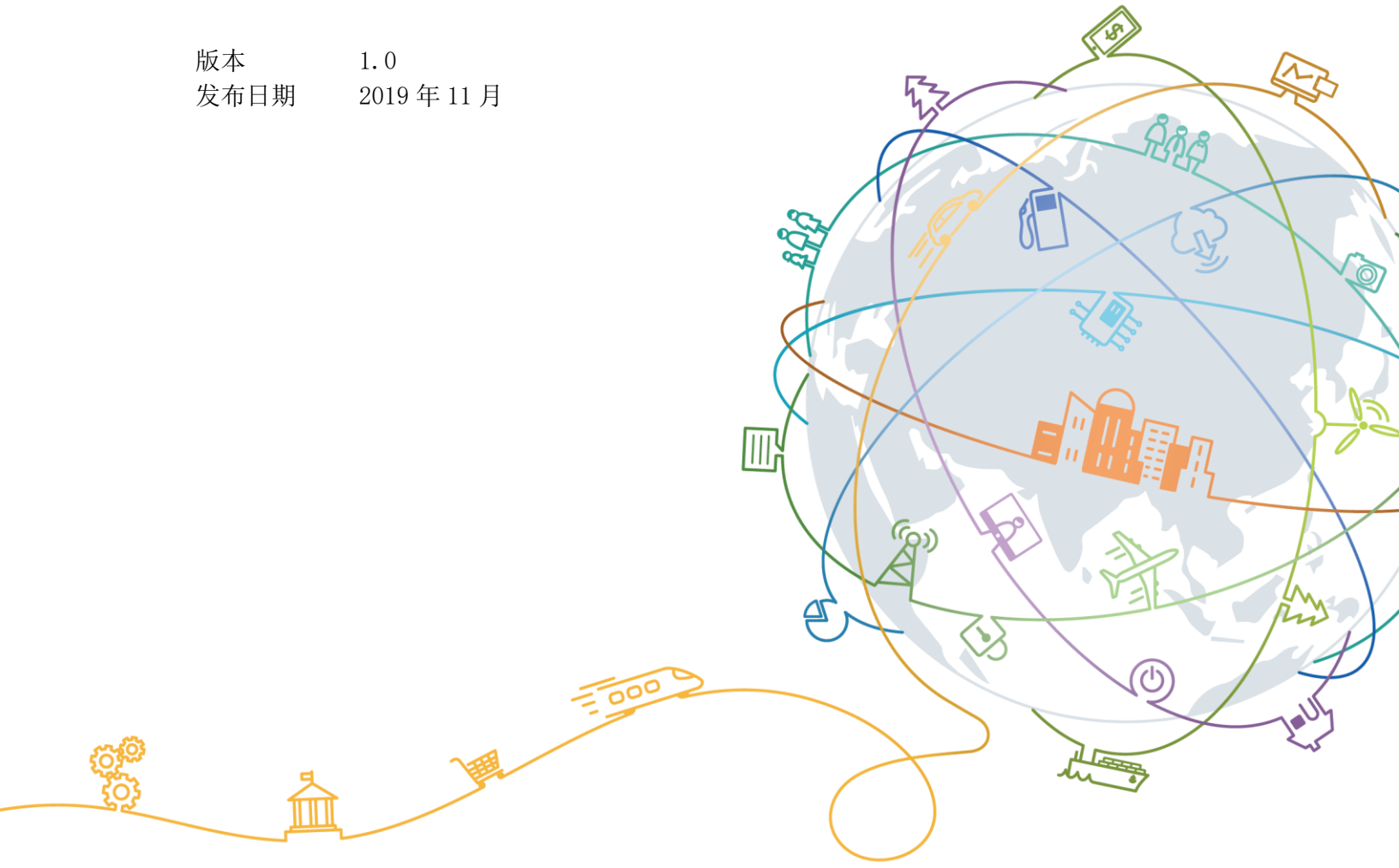
华为云 HIPAA 合规性说明

版本　　1.0
发布日期　　2019 年 11 月



华为技术有限公司

商标声明

注意

您购买的产品、服务或特性等应受华为公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为公司对本文档内容不做任何明示或暗示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

华为技术有限公司

地址：深圳市龙岗区坂田华为总部办公楼 邮编：518129

网址：华为 - http://www.huawei.com/cn/

华为云 - https://www.huaweicloud.com/

客户服务邮箱：support@huawei.com

目录

1. HIPAA 简介

美国《健康保险流通与责任法案》（HIPAA）[1]于 1996 年颁布。该法案涵盖一系列保障 PHI（受保护健康信息）的安全性和隐私性的控制要求，以加强信息共享并提高医疗保健系统的效率和质量。

HIPAA 的控制要求[2]主要包含安全规则、隐私规则以及违规通知规则三个部分，适用于所涉实体，包括医疗服务提供者、健康计划及医疗健康结算中心。此外，HIPAA 也适用于所涉实体的商业伙伴。

目前，在全球范围内，医疗行业对数字化的需求不断上升，在数字化的过程中也面临着各种挑战。云计算的高可用性、可伸缩性等特性使得医疗行业可以提高效率、降低成本。为了向医疗行业客户提供高性能、高可靠、高安全的云服务，华为云将协助医疗客户共同满足 HIPAA 的要求，让医疗客户安全、放心地使用华为云服务。

2. HIPAA 关键术语定义

- **所涉实体**

指需要遵守 HIPAA 要求的实体，包括以下三类：

1）医疗服务提供者：提供医疗服务，并且以电子形式进行符合 HHS（美国卫生与公众服务部）标准的财务或行政交易的实体。

示例：医生、诊所、药店等。

2）健康计划：任何提供医疗服务或支付医疗服务费用的个人或团体计划。

示例：医疗保险公司、雇主赞助的团体健康计划等。

3）医疗健康结算中心：任何处理或辅助处理医疗健康信息的实体。

示例：账单结算服务、社区医疗管理信息系统等。

- **商业伙伴**

商业伙伴包括以下两类：

1）代表所涉实体执行某些职能或活动且其中涉及 PHI 的使用或披露的实体（不包括所涉实体的劳动力成员）。相关的职能或活动可能包括处理或管理索赔、数据分析、质量保证、计费等。

2）为所涉实体提供某些服务且其中涉及 PHI 的使用或披露的实体（不包括所涉实体的劳动力成员）。提供的服务可能包括法律、精算、会计、咨询、数据汇总、IT 管理、认证或金融服务等。

示例：为健康计划提供涉及访问 PHI 的法律服务的律师、为医疗服务提供者提供涉及访问 PHI 的会计服务的会计师事务所。

- **PHI（受保护健康信息）**

[1] https://aspe.hhs.gov/report/health-insurance-portability-and-accountability-act-1996

[2] https://www.hhs.gov/hipaa/for-professionals/index.html

PHI 指个人可识别的健康信息，由所涉实体或商业伙伴以任何形式或媒介（包括纸质或电子形式）维护或传输。其中，个人可识别健康信息为可识别个人身份或被合理认为可识别个人身份的信息，包括：

1）与个人过去、现在或将来的身体或精神健康有关的信息；

2）与为个人提供的医疗服务有关的信息；

3）与为个人提供的医疗服务相关的过去、现在或将来的付款信息。

- **ePHI（电子受保护健康信息）**

ePHI 指以电子形式创建、接收、维护或传输的 PHI。

- **BAA（商业伙伴增订合约）**

HIPAA 要求所涉实体和商业伙伴之间以及商业伙伴和其分包商之间需签订的合约，以约束商业伙伴恰当地保护 PHI 并明确商业伙伴在何种情况下可以使用和披露 PHI。

注：分包商也被视为商业伙伴。

- **PHI 违规**

指以不允许的方式获取、访问、使用或披露 PHI 而损害 PHI 的安全性或隐私性，除非所涉实体或商业伙伴（如适用）根据以下因素进行的风险评估能够表明 PHI 已经受损的可能性很小：

1）所涉及的 PHI 的性质和范围，包括标识符的类型和重新识别的可能性；

2）未经授权使用 PHI 或接收披露的 PHI 的个人或实体；

3）PHI 是否被实际获取或查看；

4）所涉实体和商业伙伴减少 PHI 所受风险的程度。

示例：未经授权访问医院的电子病历、对相关服务器进行攻击导致 PHI 泄露等。

3. 华为云安全与隐私合规

华为云继承了华为公司完备的管理体系以及 IT 系统的建设和运营经验，对云服务各项服务的集成、运营及维护进行主动管理，并持续改进。截至目前，华为云已获得众多国际和行业安全合规资质认证[3]，全力保障客户部署业务的安全与合规，主要包括：

认证	描述
ISO 20000-1:2011	ISO 20000 是针对信息技术服务管理领域的国际标准，提供设计、建立、实施、运行、监控、评审、维护和改进服务管理体系的模型以保证服务提供商可提供有效的 IT 服务来满足客户和业务的需求。

[3] https://www.huaweicloud.com/securecenter/compliance.html

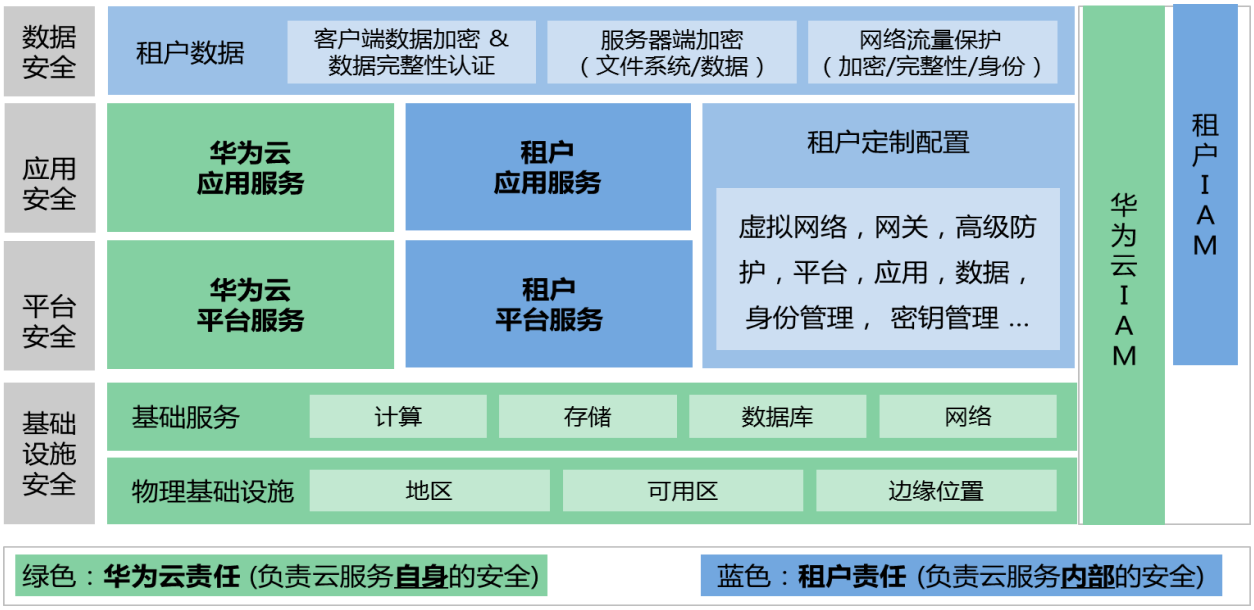
认证	描述
ISO 27001:2013	ISO 27001 是目前国际上被广泛接受和应用的信息安全管理体系认证标准。该标准以风险管理为核心，通过定期评估风险和对应的控制措施来有效保证组织信息安全管理体系的持续运行。
ISO 27017:2015	ISO 27017 是针对云计算信息安全的国际认证。ISO 27017 的通过，表明华为云在信息安全管理能力达到了国际公认的最佳实践。
ISO 22301:2012	ISO 22301 是国际公认的业务连续性管理体系标准，通过对风险的识别、分析和预警来帮助组织规避潜在事件的发生，并且制定完备的“业务连续性计划”，有效地应对中断发生后的快速恢复，保持核心功能正常运行，将损失和恢复成本降至最低。
网络安全等级保护	网络安全等级保护是中国公安部用于指导国内各组织单位进行网络安全建设的依据，目前已成为各行业广泛遵守的通用安全标准。华为云通过了网络安全等级保护三级，关键区域、节点通过了网络安全等级保护四级。
新加坡 MTCS Level 3 认证	MTCS 多层云计算安全规范是由新加坡信息技术标准委员会制定的标准。该标准要求 CSP 在云计算中采用健全的风险管理和安全实践。目前华为云新加坡大区获得 MTCS 最高安全评级的 Level 3 等级认证。
SOC 审计	SOC 审计报告是由第三方审计机构根据美国注册会计师协会（AICPA）制定的相关准则，针对外包服务商的系统和内部控制情况出具的独立审计报告。
PCI DSS 认证	支付卡行业数据安全标准（PCI DSS）是由 JCB、美国运通、Discover、万事达和 Visa 五家国际信用卡组织共同建立的一套支付卡行业数据安全标准，由支付卡行业安全标准委员会管理。它是世界上最权威、最严格的金融机构认证。
CSA STAR 金牌认证	CSA STAR 认证是由标准研发机构 BSI（英国标准协会）和 CSA（云安全联盟）合作推出的国际范围内的针对云安全水平的权威认证，旨在应对与云安全相关的特定问题，协助云计算服务商展现其服务成熟度的解决方案。
可信云金牌运维专项评估	金牌运维评估是面向已通过可信云服务认证的云服务提供商的运维能力专项评估。华为云通过“金牌运维”评估，体现了华为云服务具备完善、健全的运维管理体系，符合国内权威云服务运营和维护保障要求的认证标准。
云服务用户数据保护能力认证	云服务用户数据保护能力评估是针对云服务用户数据安全的评估机制，评测关键指标范围包括事前防范、事中保护、事后追溯三个层面。

认证	描述
工信部云计算服务能力评估	云计算服务能力评估是以《信息技术云计算云服务运营通用要求》等相关国家标准为依据的分级评估标准。华为私有云和公有云双双获得云计算服务能力“一级”符合性证书。
可信云评估	可信云评估是由数据中心联盟（DCA）组织、中国信息通信研究院（工信部电信研究院）测评的面向云计算服务和产品的权威评估。
网信办网络安全审查	网信办网络安全审查是中央网信办依据国家标准《云计算服务安全能力要求》进行的第三方安全审查。华为云服务政务云平台顺利通过该安全审查（增强级），表明华为政务云平台在安全性、可控性等方面获国家网络安全管理机构的认可。
国际通用准则 CC EAL3+	CC(Common Criteria)认证是一种信息技术产品和系统安全性的评估标准，它提供了一组通用的安全功能要求和安全保证要求，并在这些保证要求的基础上提供衡量 IT 安全性的尺度（即评估保证级 EAL），使得独立的安全评估结果可以互相比较。
ISO 27018:2014	ISO 27018 是专注于云中个人数据保护的国际行为准则。ISO 27018 的通过，表明华为云已满足国际认可的公有云个人数据保护措施的要求，可保证客户个人数据安全。
ISO 29151:2017	ISO 29151 是国际个人身份信息保护实践指南。ISO 29151 的通过，表明华为云实施国际认可的个人数据处理的全生命周期的管理措施。
ISO 27701:2019	ISO 27701 规定了建立、实施、维护和持续改进隐私相关所特定的管理体系的要求。华为云通过 ISO27701 表明了其在个人数据保护具有健全的体制。
BS 10012:2017	BS 10012 是 BSI 发布的个人信息数据管理体系标准，BS10012 认证的通过表明华为云在个人数据保护上拥有完整的体系，以保证个人数据安全。

4. 华为云安全责任共担模型

华为云的主要责任是研发并运维运营华为云数据中心的物理基础设施，华为云提供的各项基础服务、平台服务和应用服务，也包括各项服务内置的安全功能。同时，华为云还负责构建物理层、基础设施层、平台层、应用层、数据层和用户身份管理（IAM）层的多维立体安全防护体系，并保障其运维运营安全。

租户的主要责任是在租用的华为云基础设施与服务之上定制配置并且运维运营其所需的虚拟网络、平台、应用、数据、管理、安全等各项服务，包括对华为云服务的定制配置和对租户自行部署的平台、应用、用户身份管理等服务的运维运营。同时，租户还负责其在虚拟网络层、平台层、应用层、数据层和 IAM 层的各项安全防护措施的定制配置、运维运营安全、以及用户身份的有效管理。



关于华为云与租户的安全责任详情，可参见华为云已发布的《华为云安全白皮书》[4]。

5. 华为云全球基础设施

华为云目前已陆续在全球多个国家或地区开服。华为云的基础设施采用在全球部署多个地理区域（Region）和多可用区（AZ）的模式，华为云能够在多个地理区域内或同一地域内多个可用区之间灵活替换计算实例和存储数据，每个可用区都是一个独立故障维护域，也就是各可用区物理上是隔离的。用户可充分利用这些地理区域和可用区，规划应用系统在云上的部署和运行。基于多个可用区进行应用的分布式部署，可保证在大多故障情况下系统都能连续运行。关于更多华为云基础设施的信息，可参见华为云官网“全球基础设施”[5] 。

6. 华为云隐私保护控制

隐私保护一直是华为云生存的基础。华为云拥有专业的隐私保护团队，负责制定和执行相关的管控措施和流程。华为云将其丰富的隐私保护实践和经验融入到云服务的研发生命周期，确保每个云服务满足隐私保护合规要求，为客户提供隐私保护功能以满足客户的合规需求。华为云的隐私保护工作已取得明显的成果，并获得国内外权威机构的认可。关于华为云的隐私保护详情和获得的认证情况，可参见《华为云隐私保护白皮书》[6]，也可访问信任中心获取更多信息。

6.1 数据访问

华为云深刻理解客户的内容数据对客户的重要性，华为云一直恪守“不碰数据”原则，保障数据为客户所有、为客户所用、为客户创造价值。华为云的客户拥有对其内容数据的全面控制权，可了解内容数据存放的位置并设置合适的保护措施。

[4] https://res-static1.huaweicloud.com/content/dam/cloudbu-site/archive/china/zh-cn/securecenter/security_doc/SecurityWhitepaper_cn.pdf
[5] https://www.huaweicloud.com/global/
[6] https://res-static1.huaweicloud.com/content/dam/cloudbu-site/archive/china/zh-cn/securecenter/security_doc/PrivacyWhitepaper_cn.pdf

华为云根据客户的要求和授权进行相应的操作。当客户不再使用华为云服务时，华为云通过严格的数据删除机制，在约定的时间周期后执行数据删除。关于华为云数据访问的详细信息，可参见《华为云数据安全白皮书》[7]。

6.2 保障个人隐私权利的承诺

由于客户对其内容数据拥有全面控制权，客户应保障数据主体个人隐私的权利。华为云提供的统一身份认证和日志服务等，可帮助客户更好的满足保障数据主体权利的需求。本白皮书安全控制部分将详细介绍**统一身份认证服务（Identity and Access Management，简称 IAM）**[8]和**云日志服务（Log Tank Service，简称 LTS）**[9]，也可参考华为云官网关于统一身份认证以及云日志服务的内容。

7. 华为云安全控制

安全规则规定了确保电子受保护健康信息（ePHI）的机密性、完整性和可用性的控制要求。美国卫生与公众服务部（HHS）[10]表示，安全规则的主要目标是在允许所涉实体采用技术提高患者护理的质量和效率的同时保护个人健康信息的隐私。

安全规则适用于所涉实体及其商业伙伴创建、接收、维护或传输的电子形式的 ePHI，要求所涉实体和商业伙伴实施合理和恰当的管理、物理和技术方面的保障措施，从而：

- 确保创建、接收、维护或传输的所有 ePHI 的机密性、完整性和可用性；
- 识别并防范对信息的安全或完整性可能的威胁；
- 防范可能发生的不允许的使用或披露；
- 确保员工遵守规定。

下文将介绍 HIPAA 要求所涉实体及其商业伙伴为保护 ePHI 实施的管理、物理和技术方面的保障措施以及华为云对 HIPAA 要求的应答。

7.1 管理保障措施

安全管理流程：HIPAA 要求所涉实体或商业伙伴必须指定一名安全官，并制定和执行安全策略和程序，采取适当的安全措施降低风险，以保证 ePHI 的机密性、完整性和可用性。定期审查信息系统活动记录，对不遵守所涉实体或商业伙伴的安全策略和程序的员工给予适当的处罚。

客户可通过华为云的**云审计服务（Cloud Trace Service，简称 CTS）**[11]，对使用云服务资源的操作进行记录。通过 CTS，客户可实时、系统地记录所有人员对华为云上的资源和系统配置变更行为，以及记录用户在管理界面上的所有操作和用户在华为云上的所有 API 操作。借助 CTS 中记录的对象级 API 事件，用户可以通过收集 OBS 对象上的活动数据来检测数据泄露情况。CTS 作为华为云的管理服务之一，其安全设计是在华为云安全架构基础上构建的，主要涉及安全组网、网络边界安全防护、应用安全防护以及数据安全防护四个层面，确保向租户提供安全的云审计服务。

[7] https://res-static1.huaweicloud.com/content/dam/cloudbu-site/archive/china/zh-cn/securecenter/security_doc/DataSecurityWhitepaper_cn.pdf
[8] https://www.huaweicloud.com/product/iam.html
[9] https://www.huaweicloud.com/product/lts.html
[10] https://www.hhs.gov/
[11] https://www.huaweicloud.com/product/cts.html

华为把网络安全作为公司重要战略之一，通过自上而下的治理结构来实现。秉承华为网络安全战略和规范，华为云安全团队对本领域安全工作进行自主规划和管理。全面实现云服务业务和云安全业务的研发运维运营组织合一，组织结构趋于扁平化，以便适应云服务必需的 DevOps/DevSecOps 流程。华为云制定了完善的信息安全风险管理机制，定期开展内部和第三方的渗透测试和安全评估，以保证承载 ePHI 数据的云环境的安全性。

信息访问管理：HIPAA 要求所涉实体或商业伙伴必须制定访问 ePHI 信息的策略和程序，保证基于用户或接收方的角色进行适当的访问（即基于角色的访问）。

客户可通过华为云的统一身份认证服务（IAM）对使用云资源的用户账号进行管理。IAM 除了支持密码认证外还支持多因子认证，客户可自主选择是否启用。如果租户有安全可靠的外部身份认证服务商，可将 IAM 服务的联邦认证外部用户映射成华为云的临时用户，并访问租户的华为云资源。IAM 可以按层次和细粒度授权，管理员可以基于用户的工作职责规划使用云资源的权限，还可以通过设置用户访问云服务系统的安全策略，例如设置访问控制列表（ACL）来限制非信任网络的恶意接入。

华为云原则上不会触碰 ePHI 数据。如果需要协助客户维护系统，华为云仅在获取客户授权后访问。

安全意识培训：HIPAA 要求所涉实体必须针对全员（包括管理层）开展安全意识培训计划，对违反其政策和程序的工作人员实施适当的处罚。

客户应考虑制定安全培训计划，在组织内开展全员培训，并对员工的安全违规行为进行适当的处置。华为云已将此要求应用到华为云内部安全管理。

为了提升全员的网络安全意识、规避网络安全违规风险、保证业务的正常运营，华为云从意识教育普及、宣传活动开展、华为员工商业行为准则（BCG）及承诺书签署三个方面开展安全意识教育，且每年至少执行一次针对全员的安全意识培训。

评估：HIPAA 要求所涉实体必须定期评估其安全策略和程序满足安全规则要求的程度。

客户应考虑建立安全风险评估或审计机制，定期对其安全策略和程序进行符合性评估。华为云已将此要求应用到华为云内部安全管理。

华为云参考 ISO 27001 构建了完善的信息安全管理体系，制定了华为云整体信息安全策略和程序。华为云遵从 HIPAA 的安全规则定期对该体系进行评估并持续优化，以保证华为云的安全策略和程序满足企业安全战略以及安全合规的要求。

应急计划：HIPAA 要求所涉实体必须建立（并根据需要实施）应急计划，以保证能够及时响应包含 ePHI 的系统的紧急情况或其他事件。

客户可通过华为云的数据备份归档服务，对 ePHI 数据进行备份，保证在灾难发生时数据不丢失。客户可以使用对象存储服务的版本控制、云硬盘备份、云服务器备份等功能，将云上的文档、硬盘、服务器进行备份，也可以通过华为云备份归档解决方案，充分利用云服务模式下按需使用、弹性扩展、可靠性高的特点，结合备份归档软件和华为云基础设施，将客户云下数据备份归档到华为云。通过与数据加密服务集成，备份数据也可以方便、快速地实现加密存储，有效保证备份数据的安全性。为了提高数据灾难发生时的应急响应能力，客户可以定期依据计划进行恢复演练。

华为云备份归档解决方案支持客户使用备份数据，在云上即时部署的系统中恢复数据，完成后即可释放资源，极大节省了恢复演练成本。

华为云建立了完善的业务连续性管理体系，并获得 ISO 22301 认证。华为云支持在一个数据中心的多个节点内复制并存放用户数据。当单个节点出现故障时，保证用户数据不丢失，且系统实现自动检测和自愈。华为云依赖全球多区域部署的架构实现数据中心容灾和备份。华为云除了提供高可用的基础设施、冗余数据备份、可用区灾备，还制定了业务连续性计划和灾难恢复计划，并定期对其进行测试。客户可充分利用这些区域和可用区，规划应用系统在云上的部署和运行。基于多个可用区进行应用的分布式部署，可保证在大多数故障情况下（包括自然灾害和系统故障），系统都能连续运行。

7.2 物理安全措施

设施访问控制：HIPAA 要求所涉实体必须实施策略和程序，限制对电子信息系统所在设施的物理访问，以保护设施和其中的设备免受未经授权的物理访问、篡改和盗窃，同时确保允许适当授权的访问。

客户应考虑对可访问 ePHI 的信息系统所在的物理环境进行严格的访问控制，以防止物理环境中的设施遭到非授权访问、篡改和盗窃。华为云已将此要求应用到华为云内部安全管理。

华为云已制定并实施完善的物理和环境安全防护策略、规程和措施，满足 GB 50174《电子信息机房设计规范》A 类和 TIA942《数据中心机房通信基础设施标准》中的 T3+标准。华为云运维运营团队严格执行访问控制、安保措施、例行监控审计、应急响应等措施，以确保华为云数据中心的物理和环境安全。更多详细信息，请参见《华为云安全白皮书》。

工作站安全：HIPAA 要求所涉实体必须对可以访问 ePHI 的所有工作站实施物理安全措施，仅允许授权用户的访问。

客户应考虑对可访问 ePHI 的所有工作站实施物理安全控制，以防止工作站遭到非授权访问。华为云已将此要求应用到华为云内部安全管理。

华为云根据业务功能和网络安全风险将数据中心划分为多个安全区域，通过实现物理和逻辑控制并用的隔离手段，提升网络面对入侵和内鬼的分区自我保护和容错恢复能力。其中运维管理区（Operations Management，简称 OM）主要部署操作运维部件，华为云运维人员必须先通过虚拟专用网络（Virtual Private Network，简称 VPN）接入该区域，再通过跳板机访问被管理节点。管理员可从此区域访问所有区域的运维接口。此区域不向其他区域开放接口。接入云环境的办公终端严格遵守办公设备安全管理规定的要求。对于需要访问云环境的行为都需要通过堡垒机，以便对操作行为进行记录。

设备和媒介控制：HIPAA 要求所涉实体必须实施策略和程序，以管理对含有 ePHI 数据的设备和电子媒体的正确使用和访问。所涉实体也应有相应措施来管理该类设备和电子媒介的接收、转让、清除和重用。

客户应考虑规范可能含有 ePHI 数据的设备和电子媒介的正确使用和访问。华为云已将此要求应用到华为云内部安全管理。

华为云对存有 ePHI 数据的存储介质、服务器整机和存储整机制定了进出机房管理规定，以加强信息资产保护，防止物理资产流失。该规定要求存储介质、服务器整机和存储整机进出机房应

经过需求部门主管审批并留存记录；运维过程中需使用的 U 盘进出机房，应经过数据中心经理的审批并留存记录；如果服务器硬盘及服务器整机、存储整机下架，应在下架前对存储数据进行清除。除此之外，还对该类设备和媒介在机房间迁移、返还供应商、设备出机房、清退报废等场景下的安全要求进行了定义。当客户主动进行数据删除操作或因服务期满需要对数据进行删除时，华为云会严格遵循数据销毁标准和与客户之间的协议约定，对存储的客户数据进行清除。为了避免重要数据销毁后不可恢复，或因误操作丢失，建议客户在销毁数据之前慎重考虑，对拟销毁的数据做好备份（华为云提供数据备份服务，详情参见本文 7.1 节管理保障措施的应急计划部分对备份服务的介绍）。

7.3 技术保障措施

访问控制：HIPAA 要求所涉实体必须实施技术策略和程序，以确保只允许授权人员访问 ePHI。

客户应考虑在应用系统中对 ePHI 施行严格的访问控制。客户可在华为云控制台通过华为云统一身份认证服务（IAM）为可访问华为云资源的人员创建账号和赋予权限。每一位华为云客户在华为云都拥有唯一可辨识的用户 ID，并可配置多种用户身份验证机制，包括账号密码、多因素认证等。IAM 支持客户的安全管理员根据需求来设置不同强度的密码策略和更改周期，防止用户使用简单密码或长期使用固定密码而导致账号泄露。此外，IAM 还支持客户的安全管理员设置用户安全组，通过用户组对组织内部不同角色的员工进行资源访问权限管理。

未经客户授权，华为云员工不具备访问客户数据的权限。但为了进一步配合客户满足 HIPAA 的要求，华为云运维人员会遵照“权限最小化”的原则配置管理权限。在接入华为云管理网络对系统进行集中管理时，华为云运维人员须使用唯一可辨识的员工身份账号，用户账号均配置了强密码安全策略，且密码须定期更改，以防止暴力破解密码。此外，还采用双因子认证对运维人员进行身份认证，如 USB key、Smart Card 等。

审计控制：HIPAA 要求所涉实体必须实现硬件、软件和/或程序机制，记录和检查包含或使用 ePHI 的信息系统中的活动。

客户应考虑在应用系统中实现对访问或操作 ePHI 活动记录的功能。客户可通过华为云云日志服务（LTS）对所有访问或使用华为云资源的活动日志进行实时查询和转储，客户无需开发即可利用日志服务做实时决策分析。另外，LTS 可与**虚拟私有云（Virtual Private Cloud，简称 VPC）**[12]和云审计服务（CTS）配套使用，客户可以通过云审计服务管理云服务资源的操作记录，包含访问或操作 ePHI 用户活动的查询、审计和回溯功能。

完整性控制：HIPAA 要求所涉实体必须执行一个策略和程序，防止 ePHI 被篡改或破坏，并实施电子机制，以确认 ePHI 未被非授权的更改或销毁。

客户应考虑在应用系统中实施强访问控制和加密机制，以确保应用系统中的 ePHI 免受非授权的篡改或破坏，并考虑采用行业认可的加密算法对 ePHI 数据进行保护。

目前客户可通过华为云 IAM 对云资源的访问控制进行管理，另外华为云还提供了**数据加密服务（Data Encryption Workshop，简称 DEW）**[13]，将复杂的数据加解密、密钥管理逻辑进行封装。客户可自行选择使用数据加密（服务端加密）功能对云硬盘 EVS、对象存储 OBS、镜像服务 IMS 和云数据库（MySQL、PostgreSQL、SQL Server）等多个服务进行加密配置，华为云数据加密功能采

[12] https://www.huaweicloud.com/product/vpc.html
[13] https://www.huaweicloud.com/product/dew.html

用了高强度的算法（支持 RSA，DSA，ECDSA 等常见的非对称和对称算法）对存储的数据进行加密，加密的密钥可由 DEW 进行全生命周期集中管理。在未授权的情况下，除客户外的任何人均无法获取密钥对数据进行解密，确保了客户云上 ePHI 数据的安全。

DEW 采用分层密钥管理机制，方便各层密钥的轮换。通过 DEW 的控制台或 API 进行关联设置，各存储服务加密数据时使用的加密密钥，能够由保存在 DEW 中的客户主密钥进行加密，该客户主密钥又由保存在 HSM 中的根密钥进行加密，构成了一条完整的安全、可信的密钥链。HSM 经过严格的国际安全认证，能够做到防入侵、防篡改，即使是华为运维人员也无法窃取根密钥。

传输安全性：HIPAA 要求所涉实体必须实现技术安全措施，以确保网络传输中的 ePHI 免受非授权访问。

客户应考虑在应用系统层实施行业认可的传输加密机制（如：安全传输层协议 TLS），以保护在网络传输中的 ePHI 遭到非授权的访问。客户在实施 ePHI 数据传输加密时，同样可以使用华为云数据加密服务（DEW），DEW 提供了两个加密密钥管理选项，默认情况下提供一个完全托管的加密密钥服务，为客户管理服务端加密密钥。DEW 还为客户提供另外一种选择，客户可以上传自己的密钥，通过这种方式客户可全面管理自己的加密密钥。

另外，客户也可选择华为云**云专线（Direct Connect，简称 DC）**[14]、**虚拟专用网络（Virtual Private Network，简称 VPN）**[15]等服务来保证传输中的 ePHI 的安全。DC 用于搭建客户本地数据中心与华为云 VPC 之间高速、低时延、稳定安全的专属连接通道，使用现有 IT 设施的同时，充分利用华为云服务优势，实现灵活一体、可伸缩的混合云计算环境。VPN 用于搭建客户本地数据中心与华为云 VPC 之间便捷、灵活、即开即用的 IPsec 加密连接通道。

客户还可以使用华为云虚拟私有云（VPC）服务在华为云上申请隔离的、私密的虚拟网络环境。客户可以自由配置 VPC 内的 IP 地址段、子网、安全组等子服务，也可以申请弹性带宽和弹性 IP 搭建业务系统，实现不同租户间在三层网络的完全隔离。租户可以完全掌控自己的虚拟网络构建与配置，并通过配置网络访问控制策略（ACL）和安全组规则，对进出子网和虚拟机的网络流量进行严格的管控，满足租户更细粒度的网络隔离需要。

另外，华为云各服务产品和组件从设计之初就规划并实现了隔离机制，避免客户间有意或无意的非授权访问、篡改等行为，降低数据泄露风险。以数据存储为例，华为云的块存储、对象存储、文件存储等服务均将客户数据隔离作为重要特性。

8. 华为云事件管理与违规通知

华为云执行严格的安全事件管理程序和流程，设置 7*24 小时专业安全事件响应团队及专家资源池，根据安全事件对全网及客户的影响进行定级，秉持快速发现、快速定界、快速隔离与快速恢复的原则处理事件。针对个人数据泄露事件，遵从适用法律法规要求，华为云及时披露事件，同时执行应急预案及恢复流程，以降低对客户的影响。

华为云在事件处理完成后记录和分析原因以避免重复问题的发生，并根据内外部环境的变化审查和更新安全事件的识别和响应流程。

[14] https://www.huaweicloud.com/product/dc.html
[15] https://www.huaweicloud.com/product/vpn.html

作为 HIPAA 所涉实体的客户的商业伙伴，华为云建立了数据泄露通知流程，以确保在发生数据泄露时及时通知客户。华为云将向受影响的客户提供华为云可以获取的所有数据泄露相关信息以及华为云控制和调查数据泄露的步骤。客户应根据 HIPAA 的要求自行负责将泄露情况通知其他相关方，如泄露的 PHI 所对应的个人、监管机构或媒体等。

9. 作为商业合作伙伴的安排

根据 HIPAA 的规定，华为云应被视为商业伙伴（Business Associate）。处理 ePHI 的客户需要与商业伙伴签订商业伙伴增订合约（Business Associate Agreement，简称 BAA）[16]。华为云提供符合 HIPAA 要求的 BAA 模板，客户可根据自身业务需求签订 BAA。作为商业伙伴，华为云建立符合 HIPAA 的策略和流程，并根据环境变化进行更新。华为云保留这些策略的相关记录，客户可以通过第三方独立审计报告或者华为云官网信息了解其内部管理流程和执行程度。华为云提供满足合同义务的服务和安全环境，以保证客户数据不受未经授权的访问、篡改或破坏。

10. 结语

本文描述了华为云如何为客户提供符合 HIPAA 要求的云服务，有助于客户详细了解华为云在 HIPAA 要求方面的合规性，让客户安全、放心地通过华为云服务存储和处理健康信息。本文也在一定程度上指导客户如何在华为云上设计、构建和部署可以安全、可靠地处理敏感健康信息的云环境，帮助客户更好地与华为云共同承担相应的安全责任。

本白皮书仅供参考，不具备法律效应或构成法律建议。客户应酌情评估自身使用云服务的情况，并确保在使用华为云时对 HIPAA 的遵从性。

11. 版本历史

日期	版本	描述
2019 年 11 月	1.0	首次发布

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