechanism from the beginning of the design, to avoid unauthorized access and tampering from customers either intentionally or unintentionally, and reduce the risk of data breach. Using data storage as an example, HUAWEI CLOUD services including block storage, object storage, and file storage all regard customer data isolation as an important feature.

[14] https://intl.huaweicloud.com/en-us/product/dc.html
[15] https://intl.huaweicloud.com/en-us/product/vpn.html

8. HUAWEI CLOUD Incident Management and Breach Notification

HUAWEI CLOUD implements strict security incident management procedures and processes, operating a 24/7 professional security incident response team and a corresponding security expert resource pool, and classifying security incidents according to their impact on customers and the entire network. HUAWEI CLOUD strives to achieve rapid security incident responses in terms of incident detection, impact scoping, damage isolation, and service recovery. In accordance with applicable laws and regulations, HUAWEI CLOUD promptly discloses personal data breaches, and implements emergency plans and recovery processes to reduce the impact on customers.

HUAWEI CLOUD records and analyzes the causes after incident processing to avoid repeat problems. Moreover, HUAWEI CLOUD reviews and updates the security incident identification and response process according to internal and external environment changes.

As a business associate of customers who are covered entities in HIPAA, HUAWEI CLOUD has established a breach notification process to ensure that customers are notified without undue delay in cases of data breach. Affected customers will be provided with all information about the breach that HUAWEI CLOUD can access, as well as steps taken by HUAWEI CLOUD to control and investigate the data breach. According to HIPAA requirements, the customer should be responsible for informing other relevant parties such as those affected by the PHI breach, regulatory authorities, or media.

9. Arrangements as a Business Associate

According to HIPAA, HUAWEI CLOUD should be regarded as a Business Associate. Customers processing ePHI need to sign the Business Associate Agreement **(**BAA)[16]. HUAWEI CLOUD provides BAA templates that meet HIPAA requirements and customers can sign the BAA according to their business needs. As a business associate, HUAWEI CLOUD establishes HIPAA-compliant strategies and processes, and revises them according to environment changes. Relevant records of these strategies are retained. Customers can confirm their internal management processes and implementation levels through independent third-party audit reports or information from the HUAWEI CLOUD official website. HUAWEI CLOUD provides contractual services and a secure environment to protect customer data from unauthorized access, tampering, or damage.

10. Conclusion

This user guide describes how HUAWEI CLOUD provides cloud services that meet the requirements of HIPAA. This aims to help customers learn more about HUAWEI CLOUD's compliance with HIPAA requirements to assure customers that they can store and process health data securely through HUAWEI CLOUD services. To some extent, this document also guides customers on how to design, build and deploy a cloud environment that can securely and reliably

[16] https://www.hhs.gov/hipaa/for-professionals/covered-entities/sample-business-associate-agreement-provisions/index.html

process sensitive health information on HUAWEI CLOUD, and helps customers better shoulder security responsibilities together with HUAWEI CLOUD.

This user guide is for reference only and does not have legal effect or constitute legal advice. Customers should assess their own use of cloud services as appropriate and ensure compliance with HIPAA when using HUAWEI CLOUD.

11. Version History

Date	Version	Description
November 2019	1.0	First release

