腾讯云
GxP 合规白皮书

2022 年[5]月

版本 1.0

版权所有，©腾讯云计算（北京）有限责任公司，保留一切权利。

商标声明：

是腾讯云计算（北京）有限责任公司的注册商标。

在本手册中以及本手册所描述的产品中，出现的其它商标、产品名称，商品名称以及公司名称，由各自的所有人所拥有。

免责声明

本文档可能含有预测信息，包括但不限于有关未来的财务、运营、产品系列、新技术等。由于实践中存在诸多不确定因素，可能导致实际结果与预测信息存在较大差别。因此，本手册信息仅供参考，不构成要约或承诺。腾讯可能对本文档内容进行修订或更新，恕不另行通知。

目录

引言

随着医疗健康行业的蓬勃发展，制药、医疗器械、医疗软件、生物技术、医学研究等医疗健康领域的机构面临着日益复杂的业务流程和大量医疗记录的管理，这些都不断增加机构数据处理和数据存储的负担。为解决这一问题，医疗健康行业的数字化转型成为了当前趋势。作为一项创新的信息通信技术，云计算能够快速部署、弹性扩展，提高机构的竞争优势和灵活性，并能大幅降低机构针对软件和硬件基础设施的总拥有成本和维护成本，这无疑为医疗健康机构提供了一个可行的解决方案。

然而，医疗健康机构在采用云架构或云服务时却面临了多方面的挑战：一来是医疗健康机构无法全权保障云上系统运行的稳定性和安全性；二来是医疗健康通常管理着大量的患者敏感信息，机构需要确保上云后患者数据的完整性和隐私安全；三是医疗健康行业作为受监管程度最高的行业之一，需要严格遵守如 HIPAA、GxP 等法规和标准，合规性也是医疗健康机构决策过程中的重要考虑。因此，医疗健康机构将系统和数据迁移到云端前，需要对云服务提供商的服务水平、管理流程和安全合规性进行充分的了解。

经过多年来在云计算技术的深耕以及对医疗健康行业的深化了解，腾讯云为医疗健康领域的客户提供了各类安全、可靠、弹性可扩展的云服务以及集 IaaS、PaaS 和 SaaS 为一体的综合云服务解决方案，助力医疗健康领域的客户构建安全的云环境和健康的云生态，以推动医疗健康产业的数字化转型升级。

腾讯云深知“信任”是让医疗健康行业客户放心、安心地将系统和数据托管上云的前提，本白皮书基于主要的 GxP 标准向客户全面、透明地展示腾讯云如何通过环环相扣的安全保障体系协助客户实现云上系统和数据的合规。腾讯云希望能通过本白皮书，支持医疗健康行业客户有效满足 GxP 合规标准，同时高效实现数字化升级和业务的创新发展。

1. 腾讯云介绍

腾讯云，是腾讯倾力打造的云计算品牌，面向全球的企业、组织、机构和个人开发者，提供全球领先的云计算、人工智能、大数据等产品与服务。经过二十余年的技术锤炼，腾讯在 QQ、微信等 To C 产品的高速发展过程中积累的海量服务经验为腾讯云构筑了坚实的云计算基础。作为腾讯产业互联网的技术基座与连接器，腾讯云以卓越的技术能力打造丰富的行业解决方案，构建开放共赢的云端生态，助力各行各业实现数字化转型。

在医疗健康领域，腾讯致力于通过开放连接、人工智能、大数据、云计算、安全五大优势能力，提供医疗基础设施建设、智慧医疗服务、医学 AI 等产品，扮演好医疗健康领域数字化助手，支持客户实现先进科学技术与医学的跨界融合。腾讯云基于在云计算领域的先进技术、优秀服务经验以及在医疗健康行业多年的实践沉淀，为医疗健康领域的客户提供覆盖多业务场景的解决方案，并整合腾讯云的产品服务，打造开放平台，联合合作伙伴，构建覆盖医疗、康养、医药、器械、流通、保险、服务等全链条的医疗大健康生态，推动医疗健康产业智慧化升级。

1.1 腾讯云的基础设施和产品

截至目前为止，腾讯云构筑了从基础设施到行业应用领域，包括计算、存储、数据库、安全、大数据、人工智能、物联网、企业应用、行业应用、开发者应用等 13 大类超过 300 款产品，为医疗健康行业的客户提供全方位的云端解决方案。

腾讯云产品体系全景图

腾讯云凭借在基础设施方面独特的云端能力，跻身于全球云计算服务商。腾讯云部署在全球各地的服务器数量超过 100 万台，加速节点超过 2800 个，数据存储规模达到 EB 级别，带宽储备超过 200T。此外，腾讯云在包括中国大陆、亚太地区、北美地区、欧洲地区的全球 26 个地理区域内均设有数据中心，运营着 70 个可用区，为客户提供强有力的技术支持。

腾讯云数据中心分布图

1.2 腾讯云的安全资质认证

1）腾讯云已获得多项国内外安全认证

合规性是腾讯云发展的基础，腾讯云遵从不同国家和行业的合规性要求，全力打造值得客户信赖的云服务；同时，腾讯云还积极参与行业安全标准的制定及推广，坚持合规即服务，建设和运营安全可靠的云生态环境。

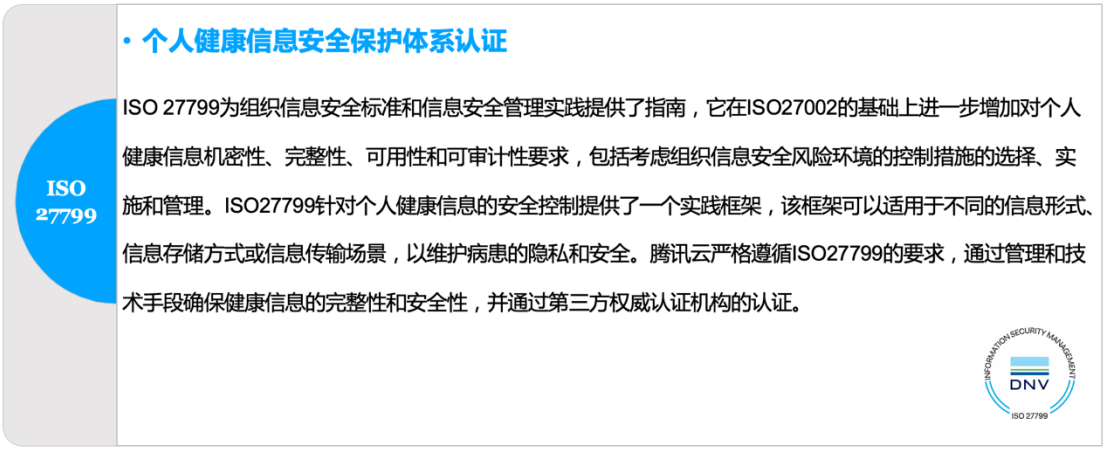
腾讯云已经按照国际认可的信息安全与 IT 管控标准规划建立起信息安全管理体系、隐私信息管理体系、质量管理体系、IT 服务管理体系、业务连续性管理体系和供应链安全管理体系等六大体系，并每年通过第三方授权测评机构的测评，为客户提供经第三方权威认证机构审核认可的云服务。腾讯云不仅严格遵守国内监管要求的各项标准，更按照各区域及行业的法规、标准和良好实践要求，不断完善相关管理体系，提升腾讯云的安全管控水平，更好的地客户展示腾讯云的合规实践。

截至目前，腾讯云已通过第三方独立审计或评估的方式，获取多项安全合规认证或资质，证明腾讯云的安全管理建设满足相关认证标准或行业良好实践，如需了解更多腾讯云合规信息，请参见**腾讯云合规性页面**。

腾讯云获取的部分安全合规资质展示

2）腾讯云医疗健康行业合规性认证

除上述安全合规资质和认证，腾讯云还获得了 ISO27799 个人健康信息安全保护认证并发布了 HIPAA（健康保险流通和责任法案）的自评估报告。作为云服务提供商，腾讯云以保护客户健康信息安全为己任，严格遵循医疗健康行业的监管要求和良好行业实践标准：



2. GxP 标准介绍

医疗健康行业关乎患者的人身健康和安全，因此医疗健康机构系统和数据的安全合规性至关重要。在医疗健康领域，GxP 一词包含广泛的合规相关的活动，它通常指一系列用于规范药物、医疗器械和医疗软件应用程序等医疗产品的研发、生产和销售的法规、准则或业界良好实践，其中“x”表示一个特定的领域，如：

- **GMP（Good Manufacturing Practices，良好药物生产规范）：**GMP 用于授权和控制药品、医疗器械、活性药物成分（API）等产品的生产，旨在指导医疗健康机构采取相关的措施来确保产品的质量和安全性。
- **GAMP （Good Automated Manufacturing Practices，良好药物自动化生产规范）：**GAMP 可以视为 GMP 的自动化版本，它指导医疗健康机构采用基于风险的方法来创建可扩展、可验证的计算机化系统，同时实现或保持合规性。
- **GLP（Good Laboratory Practice，良好实验室规范）：**GLP 旨在通过对医疗健康机构在风险管理、管理职责、质量管理和数据完整性的要求，确保医疗产品的可重复性、一致性、可靠性和完整性。
- **GCP（Good Clinical Practice，良好临床规范）：**GCP 重点关注临床试验的道德方面，规定医疗健康机构在涉及人体受试者的临床试验中，需要遵循特定的协议，以确保受试者的福祉、权利和安全不会受到侵犯。

GxP 标准的制定一方面是为了确保医疗产品在制造、存储和分销等每个阶段保持遵守质量流程；另一方面则是为了保护用于产品安全决策的数据的完整性。作为一个全球性的标准，各国家或地区都有各自的 GxP 监管机构和指导方针，本 GxP 合规白皮书将结合下列比较有代表性的 GxP 标准，对腾讯云如何协助医疗健康行业客户满足 GxP 要求作进一步说明：

地域	标准名称	标准内容概述
中国	中国国家药品监督管理局《药品生产质量管理规范》附录 1《计算机化系统》	该标准旨在确保在药品生产质量管理过程中应用的计算机化系统不会对产品的质量、过程控制和其质量保证水平造成负面影响，不增加总体风险。
	中国国家药品监督管理局《药品记录与数据管理要求（试行）》	该标准旨在加强药品研制、生产、经营、使用活动的记录和数据管理，确保有关信息真实、准确、完整和可追溯。
美国	美国食品和药物管理局 联邦法规法典第 21 篇 第 11 部分《电子记录；电子签名-范围和应用》	这部分标准包含利用计算机系统创建、修改、维护、归档、检索或分发电子记录和电子签名的相关规定，以便确保 GxP 电子数据可信且可靠，支持 GxP 合规要求。
	美国食品和药物管理局 联邦法规法典第 21 篇 第 211 部分《现行药物良好生产实践》	本部分的法规包含制备用于人类或动物的药品现行良好生产规范的最低标准，包括组织和人员、建筑物和基础设施、设备、组件和药品容器和密封性的控制、生产和流程控制、包装和标签控制、持有和分配、实验室控制、记录和报告以及退回和回收的药品等方面的要求。
	美国食品和药物管理局 联邦法规法典第 21 篇 第 820 部分《质量体系要求》	本部分适用于成品医疗器械制造商，它规定了所有供人类使用的成品设备的设计、制造、包装、标签、存储、安装和维修所使用的方法、设施和控制措施，以确保成品设备安全有效，并在其他方面符合要求。
欧盟	欧盟药品管理局《欧盟药品生产规范》 第 4 卷 附件 11《计算机系统》	本部分标准适用于良好生产规范 GMP 监管活动所涉及的所有形式的计算机化系统，旨在通过相关要求确保在计算机化系统取代人工操作的情况下，产品质量或过程控制不应因此而有所降低。

3. 腾讯云 GxP 合规白皮书概述

3.1 白皮书目标

基于多年来对医疗健康行业的深入了解，腾讯云深知医疗健康机构遵从 GxP 标准的必要性及重要性。如果在 IT 环境中引入云产品或服务，如何保证 GxP 系统的合规性和安全稳定性也成为了医疗健康机构在上云旅程中的首要关注点。因此，为向医疗健康行业客户说明腾讯云的合规体系与安全机制，腾讯云希望借此 GxP 合规白皮书，向医疗健康领域的客户说明：

- 腾讯云和客户在 GxP 合规前提下的安全责任；
- 腾讯云的质量管理体系如何支持客户的系统达到与 GxP 一致的验证状态；
- 腾讯云的管理流程和技术措施如何协助客户满足 GxP 计算机化系统的要求；
- 针对客户托管在腾讯云上的业务数据，腾讯云如何赋能客户保障数据的机密性、完整性和可用性；
- 腾讯云的产品和服务如何支持客户提高 GxP 合规能力。

3.2 白皮书受众和范围

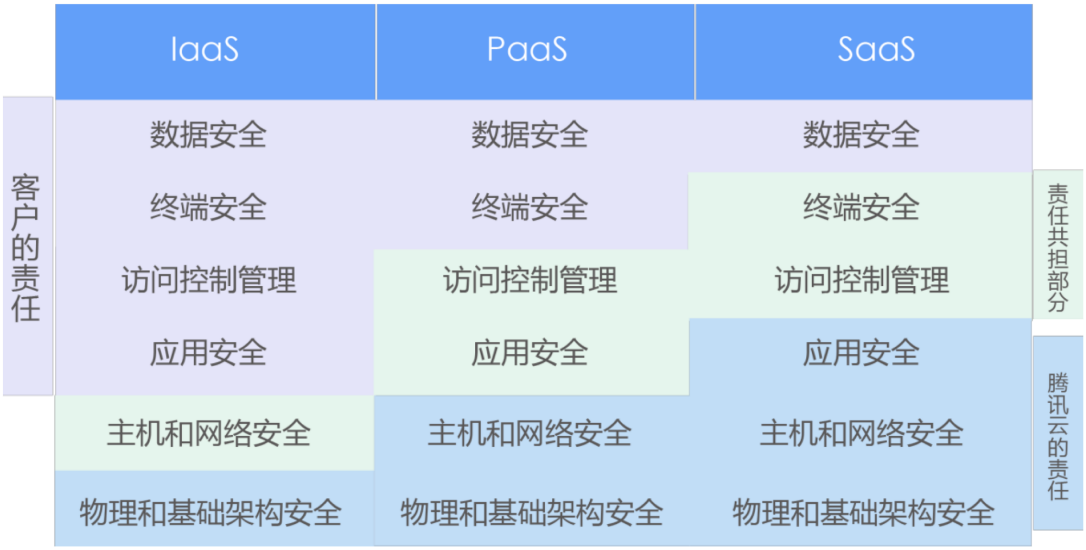
本白皮书主要面向受 GxP 监管的医疗健康机构，包括但不限于生物制药、生命科技、医疗器械、医疗服务、医学研究、医疗保险和保健品等领域的企业或组织。一般来说，这些机构中涉及 GxP 活动的系统包括自动化生产设备系统、自动化实验室设备系统、生产执行系统、实验室信息管理系统、仓储与配送系统等，覆盖人机料法环管理、生产执行及管理、质量管理的相关系统。医疗健康行业的客户如有计划将其 GxP 系统迁移上云，可以通过本白皮书

获取腾讯云的质量管理体系和安全控制的相关信息，以进一步了解腾讯云如何协助客户满足 GxP 合规。

在本白皮书中，腾讯云将从云服务提供商的角度出发，描述腾讯云如何通过相关的管理流程、技术手段和产品服务，协助客户满足相关 GxP 标准的要求；而基于腾讯云服务所建立的 GxP 系统如何满足材料纯度、设备工艺或环境要求等 GxP 业务合规标准则由客户负责在业务流程中遵守相关的规定，不在本白皮书的描述范围中。

3.3 责任共担模型

腾讯云利用统一的底层架构和资源共享形式，为客户提供其所需的网络、存储和计算等各种资源，医疗健康行业客户可以根据其需要采用腾讯云的 IaaS、PaaS 和 SaaS 等三种不同资源形态的云计算服务。腾讯云基于信息资产和产品功能建立了如下的信息安全责任共担模型，其中定义浅蓝色部分由腾讯云负责，浅紫色部分为客户负责，浅绿部分则表示腾讯云和客户将共同承担相应的责任。如需要了解更多“腾讯云安全责任共担模型”的更多信息，请参考《腾讯云安全白皮书》。



腾讯云安全责任共担模型

由于云计算的特性，医疗健康行业客户利用腾讯云服务来搭建 GxP 系统时，其 GxP 合规由客户和腾讯云共同保障。医疗健康机构作为 GxP 系统的所有者和行业监管对象，需要对其 GxP 系统以及系统所承载的业务活动负最终的合规责任。因此，医疗健康行业客户除了需要确保其业务流程严格遵守 GxP 标准外，还需要确保系统所依赖的云服务提供商具有足够的能力支撑其满足 GxP 合规。作为医疗健康机构的云服务提供商，腾讯云将基于上述安全责任共担模型，致力于为医疗健康行业客户提供一个 GxP 合规的底层云平台，并协助医疗健康行业客户构建 GxP 合规的业务系统。腾讯云将根据客户所采用的云服务类型，为客户提供安全合规的基础设施、云产品和云服务，确保腾讯云所提供的组件满足 GxP 计算机化系统的安全要求。医疗健康行业客户应在此基础上，根据其业务需求和流程选择腾讯云适当的云产品和云服务，来开发和管理 GxP 合规的业务系统。

为了能让客户更清晰地了解腾讯云所提供的安全机制和合规能力，本白皮书将基于 GxP 标准对腾讯云的适用性，从**质量管理**、**运维**、**电子记录和数据管理**三个方面出发，向客户展开具体的合规性说明。

4. 质量管理

4.1 质量管理体系

根据 GxP 的监管要求，医疗健康行业客户需要建立和维护质量管理体系，包括质量政策、质量管理架构、质量计划和相关的流程。医疗健康机构需要结合质量目标和业务流程搭建质量管理体系，建立质量政策和质量管理组织，并定期实施管理审查，确保质量管理体系运营有效。

腾讯云作为国内率先在云计算领域获得 ISO 9001 质量管理体系认证的云服务提供商之一，最初在 2015 年首次通过第三方国际认证机构的质量管理体系认证，并获得 CNAS（中国合格评定国家认可委员会）和 ANAB （美国注册机构认可委员会）的双认可。

腾讯云严格按照 ISO9001:2015 标准的要求及公司的实际情况，建立了质量管理体系，包括质量管理手册、质量管理方针和目标、以及质量管理相关的标准及程序文件，为产品质量管理及日常运营提供了规范的架构和系统性的指南，覆盖腾讯云产品或服务的策划、设计开发、质量控制、质量保证、售后服务和质量改进等全过程，为腾讯云质量管理的落地实施提供了有效保证。

4.2 质量管理审计

根据中国国家药品监督管理局《药品生产质量管理规范》附录 1《计算机化系统》第四条，医疗健康机构应当基于风险评估的结果提供与供应商质量体系和审计信息相关的文件。为了保证腾讯云质量管理体系的适用性和有效性，腾讯云建立并实施了质量审核程序，通过对质

量管理体系定期的绩效测量、内外部审核以及管理评审，确保腾讯云质量管理体系满足质量方针和目标，并符合客户的 GxP 合规要求。

1） 质量管理体系有效性测量和评价

腾讯云会在符合法律法规的要求下，从业务活动中监测并收集有关的数据，包括顾客满意度的现状和趋势、产品和服务与顾客需求的符合性、外部供应商的绩效、体系运行情况等信息进行分析，以对质量管理体系适宜性和有效性进行全面的评价。

2） 内部审核及管理评审

为了验证质量管理体系实施效果是否达到了规定要求，以及所采取的应对风险和机遇的措施是否有效，腾讯云每年针对质量管理体系进行一次内部审核，对审核时发现的问题，会责请相关责任人及时采取纠正措施，在其后的跟踪审核活动中验证和记录所采取纠正措施的实施情况及有效性，并将每次内部审核的结果提交管理评审。

腾讯云每年会针对其质量管理体系完成一次管理评审，以确保质量管理体系持续的适宜性、充分性和有效性，并与公司的战略方向相一致。评审包括评价质量管理体系改进的机会和变更的需要，包括质量方针和质量目标。

3） 第三方审核

除了内部审核与管理评审以外，腾讯云会每半年聘请专业的第三方会计师事务所依据美国注册会计师协会（AICPA）的相关准则针对云服务体系安全控制的设计适当性和执行有效性出具的报告。通过提供具有鉴证性质的 SOC 报告（System and Organization Controls Reports），向云用户机构、独立审计师、监管机构、公司股东及其他相关利益方公开腾讯云最新的服务组织内部控制情况。此外，腾讯云每年会组织独立第三方认证机构对腾讯云 ISO9001 质量管理体系的认证进行监督审核，确保腾讯云质量管理体系的合规性和有效性。

医疗健康行业客户可以通过腾讯云的官网合规页面了解腾讯云 ISO9001 认证和 SOC 审计的更多信息，或通过腾讯云咨询工单或者在线客服等渠道获取相关的 ISO9001 认证证书和 SOC 审计报告。

4.3 文档管理

根据 GxP 的相关标准，受监管的医疗健康机构应该建立和维护程序，对组织内相关文档的分发、访问、使用和变更进行充分的控制。医疗健康机构需要建立文档管理程序，对业务的标准操作流程（SOP）和系统操作和维护相关的程序进行规范管理，确保文档的准确性和有效性。

腾讯云建立了文档管理程序，覆盖文档的编制、审批、发布、保管、使用、修订、保留和作废等阶段，以对腾讯云质量管理、云安全管理、IT 服务管理、业务连续性管理等各个管理体系的文档进行统一的管理。腾讯云文档须经相关审批责任人审核批准后才可发布，审批通过的文档将在电子文档管理平台上进行电子发布，并基于内部人员的角色和职责按需开放访问权限。文档使用者只能通过电子文档管理平台查阅相关文档，而不能对文档进行修改或其他操作。

此外，根据腾讯云的文档管理要求，文档管理员会定期或在公司组织架构、业务运作流程发生变化等情况下对相应的文档进行评审和维护。如需对文档进行修订，文档编写者完成修订后需要将修订的主要内容在“版本变更记录”中标注并提交对应的审批责任人进行审批，确保文档的修订和变更都经过批准，并保留审计跟踪记录。

4.4 人员管理

GxP 相关的标准要求计算机化系统生命周期中所涉及的各种活动，如验证、使用、维护、管理等所有相关人员应按照其职责和权限接受相应的使用和管理培训，以确保其具备适当的资格和能力执行指定的任务。因此，医疗健康行业客户需要确保其业务流程所有人、业务系统所有人、系统开发和运维人员和系统使用者等相关人员紧密合作，并定期接受计算机化系统的设计、验证、安装和运行等方面的培训和指导，能安全、准确地使用计算机化系统履行其工作职责，并及时处理工作中可能遇到的错误或故障。

对于希望通过云服务对现有的 IT 基础架构及系统进行数字化转型的医疗健康行业客户，其人员同样需要掌握云服务相关的技术能力，以降低客户在腾讯云平台上开展业务及实施项目的风险。腾讯云培训认证中心依托其多年的云上产业实践经验，提供了阶梯式的岗位技术培训认证体系以及丰富的专项技术培训资源，覆盖云开发、云运维和云架构等多个方面，助力客户建立相关的上云培训体系。

腾讯云建立并实施了员工培训制度和流程，确保员工在入职前及就职期间接受充分的岗位操作规程培训、技术能力培训和信息安全意识培训，包括办公安全、安全编码规范和安全事件处理等等。除此之外，腾讯云还会对在日常工作中需处理云服务客户数据及云服务衍生数据（如客户注册信息、产品购买记录、用户日志信息、监控数据、售后工单记录、计费信息）的人员（如产品研发、运维、产品运营团队、售后支持团队等）进行信息安全意识和技能培训，确保相关人员按照腾讯云的数据管理要求，安全合法地处理客户相关数据。

此外，腾讯云建立了安全组织架构，以规范腾讯云安全管理团队的有效运作，推动云安全各项工作的顺利开展，降低腾讯云的安全风险。针对个人信息的保护，腾讯云成立了专门的隐私和数据保护部门并指定了隐私保护负责人，以推动腾讯云各项隐私保护合规工作的规划与

落实。

4.5 供应商管理

根据美国食品和药物管理局《联邦法规法典》第 21 篇第 820 部分“质量管理要求”和《欧盟药品生产规范》第 4 卷附件 11《计算机化系统》第 3 条针对供应商和服务提供商的监管要求，医疗健康机构需要针对计算机化系统的供应商的管理制定操作规程，以确保所采用的服务提供商经过充分的评估，并通过明确的服务协议确保其提供的计算机化系统和相关服务符合质量要求。

1）供应商评估

医疗健康机构在选择云服务提供商时，有责任对潜在供应商进行充分的评估和选择并保留相关的记录。在对云服务提供商的评估过程中，客户除了需要考虑供应商满足特定要求（包括但不限于质量要求、安全要求、数据保护要求等等）的能力和可靠性等关键因素外，还可以对供应商的信誉、合规性等方面进行综合的了解和评估。

腾讯云建立了严格的供应商评估和准入流程。当需要新增供应商时，腾讯云相关采购部门和需求部门会对潜在供应商的产品交付资质和能力、技术水平、质量保证能力、在业界的业绩状况以及风险管理和治理流程等方面进行综合评估，并分析潜在供应商的可选择性及与需求的匹配程度，最终选定合适的供应商。此外，腾讯云还会对供应商进行监督管理，并定期针对供应商的合同履行情况和 SLA 达标情况进行核查，对于评估服务风险较大的供应商，会采取一定的措施以降低对腾讯云服务持续运行的负面影响或风险。

2）供应商协议

根据美国食品和药物管理局《联邦法规法典》第 21 篇第 11 部分《电子记录；电子签名–范围和应用》的相关指引，受监管的医疗健康机构在通过云服务提供商处理临床调查等敏感数

据时，需要评估云服务提供商是否有足够的控制措施来确保数据的可靠性和机密性，并与云服务提供商达成服务协议。

一般情况下，腾讯云将与客户签订两份协议，即主服务协议和服务水平协议。这两份协议及腾讯云官网内所适用的其他约束条款和细则，会包含服务细节（范围、提供地域、有效期）、服务水平、数据存储地域、机密数据的保护、腾讯云的责任、客户方的责任、安全事件通报与沟通机制、审计许可权和纠纷调解机制等。同时，客户可以选择与腾讯云签订线下协议，并通过双方法务部门商定更改协议中的特定条款和细则。

除了服务协议，腾讯云还在官网中发布了《腾讯云隐私保护声明》以及《数据处理和安全协议》，明确腾讯云和客户在数据处理中的义务，并说明腾讯云如何通过数据安全技术和安全管理措施，从使用、存储、披露、传输等多方面保障客户数据安全。根据腾讯云与客户达成的协议，客户数据将保留至服务到期或终止后的一段合理时间，客户须在保留期限届满前完成客户数据的迁移。保留期限届满后，腾讯云服务系统将自动删除相关数据。

另外，美国食品和药物管理局《联邦法规法典》第 21 篇第 820 部分“质量管理要求”还提出“在可能的情况下采购文件应包括供应商同意将产品或服务的变化通知制造商的协议，以便制造商可以确定这些变化是否会影响成品设备的质量”。根据腾讯云服务协议，当遇到下列产品或服务的变化时，腾讯云会及时通知客户：

- 针对服务平台或相关设备、系统、软件等进行的常规维护（检修、维护、升级及优化等），腾讯云会至少提前 24 小时就常规维护事宜通知客户。若因不可抗力、基础运营商过错等原因导致的非常规维护，腾讯云也会及时通知客户。
- 针对机房迁移、设备更换等重大调整，腾讯云会提前 30 天通知客户，请客户对相关调整予以配合。

- 针对由于腾讯云自身运营安排而产生的部分或全部服务的调整或终止，腾讯云会提前至少 30 天通知客户，以便客户做好相关数据的转移备份以及业务调整等，保护客户的合法权益。

4.6 系统开发生命周期

基于 GxP 标准，医疗健康机构如采用计算机化系统，则需要建立和实施特定流程和标准操作规范，覆盖计算机化系统从提出需求到终止使用的整个周期，包括设计、设定标准、编程、测试、安装、运行、维护等阶段，以确保计算机化系统的使用不会对 GxP 系统的质量控制和风险管理产生负面影响。当医疗健康行业的客户采用云服务来搭建自身的 GxP 系统时，客户需要确保云服务提供商同样建立并实施了严格的系统设计开发流程，来满足其 GxP 计算机化系统的整体安全合规性。

腾讯云一直致力于持续提升自身的云计算服务能力，以质量保证和安全可靠的产品和服务获取客户的信赖，并将这种理念嵌入到系统或产品开发和运营的每一个阶段中，并形成了具有腾讯云特色的 DevOps 模型。

DevOps 关注持续集成（Continuous Integration, CI）和持续交付（Continuous Delivery, CD），旨在快速实现系统开发和变更的同时保持系统的质量、稳定性和可用性。 腾讯云的 DevOps 模型整合了开发、运营、质量管理和安全相关的方法、工具和平台，促进了研发、运维、质量和安全团队之间的沟通和协作，以更高效、迅速地响应客户业务需求，为客户持续提供服务和价值。腾讯云 DevOps 模型包括以下几个阶段：

腾讯云系统开发生命周期

1）需求分析和策划

腾讯云通过 TAPD 平台组织新需求或迭代的开发工作。针对收集到的需求，产品团队会在 TAPD 平台上开展需求分析和优先级排序。在需求分析阶段，除了可行性分析，腾讯云产品团队还需充分考虑安全问题，以降低需求自身不合理或考虑不全面而导致的安全风险。根据腾讯云的要求，云产品或服务的需求说明文档应参照内部制定的安全原则和安全检查表加入安全设计内容，如通信安全、接口安全、权限控制、数据和隐私保护、审计日志留存和其他安全合规类的要求，并在通过正式的需求评审后才能进入下一个开发阶段。此外，产品团队还需要在此阶段对产品的整体架构和服务流程进行全面的安全风险评估，并对已识别的风险制定明确的应对方案，推动问题得到适当的跟进和解决。

2）代码编写

针对编码阶段，腾讯云制定了安全编码规范，对不同编程语言及编码场景提供安全编码实践指南，另外，腾讯云产品开发团队都需要接受相关的安全培训，以提升员工的安全编码意识以及安全编码能力。在代码转测之前，腾讯云安全团队会通过集成的代码安全检查工具对代码进行安全检查和分析，腾讯云的代码安全检查分析方案集成了静态应用程序安全测试（Static Application Security Testing，SAST）、开源组件检测、敏感信息检测等多种能

力，通过代码扫描和第三方组件安全检查等手段发现程序代码存在的安全漏洞或敏感信息，降低代码层面的安全风险。

3）构建

腾讯云利用代码工具平台进行持续构建，并由专门的工程效能团队进行流水线建设。通过对每次提交的代码进行自动化的代码检查、单元测试、编译构建，腾讯云能大大降低开发人员的工作负担并持续提升代码质量与开发效率。构建过程中的各条流水线除了自动化建设外还包含多维度的质量把控，确保开发、合流等流水线在运行过程中满足各项质量检查和时间要求。

4）测试

腾讯云建立并实施了严格的测试流程和管理规范。测试开始前，相关责任人需要对测试的技术方案进行方案评审和安全评估，并准备相应的安全测试用例和测试环境。测试期间，测试团队需要按照提测规范进行验证，并通过以下内容的测试要求清单，如发现任何功能或安全上的风险项，必须完成相关的整改，只有当测试结果通过发布质量标准要求时，才能通过此阶段并输出测试报告。

- 确认上线的产品或服务的功能点正常运作；
- 确认产品或服务的性能（如响应时间、并发处理能力）能满足需求；
- 确认产品通过安全团队的各项安全性检测；
- 确认产品或服务能长期运行稳定，未发现异常情况；
- 确认单个节点的异常不影响产品或服务的可用性。

5）发布和部署

腾讯云的发布流程将持续部署流水线化，可以对产品和服务在多个不同集群环境的发布流程控制、快速回滚等进行全流程的管控。在此阶段，腾讯云产品团队需要确保新产品已经接入 Web 应用防火墙等安全工具，并通过内部渗透测试、主机安全检测、上线前安全扫

描、安全性测试、系统漏洞扫描等安全检查，在经过产品、研发、测试、安全、运维等相关团队的审批和同意后，才可灰度发布。

6）运维和监控

腾讯云要求云产品或服务及相关支撑平台都需要保留相关组件的日志并接入监控系统，并通过对系统的日志数据和指标信息进行实时监控和智能化数据分析，快速识别异常和进行告警，并及时定位和解决问题。针对腾讯云系统的运维和监控的更多信息，请参考第 5 章节“运维”部分。

4.7 验证

按照美国美国食品和药物管理局《联邦法规法典》第 21 篇第 11 部分《电子记录；电子签名–范围和应用》的 11.10 (a)的要求，计算机化系统需要经过验证以确保系统的准确性、可靠性、以及符合预期的性能。验证是指通过检查和提供客观证据，来确认特定要求已得到满足。原则上，医疗健康机构应当负责确保其 GxP 系统是经过验证的，能按照预期准确地运行；而在云服务的环境中，客户需要确认云服务商所提供的基础设施或云服务经过严格的验证程序且符合 SLA 中的要求。基于 GxP 要求，腾讯云将从以下三个方面说明如何确保所提供的产品和服务符合定义的预期用途和服务水平，或协助客户满足 GxP 的合规性要求：

1） 确保腾讯云按照正式的软件开发生命周期进行系统的设计、开发和测试

腾讯云建立并实施了 DevOps 管理模型，并将应用程序和基础架构安全性集成到软件开发生命周期的每个阶段，包括需求分析和策划、编码、构建、测试、发布和部署以及运维和监控等，并在系统开发的全生命周期中基于风险评估结果对系统进行持续检测和安全加固，确保系统的功能和性能能满足用户需求和质量要求，具体请参照第 4.5 部分：系统开发生命周期。

2）确保腾讯云平台符合质量管理以及其他安全控制要求

腾讯云作为云服务提供商，致力于为医疗健康行业客户提供稳定可靠的云产品或服务，以及符合标准的支撑性基础设施。腾讯云遵从不同国家的合规性要求的同时按照国际认可的信息安全与 IT 管控标准、各区域及行业的法规、标准和良好实践要求规划并建设云服务。

腾讯云建立并实施了风险管理程序，每年按照云安全相关的标准和良好实践要求对云平台（包括产品、服务和支撑的系统、硬件和基础设施）进行云安全风险识别、风险分析、风险处置和风险持续监控，确保腾讯云相关资产风险水平受控。

除此以外，腾讯云每年会接受包括 ISO 体系认证、MTCS（新加坡多层云安全认证）、C5（德国云计算合规性标准目录审计）、KISMS（韩国信息安全管理体系认证）和 SOC （服务组织控制）Type2 审计等众多外部审计，其中腾讯云 SOC 2 是由第三方国际审计机构执行的、具有鉴证性质的外部审计。该审计每半年进行一次，审计范围包括腾讯云全部提供服务的数据中心、支撑性基础设施和产品，能有效证明腾讯云的相关控制（包括安全性、可用性、稳定性、过程完整性、保密性等）的设计适当性和运行有效性。

3）确保腾讯云的组件以受控的方式进行变更

针对腾讯云组件的变更，腾讯云制定了严格的变更管理程序，并通过专用的变更管理平台对不同类别的变更实施管控措施，旨在以工具化的手段确保变更管理流程系统化地落地执行。腾讯云产品、服务或相关支撑系统的变更需要经过多方面严格的验证后才可以最终完成发布，保障变更发布质量：

- 确认功能的场景验证符合预期；
- 确认现网流量、日志和监控指标未有异常情况；
- 验证现网的 API 调用请求正常执行；
- 对可能影响到的旧功能进行关键路径回归验证。

5. 运维

5.1 数据备份和恢复

为确保数据的可用性和完整性，GxP 要求医疗健康机构需要定时备份相关数据，并在验证期间检查备份数据的完整性和准确性以及恢复数据的能力，确保备份数据的保存时间满足规范中的记录保存时限。医疗健康行业客户需要通过业务风险评估的结果，确定备份的数据范围、备份频率和备份存储方式等。如果客户计划将数据托管上云，则需要依据云产品或服务的功能选择合适的数据备份服务。

腾讯云根据国家相关法律规范要求，对收集、处理的重要数据进行备份。此外，腾讯云依据云产品或服务的功能为客户提供多存储副本和备份服务，并按照产品文档或产品服务水平协议中的约定为客户提供数据备份服务，对约定范围内提供的数据备份服务承担责任。在客户选购并配置了腾讯云所提供的数据备份服务的情况下，如客户想进一步了解相关信息，客户可以通过咨询工单等形式向腾讯云提出合理的请求以获取以下的信息：

- 数据备份的范围和时间表
- 备份数据的存储位置和保存期限
- 验证备份数据完整性的程序
- 备份数据恢复的程序及时间标准等等。

5.2 日志和审计跟踪

不同的国家或地区的 GxP 标准针对药物或医疗器械的研制、生产、经营、使用活动的电子记录和数据管理的核心属性均是确保信息在全生命周期内的真实性、准确性、完整性和可追

溯性。针对可追溯性，GxP 相关标准要求“在计算机化系统中建立数据审计跟踪系统，用于记录输入、更改、确认或删除数据的操作员的身份，以及操作的日期和时间”。对此，医疗健康行业客户应注意针对 GxP 系统的风险评估结果，建立 GxP 系统的审计跟踪功能，以确保符合 GxP 的合规性要求。腾讯云为客户提供了多项日志记录或审计跟踪相关的产品和服务，客户可以自行选购配置，腾讯云会依据云产品功能和客户的配置收集相关的日志，具体请见第 7 章节“日志和审计跟踪”相关产品介绍。

根据腾讯云的日志管理策略，云产品及支撑系统都需要开启日志功能，包括且不限于系统日志和应用日志。后台运维相关的登录活动和用户操作行为都由安全组件进行监控和日志记录，记录的内容包括且不限于操作对象、操作时间、操作行为、状态等，相关日志会定期上传到远程服务器进行存储备份，禁止删除、篡改或替换。在此基础上，腾讯云安全团队会定期对各业务/系统的日志进行采集，对系统异常信息进行挖掘和分析，检测系统或操作异常，实现全链路日志安全审计。

5.3 变更和配置管理

根据 GxP 相关标准的要求，医疗健康行业客户对计算机化系统的所有更改，包括系统配置，都需要按照规定的程序以受控的方式进行，程序需要包括评估、审核、批准、实施变更和验证等过程并保留记录。对此，医疗健康行业客户需要落实针对计算机化系统或医疗健康应用的变更和配置管理流程，并确保所有变更经过审批并可以被追溯。

为了向客户提供更加完善的服务，腾讯云会定期或不定期地对云平台或相关设备、系统、软件等进行维护、升级或优化等变更操作，对此，腾讯云制定了完善的变更管理程序，规范及标准化系统变更和紧急系统变更时的操作。 腾讯云要求变更发布前，变更方案必须包括明确的变更影响范围评估和监控、回滚、结果验证方案，并经过产品、研发、测试、安全、运

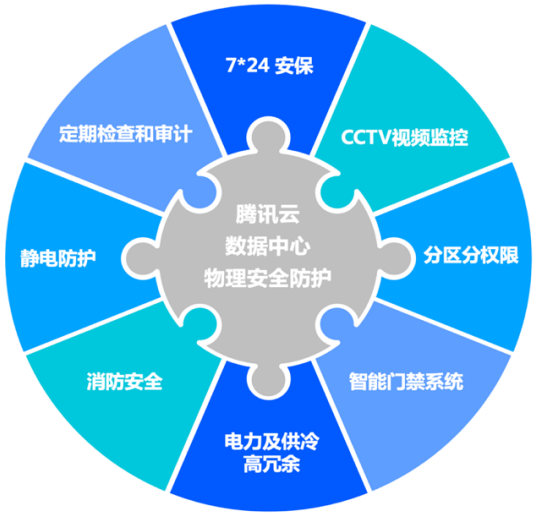
维等相关团队的评审。变更执行团队需要准确评估对客户的业务影响，做好内部团队和客户的周知，并获取相关业务负责人的变更审批。实施变更过程中，相关人员需要严格遵循变更流程的要求，并在发布后进行留守观察，对结果进行跟踪验证。除此以外，腾讯云要求每次升级尽可能安排在低峰期执行，并通过灰度分批进行发布和验证，以最大程度地减小现网影响。

除了流程方面的规范，腾讯云建立了专用的变更管理平台对不同类别的变更实施管控措施，通过工具化的手段确保变更管理流程系统化地落地执行，保障变更发布质量，提升发布实施的效率。变更管理平台通过系统地提供建单、审批、周知、发布执行服务，详细记录相关变更的申请、审批和执行过程，使得整个变更流程可追溯、可审计。

在配置管理方面，腾讯云建立了配置管理制度，并通过配置管理数据库（CMDB）统一管理各 IT 服务组件和配置项，规范配置项（CI）及其之间关系的管理，并定期对配置管理数据库进行审计，确保各配置项信息的有效性、准确性和完整性。如果变更流程中涉及配置更新，运维人员会在完成变更后根据变更方案对配置项的版本和相关信息更新到配置管理数据库。

5.4 物理安全

作为云服务提供商，腾讯云致力于为每一位客户提供安全、稳定、持续、可靠的物理设施基础，以满足 GxP 中对系统的物理安全要求，确保系统安装在适当的位置并配备充分的物理控制。



腾讯云数据中心物理安全防护措施

1）物理访问控制

腾讯云数据中心根据人员角色和访问权限建立了完整的数据中心访问控制矩阵，并在数据中心每个区域均设有门禁系统，仅授权人员才能拥有相应区域的访问权限；非长期授权人员的出入权限仅当天有效且需驻场人员或数据中心运维人员全程陪同。数据中心的监控覆盖各重要区域及出入口，并在重要区域配备了 7x24 小时无盲点的视频监控和警告系统，以禁止未经授权的访问。

2）物理环境安全

腾讯云还依据数据中心相关的国际标准和监管要求，建立了一套全方位的数据中心物理环境安全管理体系。腾讯云在全球的各数据中心均按照相关国际标准和当地安全要求进行选址、建设或租赁，并配备完整的烟雾报警系统和消防系统。各数据中心电力系统和空调系统均采用高稳定性全冗余系统，任意单点故障不会影响数据中心的电力和供冷持续性；中心内部全部安装防静电地板，机柜、线槽等均安装接地线，用以防御静电给设备带来的损害。此外，数据中心的驻场人员每日均严格遵从巡检清单和巡检计划对各数据中心和设备进行巡检，一旦发现安全违规事件，会立即启动数据中心机房管理紧急流程。

3）内外部审计

除了上述的各项物理防护措施外，腾讯云数据中心会定期进行严格的内外部审计，对机房环境、物理安全管理等维度进行符合性检查，并形成检查报告，由相关方对发现的问题及时跟进整改，通过持续改进来保证云计算数据中心的物理和环境安全。

5.5 网络安全

按照《药品记录与数据管理要求（试行）》第二十条，采用电子记录的计算机化系统的组织应确保其系统所在网络环境稳定、安全。针对云上的 GxP 系统，医疗健康行业客户需要采取访问控制或通信加密等措施，确保虚拟网络中信息传输和数据共享的安全可靠。

腾讯云制定并实施了多层级的网络安全治理和策略，以提高云平台底层网络的稳健性，包括：

1） 网络隔离

腾讯云建立了成熟的网络安全架构，腾讯云在网络边界架设防火墙，保护内部网络免受未经授权的访问。内部网络则遵从严格的隔离策略，腾讯云内部网络分开了办公网络、隔离带网络、运营网络等不同网络区域，并明确制定了区域之间的访问控制和边界防护。其中访问生产环境需要通过跳板机进行登录，未获授权的腾讯云员工不得登录到跳板机。同时，针对云端客户的网络隔离，腾讯云通过 Web 控制台访问控制、云 API 身份验证等手段确保客户只能访问自身的云资源。除此之外，腾讯云还为客户提供了私有网络（Virtual Private Cloud，VPC），客户可以通过配置网络环境、路由表、安全策略等实现网络逻辑完全隔离。

2） 网络配置安全

腾讯云还针对网络设备的安全配置制定了网络安全基线标准，包括必须启用网络设备上的安全设置、仅开放必须的网络服务功能和协议、禁止任何形式的无线网络接入生产网络、虚拟网络配置的安全策略应该与物理网络保持一致等等。腾讯云会使用配置扫描工具自动对网络设备的配置项进行扫描，如果发现异常情况，会立即触发告警并自动创建工单进行跟踪处理。

3）网络通信安全

腾讯云要求对外网开放的 Web 业务都需要配置 HTTPS 传输并使用安全的传输协议，提高外网传输的数据安全。当客户或其第三方合作伙伴、下游分包商与腾讯云之间进行通信时，客户需要结合自身安全需求和实际管控能力，采取加密措施或采用加密信道，以确保传输过程的机密性与完整性。

4）网络攻击防护

腾讯云通过内部的网络攻击防护中心实现网络安全多点监控和多层防御。网络攻击防护中心通过对流量进行分析，实时检测出各类网络攻击，快速进行网络攻击告警，协助腾讯云业务抵御来自互联网的网络攻击（如 DDOS 攻击），为业务提供安全、稳定、健康的网络运营环境。

5.6 主机安全

根据 GxP 标准，医疗健康行业在采用计算机化系统来处理和存储 GxP 活动相关的电子记录时，需要确保服务器或主机能支持系统正常运行，不对 GxP 业务造成负面影响。针对客户托管在云上的服务器，客户需要构建服务器安全防护体系。腾讯云为客户提供了云上服务器安全加固的良好实践指南以及增加主机安全能力的一系列云产品，客户可以自行选择适合的方案或产品，以降低数据泄露等网络安全风险。

在主机安全层面，腾讯云采取了一系列的防护和加固措施，以提高腾讯云底层的主机安全：

1）入侵检测与防护

入侵是指黑客利用网站和服务器漏洞，或通过窃取账号、暴力破解等方式，绕过访问控制，非法获取服务器权限，给业务造成重大损失的恶意行为。腾讯云要求业务服务器上必须部署主机安全防护和入侵检测软件，并实时检测软件的安装率。腾讯云采取分布式数据采样加上

集中分析防护的入侵检测模型，检测系统会基于特征码、用户行为等进行数据分析和挖掘，匹配入侵规则之后进行报警和防护。

2）操作系统安全

腾讯云建立并实施了基础设施与虚拟化安全管理标准，以对主机的操作系统进行安全基线检查，并根据系统的信息安全评估结果制定相应的系统加固方案，包括禁用系统中不经常使用或者不必要的服务和程序、使用足够强度的口令等等。此外，按照腾讯云的管控要求，Windows 系统必须安装防病毒软件并配置病毒库自动更新，并每月进行安全例行检查，及时对主机操作系统进行升级和更新补丁等。此外，补丁更新需要遵循变更控制流程，并对加固后的系统进行全面的测试，确保加固不会对系统业务带来负面影响。

5.7 应用程序安全

GxP 标准要求受监管机构所使用的计算机化系统所使用的应用软件需要符合相关的法律要求和管理要求。医疗健康行业客户需要确保其开发设计的应用程序能符合业务需要和合规性要求；腾讯云则通过应用防护、应用脆弱性检测和漏洞修复的闭环，全面保障云产品或服务的安全可靠性：

1）应用防护

腾讯云基于其成熟的安全技术能力为其云上应用构建了多层次、立体化的安全防护体系，并要求对外开放的资源需要接入漏洞扫描、DDoS 防护和网络应用防火墙等安全防护系统。在 Web 防护能力层面，腾讯云通过 Web 入侵防护、0Day 漏洞补丁修复、Bot 行为管理和 DNS 劫持检测等多维度防御策略全面抵御恶意攻击，保障云上系统及业务安全运营。

2）应用脆弱性检测

除了高危服务/端口开发检测、管理后台开放检测、主机入侵检测、容器运行检测等多项技术检测手段之外，腾讯云还会定期对平台与产品进行漏洞扫描。针对漏洞扫描，腾讯云要求对外的 Web 系统必须部署漏洞防护系统，并通过“定时任务”检测腾讯云的 Web 业务服务器，快速感知和修复业务中存在的风险，避免 Web 漏洞被外界恶意利用。另外，腾讯云会针对关键系统进行渗透测试，测试会通过人工模拟进行外部和内部攻击，并在设定攻击向量（Attack vector）时考虑过往腾讯云遇到的威胁和漏洞。腾讯云还会进行红蓝对抗的安全演习，通过持续对抗演习来验证整体的安全防御情况，以发现疏漏的风险盲点并提升响应效率，从而实现整体安全体系的不断完善与持续提升。

3）漏洞修复

腾讯云的安全漏洞管理平台会针对发现的安全漏洞或安全风险自动生成安全工单，相应的产品部门需要根据安全工单的类型和风险等级及时进行漏洞修复评估和快速止损，并在根因分析的基础上确定整改措施和修复计划。如评估中发现的云平台漏洞可能对客户产生影响，腾讯云会通过官网公告、站内信等方式，将漏洞概述、影响范围与程度等信息及时同步给客户，并为客户提出相关修复建议及具体操作指引。

5.8 身份认证与访问控制

GxP 标准中明确要求医疗健康机构在使用计算机化系统操作业务流程时，需要确保只有经过授权的人员方能使用系统或访问系统中的数据。医疗健康行业客户需要负责其组织内部的身份认证和访问权限管理，避免系统或数据遭受未经授权的访问。作为云服务提供商，腾讯云为客户提供了访问管理服务（Cloud Access Management, CAM）协助客户管理其腾讯

云的账号和子账号。通过 CAM，客户能安全地管理腾讯云账户的访问权限，资源管理和使用权限。关于 CAM 的更多详细介绍，请参考本白皮书第 7 部分。

对于腾讯云的底层基础设施和后台的日常运维，为降低信息资产被未经授权访问的风险，腾讯云制定了严格的云平台运维安全管理策略来规范腾讯员工针对云服务器的访问与运维行为，并确保内部访问权限矩阵满足最小授权和职责分离的原则，包括：

- 腾讯云内部所有用户的账号必须使用唯一标识符，确保账号与操作人员有唯一对应关系。
- 腾讯云员工入职时仅会被赋予职位角色所需要的最小权限，运维管理团队员工仅在必要及通过审批的情况下可获得授权，并通过双因素认证（Two-Factor Authentication）登录到跳板机和目标机器进行运维操作。
- 腾讯云安全团队部署了安全组件来记录跳板机和主机上的命令操作，相关的登录活动和用户敏感操作如修改、删除、传输档案等都会通过安全组件进行监控。

5.9 事件响应

近年来全球医疗系统遭遇网络攻击的事件时有发生，医疗健康行业逐渐成为网络安全的重灾区，各国的 GxP 标准也要求受监管的医疗健康机构需要针对系统故障或数据错误等安全事件建立操作规程，以确保所有事件都被适当地记录、评估、处理，并基于根本原因的分析采取相应的纠正和预防措施。针对发生在腾讯云责任范围内的安全事件，腾讯云已经制定了标准化、流程化的事件应急处置机制，以在第一时间对安全事件作出响应，向客户通报，并为医疗行业客户进行事件处理提供支持。如果事件是发生于客户的责任范围内，腾讯云的团队也会提供适当的协助支持客户去处理事件及事故。

根据腾讯云的安全事件应急处置机制，当安全告警被触发后，云安全团队会根据危害程度和紧急程度等对事件的风险进行评估和定级，相关团队会按照事件的定级启动应急预案，防止

事态的进一步扩大，并通过日志等方式进行排查，在确定攻击路径、告警原因和影响范围后采取措施排除故障，恢复系统或服务，必要时启动业务持续性管理计划。在消除故障影响后，相关部门需对事件进行复盘和根因分析，以采取纠正措施并优化已有的安全策略。腾讯云会按照法律法规和有关要求向相关方对事件的响应和处置过程进行报告。

此外，为了配合客户的事件响应程序，协助客户满足合规要求，腾讯云以完善的运营安全能力提供全天候技术支持。腾讯云为客户提供多个渠道，包括 7*24 小时工单、7*24 小时热线、智能客服、自助服务等，不间断处理客户提出问题和反馈。腾讯云的客服团队和技术专家会为客户提供迅速、有效的支持，协助客户高效识别问题根源，追踪事故发展，提供适合的解决方案，快速为客户解决关于云产品功能、腾讯云基础设施、底层网络与主机等问题。除基础服务支持以外，业务系统复杂的企业客户还可以选择其他适用的服务计划，获取专属支持群、专属技术服务经理、增值服务等组成的专属支持。

5.10 业务连续性管理

GxP 要求医疗健康机构需基于风险评估制定支持关键业务流程的计算机化系统的应急方案，以确保在故障发生时业务流程的连续性。为确保医疗健康系统的持续平稳运行和患者数据的完整性，保障用户的生命安全，医疗健康行业客户需要针对业务场景的敏感性制定业务连续性计划，同时确保其医疗系统组件的稳健性。腾讯云从云服务提供商角度出发，从基础架构高可用性、网络和计算单元的容灾性和日常的业务连续性管理等三个方面来保障所提供的云平台及云服务的业务连续性：

1）基础架构高可用性

腾讯云在全球 26 个地理区域内运营着 70 个可用区，底层拥有多于 10 个互联网服务供货商

（Internet Service Provider，ISP），客户可根据业务发展需求，自主将业务灵活地部署在不同区域，以保证业务的容灾性要求。另外，腾讯云数据中心的基础架构建设及环境设计，包括供电系统、空调系统、火灾检测防护系统、动力系统等都具备灾备冗余，保证客户最底层基础设施的高可用性。

2）网络和计算单元容灾性

腾讯云网络采用 N*N 的冗余建设方式，配合路由层级的路径优先和路由可达性的流量工程调度，保证不因为单点设备故障而导致网络服务中断。腾讯云还建立了基础网络灾难恢复计划，如数据中心互联线路故障流量切换，以增强腾讯云网络的跨地域容灾能力。针对运营商侧的公网故障，腾讯云的数据中心网络出口分多个地域对接多个运营商，能有效地降低带来的持续性影响。另外，腾讯云的计算单元也是采用 N*N 的冗余建设方式，单一计算单元在故障发生时会通过调度器实时剔除，保障业务的可用性要求。

3）日常业务连续性管理

腾讯云高度重视云平台自身的业务连续性管理，通过建立和实施内部流程确保业务运作能达到可用性要求，并能支持客户整合其业务连续性计划。腾讯云建立并实施了业务连续性管理体系，是国内首批通过 ISO22301 业务连续性管理体系认证的云服务提供商。

腾讯云各产品团队根据对系统和业务流程的业务影响分析结果，建立相关的业务连续性管理计划和应急预案，确保在业务中断时腾讯云能按照要求恢复并继续运行业务和系统。此外，各产品团队需要定期对其业务连续性计划和应急预案进行演练，并根据演练结果对连续性计划和应急预案的合理性和有效性组织进行评估，并对恢复时间目标、恢复点目标、操作流程或岗位职责等进行适当的审阅和更新。腾讯云与合作的数据中心运营商也会定期设计不同的灾难和紧急状况，并设定相应的应急计划来进行定期的应急训练，确保相关人员能熟练有序地完成业务恢复流程。

6. 电子记录和数据管理

6.1 电子记录和数据的管理规程

根据《药品记录和数据管理要求》的要求，从事药品研制、生产、经营、使用活动的医疗健康机构应当遵守法律、法规、规章、标准和规范，制定操作规程和管理制度，明确记录与数据的管理要求。对此，医疗健康行业客户需要结合实际的业务情况建立数据安全管理体系。腾讯云建立了数据安全相关制度和管理规范，以明确腾讯云内部员工应该遵循的数据安全流程和标准，包括数据分类分级管理、数据全生命周期管理、数据安全风险评估、数据安全审计和数据安全事件处置等多个维度的要求，以提升腾讯云数据安全的整体水位，降低数据合规数据泄露的风险。

6.2 电子记录和数据的保护

由于医疗健康数据的完整性和准确性会直接影响患者的生命安全，因此数据一直是医疗健康行业的生命线。国内《药品记录与数据管理要求（试行）》第四条、第五条和第八条，以及美国《电子记录；电子签名–范围和应用》11.10（b）、11.10（c）和 11.30 均提出了对电子记录和数据的保护要求，即医疗健康机构如果采用计算机化系统创建、修改、维护或传输电子记录，应采用相关程序和控制，以确保电子记录从创建到销毁的真实性、完整性以及机密性，使机构在整个记录保留期内准确和方便地对记录进行检索、检查或复制。

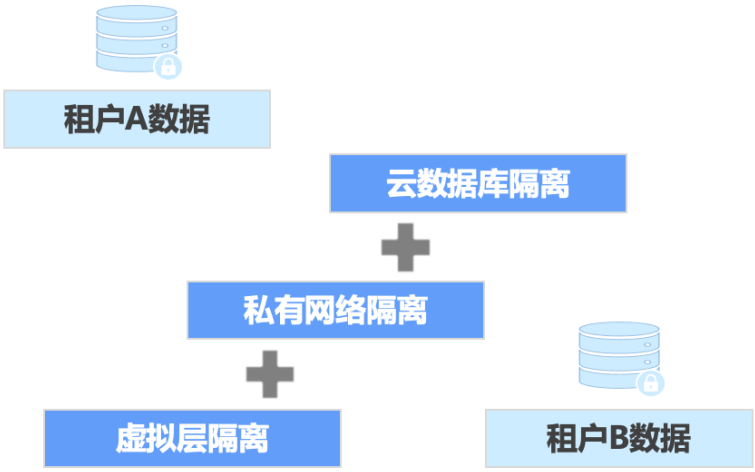
就云上 GxP 系统中的业务数据而言，客户对其托管于云端的数据拥有完全的控制权，并对自身存放在云端上的业务数据的安全管理负最终责任，因此医疗健康行业客户需要依据业务

需要和 GxP 中的要求，执行相应的管理措施或采用腾讯云上提供的相关数据安全产品或功能，确保数据在采集、处理、存储等活动中的真实、准确、完整和可追溯。

腾讯云平台本身也采取了多项管理措施和技术手段，致力于协助客户保障云上数据的机密性、完整性和可用性：

1）数据机密性：

- **数据隔离：**腾讯云通过多层技术隔离手段，保证同一资源池内客户数据互不可见，从技术上保证客户不能访问、获取或篡改其他客户的数据。
  - **虚拟层：**腾讯云应用成熟的硬件虚拟化技术在虚拟层为云服务器等资源提供完整的租户间虚拟资源隔离能力，不同用户的网络、内存、磁盘等资源均通过底层逻辑访问控制杜绝了互通互访的可能性，确保每位客户只能访问其已购买的云计算资源，有效实现不同客户之间的数据隔离。
  - **网络层：**私有网络（Virtual Private Cloud, VPC）是腾讯云为客户构建的专属云上网络空间，客户可通过配置私有网络实现网络逻辑隔离。客户可以在 VPC 内自定义网段划分、IP 地址和路由策略等，并通过网络 ACL 和安全组分别从子网和主机维度筛选流量，通过完全的网络隔离确保不同客户之间的数据隔离。
  - **云数据库层：**在客户使用云数据库时，腾讯云通过配置防火墙策略，采用白名单过滤机制对网络层进行了隔离。此外，腾讯云通过对数据库实例的权限控制机制来保证每个客户只能获取其对应的数据，而无法看到其他客户的数据。此外，腾讯云还提供独享集群数据库，可以让客户独享物理集群资源，并灵活创建多种自定义规格的云数据库。



腾讯云租户之间的数据隔离保障

- **数据加密：**腾讯云依据产品功能为传输、存储状态下的客户数据提供加密功能，并支持客户选择管理自己的加密密钥。针对传输状态下的数据，腾讯云会对客户通过互联网访问腾讯云控制台的通信进行 HTTPS 加密；同样地，客户通过云 API 与腾讯云之间的通信亦支持 HTTPS 数据加密传输协议，以提升数据的机密性。对于存储状态下的数据，腾讯云也为医疗健康行业客户提供了加密密钥管理服务以及多种用于数据存储加密的产品，客户可以按需求进行购买与配置，以保护静态数据。
  - **数据销毁：**腾讯云同样重视数据在最后一个环节中的机密性保护。针对医疗健康行业客户托管在云上的业务数据，当云服务协议终止或客户主动删除数据时，腾讯云将根据与客户达成的协议，采用业界认可的机制，对存储介质进行数据擦除和覆写，保证存储在数据盘内的数据被完全擦除，确保被删除的数据不可恢复。针对损坏或退役的存储介质的销毁，腾讯云建立了完善的数据存储介质销毁流程和方案，将采用消磁、物理损坏的方式对存有敏感数据的存储介质进行处理，并确保全流程闭环、可控，并有相关记录和录像可追溯。

2）数据完整性：

- **数据完整性校验：**腾讯云在存储数据时采用多副本冗余存储和纠删码技术，在检测到完

整性错误时立即采取必要的恢复措施，以提高数据的容错能力。此外，客户在通过腾讯云 API 发送请求时，每个请求都需要在公共请求参数中包含签名信息以验证客户的身份并保证请求的完整性。

- **数据访问控制：**作为云服务提供商，腾讯云承诺除法律法规行政规章另有规定或双方另有约定外，不会访问或使用客户托管在腾讯云中的业务数据。同时，腾讯云通过严格的运维访问控制流程和技术手段，防止腾讯云后台运维人员对客户存放在云端上的数据进行未授权的操作或非法修改。

3）数据可用性：

- **支持多存储副本：**腾讯云为客户提供多存储副本和备份服务，客户应根据自身的需求自行对数据进行备份。腾讯云支持客户选择将数据存储在不同的存储节点上，以预防由于硬件故障或其他因素导致的数据丢失。
- **容灾能力：**腾讯云在全球 26 个地理区域内运营着 70 个可用区，可用区是指在同一地域内电力和网络互相独立的物理数据中心，能够保证可用区间故障相互隔离，而不会扩散到并影响其他可用区。腾讯云的多项基础产品如云服务器、云数据库等都具备集群内容灾和跨可用区容灾的能力，有能力协助客户在发生不可预测的灾害的情况下及时恢复云端的应用程序和数据，从而缩短业务中断时间，保证客户数据的可用性。

如需要了解关于腾讯云数据安全的更多信息，请参照**《腾讯云数据安全白皮书》**。

7. 腾讯云的产品和服务如何支持客户 GxP 合规

腾讯云除了通过云平台的管理流程和技术措施满足 GxP 中的合规要求外，还致力于通过提供全方位、多样化的云产品和工具，支持医疗健康行业的客户构建安全稳定的云上 GxP 系统。以下的表格选取了一些具有代表性的腾讯云产品或服务，并说明了客户可以如何通过这些腾讯云产品或服务，增强其云上 GxP 系统的安全性和合规性。

如需要进一步了解腾讯云的更多产品和信息，请参照腾讯云官网产品页。

域	产品或服务名称	功能
系统开发生命周期	Coding DevOps	CODING DevOps 包括代码托管、项目管理、测试管理、持续集成、制品库等多款产品和服务，涵盖软件开发从构想到交付的一切所需，使研发团队在云端高效协同，实践敏捷开发与 DevOps，提升软件交付质量与速度。
	腾讯云代码分析	腾讯云代码分析是集众多代码分析工具的云原生、分布式、高性能的代码综合分析跟踪管理平台，其主要功能是持续跟踪分析代码，观测项目代码质量，支撑团队传承代码文化。
	测试服务 WeTest	测试服务 WeTest 包括标准兼容测试、专家兼容测试、手游安全测试、远程调试等多款产品，服务于海量腾讯精品游戏，涵盖兼容测试、压力测试、性能测试、安全测试、远程调试等多个方向，立体化安全防护体系，保卫您的信息安全。
数据迁移验证	数据传输服务 DTS	腾讯云数据传输服务（Data Transmission Service，DTS）可帮助用户在业务不停服的前提下轻松完成数据库迁移上云，利用实时同步通道轻松构建高可用的数据库多活架构，通过数据订阅来满足商业数据挖掘、业务异步解耦等场景需求。同时，DTS 还提供私有化独立输出版本 DTS-DBbridge，DTS-DBbridge 支持异构数据库和同构数据库之间迁移和同步，可以帮助企业实现完整数据库迁移（例如 Oracle 数据库）。通过 DTS 可以帮助客户进行数据校验，从而验证数据迁移过程中的完成性。
	迁移服务平台 MSP	迁移服务平台（Migration Service Platform，MSP）整合了各种迁移工具，并提供统一监控。用户在迁移时可选择腾讯云官方迁移工具，也可选择官方认证的第三方迁移工具。迁移服务平台帮助用户方便快捷的将系统迁移上云，并清晰掌握迁移进度。通过 MSP 可以帮助客户对迁移过程进行统一监控，防止出现迁移过程中数据完整性被破坏的可能。

域	产品或服务名称	功能
数据备份和恢复	对象存储 COS	对象存储（Cloud Object Storage，COS）是由腾讯云推出的无目录层次结构、无数据格式限制，可容纳海量数据且支持 HTTP/HTTPS 协议访问的分布式存储服务。 用户放在对象存储上的数据可以通过跨区域复制功能同时存储在多个指定区域，保证在某些意外丢失部分数据的情况下仍能通过冗余数据来查找并恢复完整数据，同时，因为多份数据存放在不同的地区，因此能避免一个地区的存储受到不可抗逆灾难时会造成的损失，从而达到多冗余备份和异地容灾的效果，保证数据的持久性和稳定性，为重要数据加上多重保险。
	云硬盘 CBS	云硬盘（Cloud Block Storage，CBS）为您提供用于 CVM 的持久性数据块级存储服务。 CBS 提供高达 99.9999999%的数据可靠性。在每个存储写入请求返回给用户之前，CBS 就已确保数据被成功写入三份跨机架的存储节点中。CBS 的数据复制机制高于业内平均水平，能够保证任何一个副本故障时快速进行数据迁移恢复，以保护您的应用程序免受组件故障的威胁。
	文件存储	文件存储（Cloud File Storage，CFS）为您提供安全可靠、可扩展的共享文件存储服务。 文件存储标准文件存储为 3 份冗余，具有极高的可用性和可靠性。文件存储可以通过用户隔离，网络隔离，以及来访白名单来限制客户端的操作权限。
	归档存储	腾讯云 COS 归档存储（COS Archive Storage）是腾讯云对象存储 COS 低成本、持久可靠的存储类型，为企业和个人开发者提供海量、非结构化数据的长时间备份能力。与本地备份相比，归档存储采用分布式云端存储架构，您无需关注硬件维护及容量扩展，当您需要数据时，可以通过 RESTful API 对存储的数据进行恢复并设置有效期来访问。
	数据库备份服务 DBS	数据库备份服务（Database Backup Service，简称 DBS）是为用户提供连续数据保护、低成本的备份服务。数据库备份拥有一套完整的数据备份和数据恢复解决方案，具备实时增量备份以及快速的数据恢复能力，它可以为多种部署形态的数据库提供强有力的保护，包括企业 IDC 数据中心、其他云厂商数据库及腾讯公有云数据库。
日志和审计跟踪	云审计 CloudAudit	云审计 CloudAudit 是一项支持对您的腾讯云账号进行监管、合规性检查、操作审核和风险审核的服务。借助 CloudAudit，您可以记录日志、持续监控并保留与整个腾讯云基础设施中操作相关的账号活动。CloudAudit 提供腾讯云账号活动的事件历史记录，这些活动包括通过腾讯云管理控制台、API 服务、命令行工具和其他腾讯云服务执行的操作。这一事件历史记录可以简化安全性分析、资源更改跟踪和问题排查工作。
	T-Sec 数据安全审计 DSAudit	腾讯云数据安全审计（Data Security Audit，DSAudit）是一款基于人工智能的数据库安全审计系统，可挖掘数据库运行过程中

域	产品或服务名称	功能
		各类潜在风险和隐患，为数据库安全运行保驾护航，是企业的等保合规利器。
	日志服务 CLS	日志服务（Cloud Log Service，CLS）是腾讯云提供的一站式日志服务平台，提供了从日志采集、日志存储到日志检索，图表分析、监控告警、日志投递等多项服务，协助用户通过日志来解决业务运维、服务监控、日志审计等场景问题。
网络安全	专线接入 DC	专线接入（Direct Connect，DC）为您提供了一种便捷的连接企业数据中心与腾讯云的方法，您可通过专线接入建立与公网完全隔离的私有连接服务，相比公网，专线接入具备更安全、更稳定、更低时延、更大带宽等特性。您只需要一条运营商物理专线一点接入腾讯云，便可快速创建多条专用通道打通部署于腾讯云的计算资源，实现灵活可靠的混合云部署。
	私有网络 VPC	私有网络（Virtual Private Cloud，VPC）是基于腾讯云构建的专属云上网络空间，为您在腾讯云上的资源提供网络服务，不同私有网络间完全逻辑隔离。作为您在云上的专属网络空间，您可以通过软件定义网络的方式管理您的私有网络 VPC，实现 IP 地址、子网、路由表、网络 ACL 、流日志等功能的配置管理。私有网络还支持多种方式连接 Internet，如弹性 IP 、NAT 网关等。同时，您也可以通过 VPN 连接或专线接入连通腾讯云与您本地的数据中心，灵活构建混合云。
	VPN 连接	VPN 连接（VPN Connections）是一种基于网络隧道技术，实现本地数据中心与腾讯云上资源连通的传输服务，它能帮您在 Internet 上快速构建一条安全、可靠的加密通道。VPN 连接具有配置简单，云端配置实时生效、可靠性高等特点，其网关可用性达到 99.95%，保证稳定、持续的业务连接，帮您轻松实现异地容灾、混合云部署等复杂业务场景。
	T-Sec DDoS 防护	DDoS 防护（Anti-DDoS）具有全面、高效、专业的 DDoS 防护能力，为企业组织提供 DDoS 高防包、DDoS 高防 IP 等多种 DDoS 解决方案，应对 DDoS 攻击问题。通过充足、优质的 DDoS 防护资源，结合持续进化的“自研+AI 智能识别”清洗算法，保障用户业务的稳定、安全运行。
	T-Sec 云防火墙	腾讯云防火墙（Cloud Firewall，CFW）是一款基于公有云环境下的 SaaS 化防火墙，主要为用户提供互联网边界的防护，解决云上访问控制的统一管理与日志审计的安全与管理需求。云防火墙不仅具备传统防火墙功能，同时也支持云上多租户、弹性扩容功能，是用户业务上云的第一个网络安全基础设施。
	T-Sec 网络入侵防护系统	网络入侵防护系统（Network Intrusion Prevention System，NIPS），是基于腾讯安全服务内部数百条业务线的运维经验积累和大数据处理能力的结合，通过旁路部署的方式，提供了网络层 ACL（访问控制）和日志审计功能，解决云平台监管、ACL 控制、安全治理等问题，并辅助客户满足适用的合规要求。
	T-Sec 高级威胁检	腾讯云高级威胁检测系统（Network Traffic Analysis System，

域	产品或服务名称	功能
	测系统	NTA，简称：腾讯御界），通过镜像方式采集企业网络边界流量，结合腾讯多年积累的海量安全数据，运用数据模型、安全模型、感知算法模型识别网络攻击及高级威胁（APT）。同时，对事件告警原始流量进行留存，方便事后追溯，可极大提升云环境下的威胁感知能力。
主机安全	T-Sec 主机安全	主机安全（Cloud Workload Protection，CWP）基于腾讯安全积累的海量威胁数据，利用机器学习为用户提供资产管理、木马文件查杀、黑客入侵检测、漏洞风险预警及安全基线等安全防护服务，解决当前服务器面临的主要网络安全风险，帮助企业构建服务器安全防护体系。现支持用户对腾讯云外服务器统一进行安全防护，轻松共享腾讯云端安全情报，让私有数据中心拥有云上同等级别的安全体验。
应用程序安全	T-Sec Web 应用防火墙	腾讯云 Web 应用防火墙（Web Application Firewall，WAF）帮助腾讯云内及云外用户应对 Web 攻击、入侵、漏洞利用、挂马、篡改、后门、爬虫等网站及 Web 业务安全防护问题。企业组织通过部署腾讯云 WAF 服务，将 Web 攻击威胁压力转移到腾讯云 WAF 防护集群节点，分钟级获取腾讯 Web 业务防护能力，为组织网站及 Web 业务安全运营保驾护航。
	T-Sec 漏洞扫描服务	漏洞扫描服务（Vulnerability Scan Service，VSS） 是一款自动探测企业网络资产并识别其风险的产品。依托腾讯二十年累积的安全能力，漏洞扫描服务能够对企业的网络设备及应用服务的可用性、安全性与合规性等进行定期的安全扫描、持续性风险预警和漏洞检测，并且为企业提供专业的修复建议，降低企业安全风险。
身份与访问控制	访问管理 CAM	访问管理（Cloud Access Management，CAM）是腾讯云提供的一套 Web 服务，用于帮助客户安全地管理腾讯云账户的访问权限，资源管理和使用权限。通过 CAM，您可以创建、管理和销毁用户（组），并通过身份管理和策略管理控制哪些人可以使用哪些腾讯云资源。
	T-Sec iOA 应用安全访问服务	iOA 应用安全访问服务（Application Secure Access Service）是一款基于零信任架构的应用安全访问云平台，为企业提供安全接入数据中心（本地、单云、混合云）的解决方案。iOA 应用安全访问服务依托腾讯云全球加速节点，为企业员工提供快速、稳定的访问体验，适用于远程办公、数据中心接入、权限控制、终端管控等多种业务场景。同时，iOA 应用安全访问服务支持对接企业微信，通过企业微信安全访问内网应用，接入简单、安全可靠、管控全面可视化。
	T-Sec 多因子身份认证 MFAS	多因子身份认证（Multi-factor Authentication Service，MFAS）的目的是建立一个多层次的防御体系，通过结合两种或三种认证因子（基于记忆的/基于持有物的/基于生物特征的认证因子）验证访问者的身份，使系统或资源更加安全。攻击者即使破解单一因子（如口令、人脸），应用的安全依然可以得到保障。
	数字身份管控平台	数字身份管控平台（Identity and Access Management）为您提

域	产品或服务名称	功能
	IDAM	供集中式的数字身份管控服务。在企业 IT 应用开发时，数字身份管控平台可为您集中管理用户账号、分配访问权限以及配置身份认证规则，避免因员工账号、授权分配不当导致的安全事故。在互联网应用开发时，数字身份管控平台可为您打通应用的身份数据，更好地实现用户画像，也可为用户提供便捷的身份认证体验，提升用户留存。
事件响应	云监控 CM	云监控（Cloud Monitor，CM）支持您针对云产品资源和自定义上报资源设置指标阈值告警。为您提供立体化云产品数据监控、智能化数据分析、实时化异常告警和可视化数据展示，让您实时、精准掌控业务和各个云产品健康状况，提升运维效率，减少运维成本。
电子记录和数据保护	T-Sec 数据安全中心 DSGC	数据安全中心（Data Security Center，DSGC）帮助企业自动梳理数据资产，对企业云上数据进行分类分级和安全风险评估，并协同腾讯云各安全能力，形成闭合的数据安全防护网，帮助企业最大化提升安全效益。
	T-Sec 密钥管理系统	密钥管理系统（Key Management Service，KMS）是一款安全管理类服务，可以让您轻松创建和管理密钥，保护密钥的保密性、完整性和可用性，满足用户多应用多业务的密钥管理需求，符合合规要求。
	T-Sec 数据脱敏	数据脱敏（Data Masking，DMask）是一款敏感数据脱敏与水印标记工具，可对数据系统中的敏感信息进行脱敏处理并在泄漏时提供追溯依据，为企业数据共享、迁移、分发提供安全保护措施。
	数据保险箱 CDCS	数据保险箱（Cloud Data Coffer Service，CDCS）为您提供更高安全系数的企业核心数据存储服务。您可以通过自定义过期天数的方法删除数据，避免误删带来的损害，还可以将数据跨地域存储，防止一些不可抗因素导致的数据丢失。数据保险箱支持通过控制台、API 等多样化方式快速简单接入，实现海量数据的存储管理。您可以使用数据保险箱对文件数据进行上传、下载，最终实现数据的安全存储和提取。

结语

医疗健康行业的数字化转型浪潮驱动越来越多的医疗健康机构将业务系统和数据都迁移到云端，而机构在使用云服务提供商所提供的基础设施或云服务来搭建 GxP 系统则需要对业务上云进行充分的规划和评估。医疗健康行业客户一方面需要梳理和了解其 GxP 系统中的云架构，另一方面也需要对云服务提供商进行评估，了解云服务提供商是否具备充分的安全能力和控制措施来确保系统的稳定和数据的安全。

本白皮书从质量管理、运维和电子记录和数据管理等三个方面描述了腾讯云如何通过内部管理流程和安全技术手段，保障云产品和服务的质量和安全可靠性，协助医疗健康行业的客户满足 GxP 的合规要求。经过多年的云服务经验积累和安全能力沉淀，腾讯云不仅能为客户提供符合行业良好实践的云产品和服务，还通过专业的安全能力和技术手段协助客户对云上 GxP 系统进行持续的安全防护和快速的安全事件响应，携手客户构建云上 GxP 系统的安全保障体系，赋能医疗健康行业客户进一步提升 GxP 合规管控能力，为医疗健康行业客户的上云之旅保驾护航。

附录：GxP 标准分析及映射表

欧盟药品管理局《欧盟药品生产规范》 第 4 卷 附件 11《计算机系统》			
序号	**域**	**GxP 标准要求**	**腾讯云适用性及 白皮书对应章节**
1	风险管理	应在计算机化系统的整个生命周期中应用风险管理，并考虑到患者安全、数据完整性和产品质量。 作为风险管理系统的一部分，关于验证程度和数据完整性控制的决定应基于对计算机化系统的合理且记录在案的风险评估。	客户应对 GxP 系统的整个生命周期进行风险评估。 腾讯云将风险管理融入至系统的全生命周期中，具体请见 4.6 系统开发生命周期和 4.7 验证部分。
2	人员	流程所有者、系统所有者、持证人员和 IT 等所有相关人员之间应密切合作。所有人员都应具备适当的资格、访问级别和明确的职责，以履行其分配的职责。	客户需要确保 GxP 系统的相关人员具备相关的系统、流程操作技能和资质。 腾讯云建立并实施了人员培训的相关机制，确保自身员工具有足够的资质、能力和信息安全意识，具体请见 4.4 人员管理。
3	供应商管理	3.1 当使用第三方（例如供应商、服务提供商）时，例如 提供、安装、配置、集成、验证、维护（例如通过远程访问）、修改或保留计算机化系统或相关服务或用于数据处理，制造商与任何第三方之间必须存在正式协议，这些协议应包括明确说明第三方的责任。公司内部 IT 部门与第三方服务商同等处理。 3.2 供应商的能力和可靠性是选择生产服务供应商的关键因素。审计的必要性应基于风险评估。	客户有责任对供应商的能力进行评估并和供应商签订协议，明确双方责任。 腾讯云作为云服务提供商，会配合医疗健康行业客户 GxP 的合规需要，配合客户对腾讯云的供应商评估和供应商协议制定，具体请见 4.5 供应商管理。

欧盟药品管理局《欧盟药品生产规范》 第 4 卷 附件 11《计算机系统》			
序号	**域**	**GxP 标准要求**	**腾讯云适用性及 白皮书对应章节**
		3.3 商业现货产品提供的文件应由受监管的用户审查，以检查用户要求是否得到满足。 3.4 与供应商或软件开发商和实施系统有关的质量体系和审计信息应按要求提供给检查员。	腾讯云建立并实施了质量审核程序，通过对质量管理体系的定期审核，确保腾讯云质量管理体系满足质量方针和目标，并符合客户的 GxP 合规要求。具体请见 4.2 质量管理审计。
4	验证	4.1 验证文件和报告应涵盖生命周期的相关步骤。制造商应能够根据风险评估证明其标准、协议、验收标准、程序和记录的合理性。 4.2 验证文件应包括变更控制记录（如果适用）和在验证过程中观察到的任何偏差的报告。 4.3 应提供所有相关系统及其良好生产规范 GMP 功能（清单）的最新列表。对于关键系统，应提供最新的系统描述，详细说明物理和逻辑安排、数据流和与其他系统或流程的接口、任何硬件和软件先决条件以及安全措施。 4.4 用户要求规范应描述计算机化系统所需的功能，并基于记录的风险评估和良好生产规范 GMP 影响。用户需求应该在整个生命周期中是可追溯的。 4.5 受监管的用户应采取一切合理的步骤，以确保系统的开发符合适当的质量管理体系。应适当评估供应商。 4.6 对于全定制或半定制的计算机化系统的验证，应该有一个流程来确保对系统的所有生命周期阶段的质量和性能测量进行正式评估和报告。 4.7 应证明适当的测试方法和测试场景的证据。特别应考虑系统（过程）参数限制、数据限制和错误处理。自动化测试工具和测试环境应该对其充分性进行记录评估。	客户需要根据风险评估的结果确定验证的范围与程度，确保系统组件功能符合预定用途。 腾讯云通过系统开发生命周期对所提供的云平台服务和产品进行质量和安全管理，并确保相关组件保持验证的状态，具体请见 4.6 系统开发生命周期 和 4.7 验证。 腾讯云制定了完善的变更管理程序、规范及标准化系统变更和紧急系统变更时的操作，具体请见 5.3 变更和配置管理。

欧盟药品管理局《欧盟药品生产规范》 第 4 卷 附件 11《计算机系统》			
序号	**域**	**GxP 标准要求**	**腾讯云适用性及 白皮书对应章节**
		4.8 如果数据被转移到另一种数据格式或系统，验证应包括检查数据在此迁移过程中的价值和/或含义是否没有改变。	
5	数据	与其他系统以电子方式交换数据的计算机化系统应包括适当的内置检查，以确保正确、安全地输入和处理数据，以将风险降至最低。	受 GxP 监管的医疗健康机构需要结合业务流程使用合适的内置检查节点或加密手段，确保电子数据以安全的方式进行数据交换和数据处理。 腾讯云会对客户通过互联网访问腾讯云控制台的通信进行 HTTPS 加密，腾讯云云 API 与腾讯云之间的通信亦支持 HTTPS 数据加密传输协议，具体请见 6.2 电子记录和数据的保护。
6	准确性检查	对于手动输入的关键数据，应额外检查数据的准确性。该检查可以由第二个操作员或通过验证的电子方式完成。 风险管理应涵盖错误或错误输入系统数据的严重性和潜在后果。	此要求对腾讯云不适用，需由受 GxP 监管的医疗健康机构采取措施确保手动输入数据的准确性。
7	数据存储	7.1 应通过物理和电子方式保护数据免受损坏。应检查存储数据的可访问性、可读性和准确性。应确保在整个保留期内访问数据。 7.2 应定期备份所有相关数据。应在验证期间检查备份数据的完整性和准确性以及恢复数据的能力，并定期进行监控。	客户对其托管于云端的数据拥有完全的控制权 ,对这些数据的安全管理负最终责任。客户需要执行相应的管理措施或采用腾讯云上提供的相关数据安全产品或功能 ,确保数据在采集、处理、存储等活动中的真实、准确、完整和可追溯。 腾讯云平台本身也采取了多项管理措施和技术手段，致力于协助客户保障云上数据的机密性、完整性和可用

欧盟药品管理局《欧盟药品生产规范》 第 4 卷 附件 11《计算机系统》			
序号	**域**	**GxP 标准要求**	**腾讯云适用性及 白皮书对应章节**
			性。针对腾讯云的数据备份服务，客户可以通过工单了解备份和验证的更多信息，具体请见 6.2 记录和数据的保护和 5.1 数据备份和恢复。
8	数据输出	8.1 应该可以获得电子存储数据的清晰打印副本。 8.2 对于支持批量放行的记录，应该可以生成纸质版本，表明自原始输入以来是否有任何数据已更改。	此要求对腾讯云不适用。客户对其托管于云端的数据拥有完全的控制权。
9	审计跟踪	根据风险评估，应考虑在系统中建立所有良好生产规范 GMP 相关更改和删除的记录（系统生成的“审计跟踪”）。 对于良好生产规范 GMP 相关数据的更改或删除，应记录原因。 审计跟踪需要保证可用性，并可转换为一般可理解的形式并定期审查。	客户需要确保系统保留了相关的日志以备审计追踪。 腾讯云建立了日志和审计管理制度，并对云产品后台运维进行日志记录并定期审计，请见 5.2 日志和审计跟踪。
10	变更和配置管理	对计算机化系统（包括系统配置）的任何更改只能按照规定的程序以受控方式进行。	客户需要确保其 GxP 系统和配置的变更具有相关控制流程和操作规范。 针对腾讯云的产品和支撑平台，腾讯云建立并实施了严格的变更和配置管理流程，并通过变更管理平台确保变更安全受控，具体请见 5.3 变更和配置管理。

欧盟药品管理局《欧盟药品生产规范》 第 4 卷 附件 11《计算机系统》			
序号	**域**	**GxP 标准要求**	**腾讯云适用性及 白皮书对应章节**
11	定期评估	应定期评估计算机化系统，以确认它们保持有效状态并符合良好生产规范 GMP。在适当的情况下，此类评估应包括当前功能范围、偏差记录、事件、问题、升级历史、性能、可靠性、安全性和验证状态报告。	客户需要定期对其计算机化系统进行评估，确认其 GxP 的合规性。 针对腾讯云所提供的 GxP 组件，腾讯云每年都会通过独立第三方审计进行系统质量和安全性审计，以确认腾讯云所提供的产品或服务保持有效状态。具体请见 4.2 质量管理审计。
12	安全	12.1 物理和/或逻辑控制应到位，以限制授权人员访问计算机化系统。 防止未经授权进入系统的合适方法可以包括使用钥匙、通行卡、带有密码的个人代码、生物特征、限制对计算机设备和数据存储区域的访问。 12.2 安全控制的程度取决于计算机系统的关键程度。 12.3 应记录访问授权的创建、更改和取消。 12.4 数据和文件的管理系统应设计用于记录操作员输入、更改、确认或删除数据的身份，包括日期和时间。	针对物理控制，如客户通过腾讯云搭建云上 GxP 系统，则底层的物理安全部分由腾讯云负责。腾讯云通过访问控制、物理环境管控、定期巡检和审计等手段，确保物理管控到位，具体请见 5.4 物理安全。 针对逻辑控制，客户需要在组织内部采取身份认证和访问控制措施，确保内部人员对 GxP 业务系统的访问受控。腾讯云通过多项身份认证和访问控制措施确保后台运维操作经过授权并保留日志供安全审计，具体请见 5.8 身份认证与访问控制。
13	事件管理	所有事件，不仅是系统故障和数据错误，都应该报告和评估。 应识别关键事件的根本原因，并应形成纠正和预防措施的基础。	客户需要建立事件管理流程，并采取相应的纠正和预防措施。 腾讯云建立了完备的事件响应流程，确保第一时间对事件作出处理，降低负面影响；如事件会影响到客户业

欧盟药品管理局《欧盟药品生产规范》 第 4 卷 附件 11《计算机系统》			
序号	**域**	**GxP 标准要求**	**腾讯云适用性及 白皮书对应章节**
			务，腾讯云会尽快同步客户并为客户提供事件处理建议，具体请见 5.9 事件响应。
14	电子签名	电子记录可以以电子方式签署。 电子签名应： a. 与公司范围内的手写签名具有相同的影响， b. 永久链接到他们各自的记录， c. 包括应用它们的时间和日期。	此要求对腾讯云不适用，需由受 GxP 监管的医疗健康机构在使用电子签名时遵守相关规定。
15	批量放行	当使用计算机系统记录认证和批量放行时，该系统应仅允许合格人员认证批量放行，并应清楚地识别和记录批量放行或批量认证的人员。这应该使用电子签名来执行。	此要求对腾讯云不适用，需由受 GxP 监管的医疗健康机构在产品批量发行时遵守相关规定。
16	业务连续性	对于支持关键流程的计算机化系统的可用性，应作出规定，以确保在系统故障（例如手动或替代系统）的情况下对这些流程的支持的连续性。 将替代安排投入使用所需的时间应基于风险并适合特定系统及其支持的业务流程。这些安排应充分记录和测试。	客户需要根据业务影响分析为 GxP 系统制定业务连续性计划并进行演练，以确保有效性。 腾讯云建立了业务连续性管理体系以及产品和服务的应急预案，并会全力配合医疗健康行业客户的业务连续性计划，具体请见 5.10 业务连续性管理。

欧盟药品管理局《欧盟药品生产规范》 第 4 卷 附件 11《计算机系统》			
序号	**域**	**GxP 标准要求**	**腾讯云适用性及 白皮书对应章节**
17	数据归档	数据可能会被存档。 应检查这些数据的可访问性、可读性和完整性。 如果要对系统（例如计算机设备或程序）进行相关更改，则应确保和测试检索数据的能力。	针对客户托管在腾讯云上的归档数据，腾讯云采取了一系列数据保护措施以协助客户确保数据的可访问性、可读性和完整性，具体请见 6. 电子记录和数据管理。

中国国家药品监督管理局《药品生产质量管理规范》附录 1《计算机化系统》			
序号	**域**	**GxP 标准要求**	**腾讯云适用性及 白皮书对应章节**
第三条	风险管理	风险管理应当贯穿计算机化系统的生命周期全过程，应当考虑患者安全、数据完整性和产品质量。作为质量风险管理的一部分，应当根据书面的风险评估结果确定验证和数据完整性控制的程度。	客户应对 GxP 系统的整个生命周期进行风险评估。 腾讯云将风险管理融入至系统的全生命周期中，具体请见 4.6 系统开发生命周期和 4.7 验证部分。
第四条	供应商管理	企业应当针对计算机化系统供应商的管理制定操作规程。供应商提供产品或服务时（如安装、配置、集成、验证、维护、数据处理等），企业应当与供应商签订正式协议，明确双方责任。企业应当基于风险评估的结果提供与供应商质量体系和审计信息相关的文件。	客户有责任对供应商的能力进行评估并和供应商签订协议，明确双方责任。 腾讯云作为云服务提供商，会配合医疗健康行业客户 GxP 的合规需要，配合客户对腾讯云的供应商评估和供应商协议制定，并为客户提供腾讯云 ISO9001 质量管理体系认证证书，具体请见 4.5 供应商管理。
第五条	人员	计算机化系统生命周期中所涉及的各种活动，如验证、使用、维护、管理等，需要各相关的职能部门人员之间的紧密合作。应当明确所有使用和管理计算机化系统人员的职责和权限，并接受相应的使用和管理培训。应当确保有适当的专业人员，对计算机化系统的设计、验证、安装和运行等方面进行培训和指导。	客户需要确保 GxP 系统的相关人员具备相关的系统、流程操作技能和资质。 腾讯云建立并实施了人员培训的相关机制，确保自身员工具有足够的资质、能力和信息安全意识，具体请见 4.4 人员管理。
第六条 至 第九条	验证	第六条　计算机化系统验证包括应用程序的验证和基础架构的确认，其范围与程度应当基于科学的风险评估。风险评估应当充分考虑计算机化系统的使用范围和用途。 应当在计算机化系统生命周期中保持其验证状态。	客户需要根据风险评估的结果确定验证的范围与程度，进行应用程序的验证和基础架构的确认，确保系统功能符合预定用途。

中国国家药品监督管理局《药品生产质量管理规范》附录 1《计算机化系统》			
序号	**域**	**GxP 标准要求**	**腾讯云适用性及 白皮书对应章节**
		第七条　企业应当建立包含药品生产质量管理过程中涉及的所有计算机化系统清单，标明与药品生产质量管理相关的功能。清单应当及时更新。 第八条　企业应当指定专人对通用的商业化计算机软件进行审核，确认其满足用户需求。 在对定制的计算机化系统进行验证时，企业应当建立相应的操作规程，确保在生命周期内评估系统的质量和性能。 第九条　数据转换格式或迁移时，应当确认数据的数值及含义没有改变。	腾讯云通过系统开发生命周期对所提供的云平台服务和产品进行质量和安全管理，并确保相关组件保持验证的状态，具体请见 4.6 系统开发生命周期 和 4.7 验证。腾讯云制定了完善的变更管理程序、规范及标准化系统变更和紧急系统变更时的操作，具体请见 5.3 变更和配置管理。
第十条	系统	系统应当安装在适当的位置，以防止外来因素干扰。	针对物理控制，如客户通过腾讯云搭建云上 GxP 系统，则底层的物理安全部分由腾讯云负责。腾讯云通过访问控制、物理环境管控、定期巡检和审计等手段，确保物理管控到位，具体请见 5.4 物理安全。
第十一条	系统	关键系统应当有详细阐述的文件（必要时，要有图纸），并须及时更新。此文件应当详细描述系统的工作原理、目的、安全措施和适用范围、计算机运行方式的主要特征，以及如何与其他系统和程序对接。	客户应该考虑为 GxP 系统制定相关的说明文档。 腾讯云的服务或产品可以通过官网找到具体的介绍文档和 API/SDK 调用方式，具体请见**腾讯云官网产品页**。
第十二条	系统	软件是计算机化系统的重要组成部分。企业应当根据风险评估的结果，对所采用软件进行分级管理（如针对软件供应商的审计），评估供应商质量保证系统，保证软件符合企业需求。	客户有责任对供应商的能力进行评估并和供应商签订协议，明确双方责任。 腾讯云作为云服务提供商，会配合医疗健康行业客户 GxP 的合规需要，配合客户对腾讯云的供应商评估和供

中国国家药品监督管理局《药品生产质量管理规范》附录 1《计算机化系统》			
序号	**域**	**GxP 标准要求**	**腾讯云适用性及 白皮书对应章节**
			应商协议制定，并为客户提供腾讯云 ISO9001 质量管理体系认证证书。具体请见 4.5 供应商管理。
第十三条	系统	在计算机化系统使用之前，应当对系统进行全面测试，并确认系统可以获得预期的结果。当计算机化系统替代某一人工系统时，可采用两个系统（人工和计算机化）平行运行的方式作为测试和验证内容的一部分。	客户需要根据风险评估的结果确定验证的范围与程度，确保系统功能符合预定用途。 腾讯云通过系统开发生命周期对所提供的云平台服务和产品进行质量和安全管理，并确保相关组件保持通过全面的质量和安全测试，具体请见 4.6 系统开发生命周期和 4.7 验证。
第十四条	系统	只有经许可的人员才能进入和使用系统。企业应当采取适当的方式杜绝未经许可的人员进入和使用系统。 应当就进入和使用系统制订授权、取消以及授权变更的操作规程。必要时，应当考虑系统能记录未经许可的人员试图访问系统的行为。对于系统自身缺陷，无法实现人员控制的，必须具有书面程序、相关记录本及相关物理隔离手段，保证只有经许可的人员方能进行操作。	客户需要采取身份认证和访问控制措施，确保其 GxP 业务系统的访问受控，防止未经授权的访问；并根据系统的重要程度设置相关日志功能。 腾讯云为客户提供了身份认证和访问控制的相关产品和工具，还通过多项身份认证和访问控制措施确保腾讯云后台运维操作经过授权并保留日志供安全审计，具体请见 5.8 身份认证与访问控制。腾讯云产品及支撑系统都需要开启日志功能，后台运维相关的登录活动和用户操作行为都由安全组件进行监控和日志记录，具体请见 5.2 日志和审计跟踪。

中国国家药品监督管理局《药品生产质量管理规范》附录 1《计算机化系统》			
序号	**域**	**GxP 标准要求**	**腾讯云适用性及 白皮书对应章节**
第十五条	系统	当人工输入关键数据时，应当复核输入记录以确保其准确性。这个复核可以由另外的操作人员完成，或采用经验证的电子方式。必要时，系统应当设置复核功能，确保数据输入的准确性和数据处理过程的正确性。	此要求对腾讯云不适用，需由受 GxP 监管的医疗健康机构采取措施确保手动输入数据的准确性。
第十六条	系统	计算机化系统应当记录输入或确认关键数据人员的身份。只有经授权人员，方可修改已输入的数据。每次修改已输入的关键数据均应当经过批准，并应当记录更改数据的理由。应当根据风险评估的结果，考虑在计算机化系统中建立数据审计跟踪系统，用于记录数据的输入和修改以及系统的使用和变更。	客户应该建立相关的记录访问控制和修改权限审批流程，并记录系统的相关日志以备审计。 腾讯云为客户提供了身份认证和访问控制措施，并对腾讯云后台运维的访问进行严格的管控，具体请见 5.8 身份认证与访问控制。腾讯云产品及支撑系统都需要开启日志功能，后台运维相关的登录活动和用户操作行为都由安全组件进行监控和日志记录，具体请见 5.2 日志和审计跟踪。
第十七条	系统	计算机化系统的变更应当根据预定的操作规程进行，操作规程应当包括评估、验证、审核、批准和实施变更等规定。计算机化系统的变更，应经过该部分计算机化系统相关责任人员的同意，变更情况应有记录。	客户需要确保其 GxP 系统和配置的变更具有相关控制流程和操作规范。 针对腾讯云的产品和支撑平台，腾讯云建立并实施了严格的变更和配置管理流程，并通过变更管理平台确保变更安全受控，具体请见 5.3 变更和配置管理。

中国国家药品监督管理局《药品生产质量管理规范》附录 1《计算机化系统》			
序号	**域**	**GxP 标准要求**	**腾讯云适用性及 白皮书对应章节**
第十八条	系统	对于电子数据和纸质打印文稿同时存在的情况，应当有文件明确规定以电子数据为主数据还是以纸质打印文稿为主数据。	此要求对腾讯云不适用，需由受 GxP 监管的医疗健康机构结合自身的需求决定并遵循相关规定。
第十九条	系统	以电子数据为主数据时，应当满足以下要求： （一）为满足质量审计的目的，存储的电子数据应当能够打印成清晰易懂的文件。 （二）必须采用物理或者电子方法保证数据的安全，以防止故意或意外的损害。日常运行维护和系统发生变更（如计算机设备或其程序）时，应当检查所存储数据的可访问性及数据完整性。 （三）应当建立数据备份与恢复的操作规程，定期对数据备份，以保护存储的数据供将来调用。备份数据应当储存在另一个单独的、安全的地点，保存时间应当至少满足本规范中关于文件、记录保存时限的要求。	客户需要采取相关的管理和技术手段保证电子数据的可用性和完整性。 腾讯云提供了相关的数据保护机制和产品，协助客户保护托管在腾讯云中的数据的完整性、可用性和机密性，具体请见 5.1 数据备份和恢复 和 6.电子记录和数据管理。
第二十条	系统	企业应当建立应急方案，以便系统出现损坏时启用。应急方案启用的及时性应当与需要使用该方案的紧急程度相关。例如，影响召回产品的相关信息应当能够及时获得。	客户需要根据业务影响分析为 GxP 系统制定业务连续性计划并进行演练，以确保有效性。 腾讯云建立了业务连续性管理体系以及产品和服务的应急预案，并会全力配合医疗健康行业客户的业务连续性计划，具体请见 5.10 业务连续性管理。

中国国家药品监督管理局《药品生产质量管理规范》附录 1《计算机化系统》			
序号	**域**	**GxP 标准要求**	**腾讯云适用性及 白皮书对应章节**
第二十一条	系统	应当建立系统出现故障或损坏时进行处理的操作规程，必要时对该操作规程的相关内容进行验证。 包括系统故障和数据错误在内的所有事故都应当被记录和评估。重大的事故应当进行彻底调查，识别其根本原因，并采取相应的纠正措施和预防措施。	客户需要建立事件管理流程，并采取相应的纠正和预防措施。 腾讯云建立了完备的事件响应流程，确保第一时间对事件作出处理，降低负面影响；如事件会影响到客户业务，腾讯云会尽快同步客户并为客户提供事件处理建议，具体请见 5.9 事件响应。
第二十二条	系统	当采用计算机化系统放行产品时，计算机化系统应当能明示和记录放行产品人员的身份。	此要求对腾讯云不适用，需由受 GxP 监管的医疗健康机构在采用计算机系统放行产品时遵守相关规定。
第二十三条	电子签名	电子数据可以采用电子签名的方式，电子签名应当遵循相应法律法规的要求。	此要求对腾讯云不适用，需由受 GxP 监管的医疗健康机构在使用电子签名时遵守相关规定。

中国国家药品监督管理局《药品记录与数据管理要求（试行）》			
序号	**域**	**GxP 标准要求**	**腾讯云适用性及 白皮书对应章节**
第四条	基本要求	记录可以根据用途，分为台账、日志、标识、流程、报告等不同类型。从事药品研制、生产、经营、使用活动，应当根据活动的需求，采用一种或多种记录类型，保证全过程信息真实、准确、完整和可追溯。记录载体可采用纸质、电子或混合等一种或多种形式。	客户需要采取相关的管理和技术手段保证电子数据的可用性和完整性。 腾讯云提供了相关的数据保护机制 ,协助客户保护托管在腾讯云中的数据的完整性、可用性和机密性，具体请见 5.1 数据备份和恢复 和 6.电子记录和数据管理。
第五条	基本要求	采用计算机（化）系统生成记录或数据的，应当采取相应的管理措施与技术手段，确保生成的信息真实、准确、完整和可追溯。	客户需要采取相关的管理和技术手段保证电子数据的可用性和完整性。 腾讯云提供了相关的数据保护机制，协助客户保护托管在腾讯云中的数据的完整性、可用性和机密性，具体请见 5.1 数据备份和恢复 和 6.电子记录和数据管理。
第六条	基本要求	电子记录至少应当实现原有纸质记录的同等功能，满足活动管理要求。 对于电子记录和纸质记录并存的情况，应当在相应的操作规程和管理制度中明确规定作为基准的形式。	此要求对腾讯云不适用，纸质记录相关的要求需由受 GxP 监管的医疗健康机构结合业务情况遵循。
第七条	基本要求	应当根据记录的用途、类型与形式，制定记录管理规程，明确记录管理责任，规范记录的控制方法。	客户需要建立数据或记录的管理规程，并明确各类型数据的管理责任与控制要求。 腾讯云已经建立了数据安全保护相关的管理流程和规范，具体请见 6.1 记录和数据的管理规程。

中国国家药品监督管理局《药品记录与数据管理要求（试行）》			
序号	**域**	**GxP 标准要求**	**腾讯云适用性及 白皮书对应章节**
第八条	基本要求	数据的采集、处理、存储、生成、检索、报告等活动，应当满足相应数据类型的记录填写或数据录入的要求，保证数据真实、准确、完整和可追溯。	客户需要建立数据或记录的管理规程，并明确各类型数据的管理责任与控制要求。 腾讯云已经建立了数据安全保护相关的管理流程和规范，具体请见 6.1 记录和数据的管理规程。
第九条	基本要求	根据数据的来源与用途，可将数据分为基础信息数据、行为活动数据、计量器具数据、电子数据及其它类型数据，不同类型的数据应当采用适当的管理措施与技术手段。	此要求对腾讯云不适用，客户需要根据其 GxP 业务数据的来源和用途进行数据分类分级并采取相应的管控措施。
第十条	基本要求	从事记录与数据管理的人员应当接受必要的培训，掌握相应的管理要求与操作技能，遵守职业道德守则。	客户需要确保 GxP 系统的相关人员具备相关的系统、流程操作技能和资质。 腾讯云建立并实施了人员培训的相关机制 ,确保自身员工具有足够的资质、能力和信息安全意识 ,具体请见 4.4 人员管理。
第十一条	基本要求	通过合同约定由第三方产生的记录与数据，应当符合本要求规定，并明确合同各方的管理责任。	客户有责任对供应商的能力进行评估并和供应商签订协议，明确双方责任。 腾讯云作为云服务提供商，会配合医疗健康行业客户 GxP 的合规需要，配合客户的协议制定事宜，具体请见 4.5 供应商管理。

中国国家药品监督管理局《药品记录与数据管理要求（试行）》			
序号	**域**	**GxP 标准要求**	**腾讯云适用性及 白皮书对应章节**
第二十条	电子记录管理要求	采用电子记录的计算机（化）系统应当满足以下设施与配置： （一）安装在适当的位置，以防止外来因素干扰； （二）支持系统正常运行的服务器或主机； （三）稳定、安全的网络环境和可靠的信息安全平台； （四）实现相关部门之间、岗位之间信息传输和数据共享的局域网络环境； （五）符合相关法律要求与管理需求的应用软件与相关数据库； （六）能够实现记录操作的终端设备及附属装置； （七）配套系统的操作手册、图纸等技术资料。	客户需要根据其采用的云服务模式，确保其 GxP 计算机化系统满足有关的主机、网络、应用程序、终端和配置的安全要求。 腾讯云通过相关管理流程和技术手段保障底层基础设施的安全可靠，具体请看 5.4 物理安全、5.5 网络安全、5.6 主机安全和 5.7 应用程序安全。
第二十一条	电子记录管理要求	采用电子记录的计算机（化）系统至少应当满足以下功能要求： （一）保证记录时间与系统时间的真实性、准确性和一致性； （二）能够显示电子记录的所有数据，生成的数据可以阅读并能够打印； （三）系统生成的数据应当定期备份，备份与恢复流程必须经过验证，数据的备份与删除应有相应记录； （四）系统变更、升级或退役，应当采取措施保证原系统数据在规定的保存期限内能够进行查阅与追溯。	客户需要确保存储在计算机化系统中的电子记录的真实性、准确性、完整性和可用性。 腾讯云依据产品的功能为客户提供数据备份服务，并严格依据变更流程管理云产品和支撑平台的变更，具体请见 5.1 数据备份和恢复、5.3 变更和配置管理。
第二十二条	电子记录管理要求	电子记录应当实现操作权限与用户登录管理，至少包括： （一）建立操作与系统管理的不同权限，业务流程负责人的用户权限应当与承担的职责相匹配，不得赋予其系统（包括操作系统、应用程序、数据库等）管理员的权限； （二）具备用户权限设置与分配功能，能够对权限修改进行跟踪与查询；	客户需要采取身份认证和访问控制措施，确保其 GxP 业务系统的访问受控，防止未经授权的访问； 腾讯云为客户提供了身份认证和访问控制的相关产品和工具，还通过多项身份认证和访问控制措施确保腾讯云后

中国国家药品监督管理局《药品记录与数据管理要求（试行）》			
序号	**域**	**GxP 标准要求**	**腾讯云适用性及 白皮书对应章节**
		（三）确保登录用户的唯一性与可追溯性，当采用电子签名时，应当符合《中华人民共和国电子签名法》的相关规定； （四）应当记录对系统操作的相关信息，至少包括操作者、操作时间、操作过程、操作原因；数据的产生、修改、删除、再处理、重新命名、转移；对计算机（化）系统的设置、配置、参数及时间戳的变更或修改。	台运维操作经过授权并保留日志供安全审计，具体请见 5.8 身份认证与访问控制。
第二十三条	电子记录管理要求	采用电子记录的计算机（化）系统验证项目应当根据系统的基础架构、系统功能与业务功能，综合系统成熟程度与复杂程度等多重因素，确定验证的范围与程度，确保系统功能符合预定用途。	客户需要根据风险评估的结果确定验证的范围与程度，确保系统功能符合预定用途。 腾讯云通过系统开发生命周期对所提供的云平台服务和产品进行质量和安全管理，并确保相关组件保持验证的状态，具体请见 4.6 系统开发生命周期 和 4.7 验证。
注：《药品记录与数据管理要求（试行）》中的对纸质记录和业务数据管理要求对腾讯云不适用，需由受 GxP 监管的医疗健康机构遵循相关的业务操作要求，在此不再更多介绍。			

美国食品和药物管理局 联邦法规法典第 21 篇			
序号	**域**	**GxP 标准要求**	**腾讯云适用性及 白皮书对应章节**
820.5	质量管理	每个制造商都应建立和维护适用于设计或制造的特定医疗器械并满足本部分要求的质量体系。	客户应建立并维护自身的质量管理体系。 腾讯云基于国际标准建立了质量管理体系并通过了国际权威第三方的认证，具体请见 4.1 质量管理体系和 4.2 质量管理审计。
820.20	质量管理	(a) 质量政策。 负有执行责任的管理层应建立其质量方针和目标，以及对质量的承诺。 负有执行责任的管理层应确保质量方针在组织的各个层面得到理解、实施和维护。 (b) 组织。每个制造商应建立并保持适当的组织结构，以确保设备的设计和生产符合本部分的要求。 (1) 责任和权限。每个制造商应为管理、执行和评估影响质量的工作的所有人员建立适当的职责、权限和相互关系，并提供执行这些任务所需的独立性和权限。 (2) 资源。每个制造商应为管理、工作绩效和评估活动（包括内部质量审核）提供足够的资源，包括指派受过培训的人员，以满足本部分的要求。 (3) 管理代表。负有行政责任的管理层应任命并记录任命一名管理层成员，无论其他职责如何，该成员应具有对以下方面的权力和责任： (i) 确保按照本部分有效建立和有效维护质量体系要求；和 (ii) 向负有执行审查责任的管理层报告质量体系的绩效。 (c) 管理审查。 负有执行责任的管理层应按照既定程序以规定的时间间隔和足够的频率审查质量体系的适用性和有效性，以确保质量体系满足本部分的要求和制造商既定的质量方针和目标。 质量体系评审的日期和结果应形成文件。	客户应建立并维护自身的质量管理体系。 腾讯云基于国际标准建立了质量管理体系并通过了权威第三方的认证，具体请见 4.1 质量管理体系 和 4.2 质量管理审计。

美国食品和药物管理局 联邦法规法典第 21 篇			
序号	**域**	**GxP 标准要求**	**腾讯云适用性及 白皮书对应章节**
		(d) 质量规划。 每个制造商都应制定质量计划，定义与设计和制造的器械相关的质量实践、资源和活动。 制造商应确定如何满足质量要求。 (e) 质量体系程序。 每个制造商应建立质量体系程序和说明。 适当时应建立质量体系中使用的文件结构大纲。	
820.22	质量审核	每个制造商应建立质量审核程序并进行此类审核，以确保质量体系符合既定的质量体系要求并确定质量体系的有效性。质量审核应由对被审核事项不直接负责的个人进行。必要时应采取纠正措施，包括重新审核有缺陷的事项。应就每次质量审核和重新审核的结果作出报告，并由负责审核事项的管理层审查此类报告。质量审核和再审核的日期和结果应形成文件。	客户应建立并维护自身的质量管理体系 ,并对体系进行审核。 腾讯云基于国际标准建立了质量管理体系并通过了权威第三方的认证 ,具体请见 4.1 质量管理体系 和 4.2 质量管理审计。
820.25	人员	(a) 一般。 每个制造商都应有足够的人员具有必要的教育、背景、培训和经验，以确保正确执行本部分要求的所有活动。 (b) 培训。 每个制造商应建立确定培训需求的程序，并确保所有人员都经过培训以充分履行其指定的职责。 培训应形成文件。 (1) 作为培训的一部分 ,应使员工了解可能因不当执行特定工作而导致的设备缺陷。 (2) 执行验证和确认活动的人员应了解在其工作职能中可能遇到的缺陷和错误。	客户需要确保 GxP 系统的相关人员具备相关的系统、流程操作技能和资质。 腾讯云建立并实施了人员培训的相关机制，确保自身员工具有足够的资质、能力和信息安全意识，具体请见 4.4 人员管理。

美国食品和药物管理局 联邦法规法典第 21 篇			
序号	**域**	**GxP 标准要求**	**腾讯云适用性及 白皮书对应章节**
820.40	文档管理	每个制造商应建立和维护程序来控制本部分要求的所有文件。程序应规定以下内容： (a) 文件批准和分发。每个制造商应指定一个或多个人来审查充分性并在发布所有为满足本部分要求而建立的文件之前批准。批准，包括批准文件的个人的日期和签名，应记录在案。为满足本部分要求而建立的文件应在指定、使用或其他必要的所有位置可用，所有过时的文件应立即从所有使用点移除或以其他方式防止意外使用。 (b) 文件更改。除非另有特别指定，否则文件的更改应由执行原始审查和批准的同一职能或组织中的个人审查和批准。批准的变更应及时传达给适当的人员。每个制造商应保存文件更改的记录。变更记录应包括变更说明、受影响文件的标识、批准人的签名、批准日期以及变更生效的时间。	客户需要建立文档管理程序，对业务的标准操作流程（SOP）和系统操作和维护相关的程序进行规范管理，确保文档的准确性和有效性。 腾讯云建立了文档管理程序，覆盖文档的编制、审批、发布、保管、使用、修订、保留和作废等阶段，并通过电子文档管理平台以对腾讯云各个管理体系的文档进行统一的管理，具体请见 4.3 文档管理。
820.50	供应商控制	每个制造商应建立和维护程序，以确保所有购买或以其他方式收到的产品和服务符合规定的要求。 (a) 对供应商、承包商和顾问的评估。 每个制造商应建立并保持供应商、承包商和顾问必须满足的要求，包括质量要求。 每个制造商应： (1) 根据潜在供应商、承包商和顾问满足特定要求（包括质量要求）的能力来评估和选择他们。 评估应形成文件。 (2) 根据评估结果，确定对产品、服务、供应商、承包商和顾问实施控制的类型和程度。 (3) 建立和维护可接受的供应商、承包商和顾问的记录。	客户有责任对供应商的能力进行评估并和供应商签订协议，明确双方责任。 腾讯云作为云服务提供商，会配合医疗健康行业客户 GxP 的合规需要，配合客户对腾讯云的供应商评估和供应商协议制定，并为客户提供腾讯云 ISO9001 质量管理体系认证证书。具体请见 4.5 供应商管理。

美国食品和药物管理局 联邦法规法典第 21 篇			
序号	**域**	**GxP 标准要求**	**腾讯云适用性及 白皮书对应章节**
		(b) 采购数据。 每个制造商应建立和维护清楚地描述或引用特定要求的数据，包括质量要求，用于购买或以其他方式接收的产品和服务。 在可能的情况下，采购文件应包括供应商、承包商和顾问同意将产品或服务的变化通知制造商的协议，以便制造商可以确定这些变化是否会影响成品设备的质量。 采购数据应根据 820.40 进行批准。	
注：Part 820 中的其他要求对腾讯云不适用，需由受 GxP 监管的医疗健康机构遵循相关的业务操作要求，在此不再更多介绍。			
11.10 (a)	电子记录；电子签名-对于封闭系统的控制	验证系统以确保准确性、可靠性、一致的预期性能以及识别无效或更改记录的能力。	客户需要根据风险评估的结果确定验证的范围与程度，确保系统功能符合预定用途。 腾讯云通过系统开发生命周期对所提供的云平台服务和产品进行质量和安全管理，并确保相关组件保持验证的状态，具体请见 4.6 系统开发生命周期 和 4.7 验证。
11.10 (b)	电子记录；电子签名-对于封闭系统的控制	能够以适合机构检查、审查和复制的人类可读和电子形式生成准确和完整的记录副本。 如果对机构对电子记录进行此类审查和复制的能力有任何疑问，应联系该机构。	客户需要采取相关的管理和技术手段保证电子数据的可用性和完整性。 腾讯云提供了一系列数据保护机制和产品，赋能客户保护其数据的完整性、可用性和机密性，具体请见 5.1 数据备份和恢复 和 6.电子记录和数据的要求。

美国食品和药物管理局 联邦法规法典第 21 篇			
序号	**域**	**GxP 标准要求**	**腾讯云适用性及 白皮书对应章节**
11.10 (c)	电子记录；电子签名-对于封闭系统的控制	保护记录，使其在整个记录保留期内能够准确和方便地检索。	客户需要采取相关的管理和技术手段保证电子数据的可用性和完整性。 腾讯云提供了一系列数据保护机制和产品，赋能客户保护其数据的完整性、可用性和机密性，具体请见 5.1 数据备份和恢复 和 6. 电子记录和数据的管理。
11.10 (d)	电子记录；电子签名-对于封闭系统的控制	限制授权个人访问系统。	客户需要采取身份认证和访问控制措施，确保其 GxP 业务系统的访问受控，防止未经授权的访问； 腾讯云为客户提供了身份认证和访问控制的相关产品和工具 ,还通过多项身份认证和访问控制措施确保腾讯云后台运维操作经过授权并保留日志供安全审计，具体请见 5.8 身份与访问控制。
11.10 (e)	电子记录；电子签名-对于封闭系统的控制	使用安全的、计算机生成的、带有时间戳的审计跟踪来独立记录操作员输入的日期和时间以及创建、修改或删除电子记录的操作。 记录更改不得掩盖以前记录的信息。 此类审计跟踪文件应至少保留与主题电子记录所需的时间一样长的时间，并应可供机构审查和复制。	客户需要确保系统保留了相关的日志以备审计追踪。 腾讯云建立了日志管理制度 ,并对云产品后台运维的操作进行日志记录并定期审计，请见 5.2 日志和审计跟踪。
11.10 (f)	电子记录；电子签名-对于封闭系统的控制	酌情使用操作系统检查来强制执行允许的步骤和事件顺序。	此要求对腾讯云不适用，需由受 GxP 监管的医疗健康机构遵守相关规定。

美国食品和药物管理局 联邦法规法典第 21 篇			
序号	**域**	**GxP 标准要求**	**腾讯云适用性及 白皮书对应章节**
11.10 (g)	电子记录；电子签名-对于封闭系统的控制	使用权限检查以确保只有经过授权的个人才能使用系统、对记录进行电子签名、访问操作或计算机系统输入或输出设备、更改记录或执行手头的操作。	客户需要采取身份认证和访问控制措施，确保其 GxP 业务系统的访问受控，防止未经授权的访问； 腾讯云为客户提供了身份认证和访问控制措施，并对腾讯云后台运维的访问进行严格的管控，具体请见 5.8 身份认证与访问控制。
11.10 (h)	电子记录；电子签名-对于封闭系统的控制	使用设备（例如终端）检查以确定数据输入或操作指令来源的有效性。	此要求对腾讯云不适用，需由受 GxP 监管的医疗健康机构遵守相关规定。
11.10 (i)	电子记录；电子签名-对于封闭系统的控制	确定开发、维护或使用电子记录/电子签名系统的人员具有执行指定任务的教育、培训和经验。	客户需要确保 GxP 系统的相关人员具备相关的系统、流程操作技能和资质。 腾讯云建立并实施了人员培训的相关机制，确保自身员工具有足够的资质、能力和信息安全意识，具体请见 4.4 人员管理。
11.10 (j)	电子记录；电子签名-对于封闭系统的控制	制定并遵守书面政策，要求个人对其电子签名下发起的行为负责，以阻止记录和签名伪造。	此要求对腾讯云不适用，需由受 GxP 监管的医疗健康机构在使用电子签名时遵守相关规定。

美国食品和药物管理局 联邦法规法典第 21 篇			
序号	**域**	**GxP 标准要求**	**腾讯云适用性及 白皮书对应章节**
11.10 (k)	电子记录；电子签名-对于封闭系统的控制	对系统文件使用适当的控制，包括： (1) 对系统操作和维护文档的分发、访问和使用进行充分控制。 (2) 修订和变更控制程序，以维护记录系统文档的时间顺序开发和修改的审计跟踪。	客户需要建立文档管理程序，对业务的标准操作流程（SOP）和系统操作和维护相关的程序进行规范管理，确保文档的准确性和有效性。 腾讯云建立了文档管理程序，覆盖文档的编制、审批、发布、保管、使用、修订、保留和作废等阶段，并通过电子文档管理平台以对腾讯云各个管理体系的文档进行统一的管理，具体请见 4.3 文档管理。
11.30	电子记录；电子签名-对于开放系统的控制	使用开放系统创建、修改、维护或传输电子记录的人员应采用旨在确保电子记录从创建到其发送点的真实性、完整性以及适当情况下的机密性的程序和控制。此类程序和控制应酌情包括第 11.10 节中确定的程序和控制，以及其他措施，例如文件加密和使用适当的数字签名标准，以确保在必要时根据情况记录真实性、完整性和机密性。	客户需要采取相关的管理和技术手段保证电子数据的可用性和完整性。 腾讯云提供了一系列数据保护机制和产品，赋能客户保护其数据的完整性、可用性和机密性，具体请见 5.1 数据备份和恢复 和 6.电子记录和数据的管理。
注：Part 11.50-11.300 要求对腾讯云不适用，需由受 GxP 监管的医疗健康机构在使用电子签名时遵守相关规定，在此不再更多介绍。			
211.68 (b)	自动、机械和电子设备	应对计算机或相关系统实施适当的控制，以确保主生产和控制记录或其他记录的更改仅由授权人员进行。应检查计算机或相关系统的公式或其他记录或数据的输入和输出的准确性。输入/输出验证的程度和频率应基于计算机或相关系统的复杂性和可靠性。应保留输入计算机或相关系统的数据备份文件，除非某些数据（例如与实验室分析相关的计算）通过计算机化或其他自动化过程消除。在这种情况下，程序的书面记录应与适当的验证数据一起保存。硬拷贝或替代系统，	客户需要采取相关的管理和技术手段保证电子数据的可用性和完整性。 腾讯云提供了一系列数据保护机制和产品 赋能客户保护其数据的完整性、可用性和机密性，具体请见 5.1 数据备份和恢复 和 6.电子记录和数据的管理。

美国食品和药物管理局 联邦法规法典第 21 篇			
序号	**域**	**GxP 标准要求**	**腾讯云适用性及 白皮书对应章节**
		例如副本、磁带或缩微胶卷，旨在确保备份数据准确和完整，并确保其不会被更改、无意擦除或丢失。	
注：Part 211 中的其他要求对腾讯云不适用，需由受 GxP 监管的医疗健康机构遵循相关的业务操作要求，在此不再更多介绍。			