MEDIDATA

白皮书

信息安全

目录

执行摘要 4

目的 5

Medidata 安全文化 5

企业风险管理 6

信息安全框架和审计 7

保护和确保边界安全 7

身份提供商和服务（Identity Provider and Services, IdP IpS） 7

识别、认证和授权 8

网络安全和信息安全意识培训 8

审计或监测 8

SIEM 8

配置管理 8

业务连续性和灾难恢复(BC/DR) 9

事件响应和处理 9

维护 9

媒体保护 9

数据丢失预防 10

环境安全 10

安全规划 10

人事安全 - 人力资本 10

产品和服务资格认证 11

系统和信息完整性 11

第三方风险管理(Third Party Risk Management, TPRM) 11

供应商评估和审计 11

反病毒和反恶意软件保护 12

数据加密 12

传输中的数据加密 12

静态加密 12

系统加固标准 12

远程连接 12

隐私计划 13

设计隐私保护 13

安全设计 14

安全编码标准 14

软件开发生命周期 14

漏洞识别和管理 14

应用程序安全漏洞评估 14

网络安全漏洞评估（渗透测试） 15

独立测试和审查 15

ISO/IEC27001 16

ISO/IEC27701 16

ISO/IEC27017 16

ISO/IEC27018 16

FISMA 中等级别 17

欧盟-美国数据隐私框架（DPF）及相关框架 17

FIPS 140-2 17

健康保险便利与责任法案（HIPAA） 17

关闭 18

免责声明 18

执行摘要

Medidata 认识到，有效的信息安全和网络防御计划必须针对整个产品生命周期，包括产品及其任何相关数据的设计、开发、生产、分销、部署、维护和处置。

Medidata 已实施行政、技术和物理保障措施，以帮助防范涉及所有 Medidata 产品的安全事件和隐私泄露，但这些产品必须按照 Medidata 的使用说明使用。然而，随着系统和威胁的不断发展，任何系统都无法防范所有威胁和漏洞。前瞻性战略和持续评估是健全国防计划的关键组成部分。我们的客户非常重要，我们与您携手合作，共同维护我们管理的所有数据和服务的安全与隐私保护措施。

请随时向我们表达您的顾虑，我们将会对您的每一项担忧进行调查。在适当的情况下，我们将通过产品变更、技术公告和/或向客户和监管机构进行负责任的披露来解决该问题。Medidata 在整个产品生命周期中不断努力提高安全性和隐私性，采用的做法包括：设计时考虑隐私和安全、产品和供应商风险评估、漏洞和补丁管理、自动化漏洞扫描、外部第三方测试、与客户访问和数据相适应的访问控制，以及事件响应。

“信息安全对保护患者隐私至关重要，在某些情况下甚至关系到患者的生命；当我成为一名临床试验的患者时，我的医疗数据保护变得与个人息息相关。我可以告诉你们，作为一名试验患者和了解网络威胁的安全专业人士，Medidata 是我唯一希望存储和处理我的信息的公司。”

- Glenn Watt，Medidata，首席信息安全官（2007-2018）

Medidata 公司致力于为客户服务，并鼓励受众与我们联系，提出问题、疑虑以及改进我们的产品和服务。

如有任何疑问或澄清，请随时联系 **Medidata.asksecurity@3ds.com**

目的

本文件旨在讨论有关 Medidata 安全和隐私惯例如何应用于 Medidata Clinical Cloud (MCC) 的公开信息。它包含说明 Medidata 如何维护我们产品每个领域的安全性，以及我们如何与您合作以确保整个产品生命周期的安全性。

我们希望在不泄露机密或专有安全产品名称、配置和操作程序的前提下，向您提供关于Medidata 安全议题的广泛讨论与专业解答。本文件的任何部分都不应被视为履行合同义务，因为这些做法和技术可能会更新，恕不另行通知。

对于更详细、更机密的查询，请咨询您的 Medidata 联系人/销售工程师/专业服务人员/客户经理以获取相关信息。

Medidata 安全文化

我们的价值观是组织中每个人都认同的，它决定了人们如何看待和处理安全问题。建立一个健全的安全文化能够培养出具有安全意识的员工队伍，并促进员工展现所需的安全行为。这就是所谓的“人体防火墙”。无论是 Medidata 还是合作伙伴的员工，都能“识别”出什么是不寻常的，什么是可疑的。个人经验和观察无法自动化。这就是我们购买和部署工具的极限。

Medidata 以“安全设计”的理念开发产品。开放式全球应用程序安全项目（Open Worldwide Application Security Project, OWASP）软件开发原则为我们的软件开发生命周期（Software Development Life Cycle, SDLC）以及企业技术架构的设计和修改奠定了核心策略。

OWASP 安全设计原则是：

- **最小化攻击表面积** - 仅向用户提供其所需的功能
- **建立安全默认设置** - 管理用户及其访问权限的强大安全规则
- **最小权限原则** - 用户应拥有执行特定任务所需的最小权限集
- **深度防御** - 产品必须具备多层验证、额外的安全审计工具和日志记录功能
- **安全失败** - 故障程序应默认为更少或无访问权限
- **不要相信服务** - 程序中使用的第三方软件和服务不应被赋予更高级别的权限，数据流必须经过验证
- **职责分离** - 防止个人欺诈行为
- **避免隐晦式安全** - 在不隐藏核心功能或源代码的情况下，使用足够的安全控制来保证应用程序的安全
- **保持安全简单** - 尽可能减少复杂性，保持代码可见性
- **正确修复安全问题** - 必须对缺陷进行根源分析，然后采取行动

信息安全也是 Medidata 企业文化的一部分。Medidata 建立信息安全治理的战略包括维护客户数据的机密性、完整性和可用性，最大限度地降低勒索软件或数据泄露等恶意事件对业务造成损害的可能性。

Medidata 的治理策略是通过结合行业领先的培训和教育，以及由多样化的、经验丰富的、经过认证的安全专业人员团队支持实施的。该团队围绕专业能力组织，包括安全运营、安全工程、安全架构、事件响应、身份和访问管理、风险管理以及安全框架等方面。Medidata 的安全管理实施情况至少每年接受一次测试和审计，以确保 Medidata 始终遵守所有适当的安全和隐私要求。

企业风险管理

Medidata 的执行委员会 (Executive Committee, XCOM) 认识到，他们对客户的责任需要一个强有力的控制结构。因此，承诺帮助确保有效的安全控制已成为 Medidata 公司整体风险管理战略不可分割的一部分。

在首席信息安全官的监督下，这一流程利用战略监督的成果来建立战略风险登记册。该风险登记册包含了安全要求和控制措施的高层视图，以及运营中识别的威胁和新出现的全球网络安全威胁。

这些风险及其应对措施是我们向 Dassault Systèmes 董事会提交的最新报告的一部分。因为这是本组织的一项战略计划，我们将继续得到自上而下的支持。

具有前瞻性思维的组织知道，风险与每个人都息息相关。它不能被局限在单一业务线中，也不能在运营的孤立领域内临时性地执行。风险所有权必须在企业内部共享，并且需要深度合作和透明化。鉴于当前全球市场的动荡和过去几年的惨痛教训，Medidata 深知这一点，所有这些都极大地扰乱了我们的经济、商业和社会生态系统。

在一个理想的世界中，实时信息的流动将有效管理和缓解各类干扰与风险（涵盖网络、业务、运营及声誉等方面）变得可能，这些信息将顺畅地进入公司，并在一群界定清晰、利益相关的参与者之间进行共享。这些参与者将协同工作，拥有做出迅速且充分了解情况的决策的权力。

Medidata 致力于达成这一理想境界。若我们期望在这个不断变化、日新月异的世界中取得成功，并应对由此衍生的日益增长的威胁，那么在座的每一位都应当为实现这一目标而共同努力。

Medidata 的成功建立在构建积极主动的综合安全和风险管理解决方案的基础上，这些解决方案利用必要的系统和流程，在潜在风险事件发生时实时检测到它们。

信息安全框架和审计

Medidata 实施了多个认证的安全框架、安全控制和安全方法，包括 ISO 27001、27002、27701、27017 和 27018、SOC1& SOC2+ 和 NIST 800-53v5，并遵守《通用数据保护条例》（General Data Protection Regulation, GDPR）和其他地方法规。我们还获得了美国联邦客户的 FISMA MODERATE 运营授权。外部审计由经认证的第三方执行，每年针对 ISO、FISMA 和 SOC2+ 进行一次，涵盖与提供和支持产品、软件或服务的 Medidata 人员、流程和技术相关的细节。

每次认证审计都向我们现有的和潜在的客户保证，Medidata 公司遵守地区、国家/地区和国际法律法规。每项审计都由外部审计人员进行，任何发现或不合规情况都会在 Medidata 票单系统中进行跟踪。这些票单包含根本原因的详细信息，并需要定期更新，说明解决问题所需的努力。每月向信息安全领导层提交一份报告，供其审查并在必要时上报。

Medidata 根据这些安全框架规定的要求，采用“同类最佳”的混合解决方案（组织和技术）。这种整体方法支持全面实施符合所有既定要求的安全控制和机制。

保护和确保边界安全

Medidata 实施访问控制的目的是确保对所有账户进行持续管理，并根据指定用户的角色和职责，限制和尽量减少特权和非特权账户的访问权限。访问管理要求用于提供添加/删除/更改所有账户访问权限的说明，确定控制系统以确保限制访问权限得到执行，并确定审查所有已授予访问权限的频率。持续使用各种自动化工具来执行账户管理，包括在需要时自动禁用账户，以及审计所有账户管理活动（账户创建、修改、启用、禁用和删除）。

预先批准的互联用于确保根据既定的服务水平协议在系统内执行信息流。Medidata 要求至少有两名管理员协调账户处理活动，而且所有请求均由一个票单系统管理。账户由身份访问管理团队审查，每季度一次。根据 CIS 基准建立的指导原则，限制失败的登录尝试并执行锁定后自动恢复的机制。未经识别和验证，用户或设备不得进行任何操作。所有连接均通过 MFA 和加密实现远程访问。所有账户访问都通过安全事件和事故管理器以及网关保护方法进行监控。

身份提供商和服务（Identity Provider and Services, IdP IpS）

Medidata 使用身份提供商（简称 IdP 或 IDP）进行 Medidata 系统访问，该身份提供商负责创建、维护和管理委托人的身份信息，并为联盟或分布式网络中的依赖应用提供身份验证服务。

我们将用户身份验证作为一项服务，通过使用可信的 IDP 来管理对应用程序的访问。身份提供商是一个值得信赖的提供商，可让您使用单点登录（single sign-on, SSO）访问其他网站，通过减少密码疲劳提高可用性，并通过减少潜在攻击面提供更好的安全性。

身份提供商可以促进云计算资源和用户之间的连接，从而减少用户在使用移动和漫游应用时重新认证的需要。

通过遵守 CIS 基准配置设置和应用各种主机和网关访问限制来实现最低权限功能。

识别、认证和授权

Medidata 实施的识别和认证方法符合 ISO 和 NIST 规定的要求。所有用户，包括 Medidata 员工和客户用户，都使用唯一的 ID 进行身份验证。用户账户和密码必须针对特定用户，不允许共享凭证。Medidata 还对所有员工实施多因素身份验证，并为客户提供可选的多因素身份验证。

MCC 提供访问和授权控件、全面的审计跟踪以及一个电子签名系统，将电子签名与电子记录关联，确立不可否认性。Medidata 要求其客户和员工在激活用户账户以及管理和支持操作时，签署对这些要求的理解。

网络安全和信息安全意识培训

Medidata 实施网络安全培训的目的是确保包括承包商在内的所有员工都能接受与其职位和安全责任相适应的培训。

Medidata 公司采用了多个有针对性的培训模块。对年度培训进行跟踪，未完成课程的员工或承包商将被取消访问所有 Medidata 系统的权限。永久复职需要完成培训并获得经理批准。

培训通过 Medidata 学习管理系统的电子学习培训课程进行管理，3DS 学习管理系统还提供其他按需课程。

审计或监测

Medidata 实施安全事件审计的目的是确保捕获所有必要的可审计事件，并符合 ISO 27001 系列和 NIST 800-53 的要求。Medidata 使用各种 SIEM 工具，根据这些要求进行监控和审计，包括对安全漏洞、入侵尝试、完整性事件、系统和组件故障以及用户活动事件进行审计。对所有可审计事件进行持续监控。

SIEM

在整个环境中实施安全信息和事件管理（Security Information and Event Management, SIEM）功能。整个系统采用符合 FIPS 140-2 标准的加密方法和解决方案。

配置管理

Medidata 利用各种配置变更管理工具、流程和程序，在所有系统和组件的整个生命周期内实施配置管理。基线配置保存在由自动工具支持的验证包中。所有更改都会得到系统跟踪。测试和验证是配置管理流程不可分割的一部分。安全和隐私代表是变更审查委员会 (Change Review Board, CRB) 的成员，并在适当时提供安全和隐私风险评估。

业务连续性和灾难恢复(BC/DR)

Medidata 在整个组织内实施全面的业务连续性和灾难恢复 (Business Continuity and Disaster Recovery, BC/DR) 能力。

规划过程不仅受 Medidata 自身需求的驱动，也受客户在 SLA 中提出的要求的驱动。Medidata 的所有关键人员和组织都参与灾难恢复计划的年度演练和审查，包括我们的服务交付、客户成功和专业服务团队。我们的规划流程包括在客户 SLA 规定的恢复时间目标内恢复所有任务和业务功能。在这一规划过程中，所有关键系统资产以及所有任务和业务功能都会被确定。由此产生的计划至少每年测试一次，并利用反馈和测试结果不断提高我们的能力。

事件响应和处理

Medidata 拥有一套全面的事件响应计划，能够有效地快速识别、控制并修复对系统和数据机密性、完整性及可用性构成的直接威胁。

Medidata 拥有一支专门的全天候安全运营团队，即全球网络运营中心 (Global Network Operations Center, G-NOC)，负责监控和支持所有事件处理活动。Medidata 的安全运营团队使用各种自动化事件管理工具，包括 SIEM 以及各种日志、事件管理和报告工具。信息安全警报由我们的安全运营中心 (Security Operations Center, SOC) 或全球网络运营中心 (GNOC) 系统上报给信息安全人员，然后再上报给研发副总裁（信息安全）和高级管理层。我们的事件响应框架详细说明了触发客户警报的情况以及如何通知客户。该政策还提到了控制安全事件生命周期的应对措施。该计划描述了从事件或事故的识别、准备和遏制，到恢复、通知和事后分析的各个阶段以及与这些阶段相关的行动。在检测后的合理时限内，Medidata 将确认安全事件并进行影响分析，并通过服务协议中规定的沟通渠道通知 Medidata 客户。所有问题都在一个在线数据库驱动的问题管理系统中进行跟踪。Medidata 将事件响应培训和测试纳入其年度灾难恢复测试。

维护

Medidata 实施严格的维护计划，包括对所有更改进行优先排序和审批要求，总体目标是确保所有安全保护措施保持完好。实施漏洞扫描、应用程序扫描和恶意软件保护措施，以检查维护活动中使用的所有媒体。外部设备未经扫描不得连接，而且只能在运行人员的控制下连接。作为变更管理流程的一部分，所有维护工作都要记录在案并获得授权，其中包括回退计划以及测试和验证要求。

媒体保护

Medidata 在处理或存储数据的每个地点实施媒体保护。所有数据都被视为限制访问的数据，由我们的业务人员进行访问管理。这包括以销毁、删除、备份和恢复数据为目的的访问。对所有指定销毁的媒体进行跟踪，并为每个销毁的媒体出具销毁证书。媒体绝不会在 Medidata 之外重复使用。所有使用中、传输中或存储中的媒体都使用符合 FIPS 140-2 标准的加密方法进行保护，以确保数据的完整性和保密性。

数据丢失预防

在 Medidata，数据丢失防护（Data Loss Prevention, DLP）是一套工具和流程，用于确保敏感数据不丢失、不被滥用或不被未经授权的用户访问。DLP 软件对受监管的机密数据和关键业务数据进行分类，并识别违反组织定义的政策或预定义政策包的行为，这些政策通常由 HIPAA 或 GDPR 等监管合规性驱动。一旦发现这些违规行为，DLP 就会通过警报、加密和其他保护措施进行补救，防止最终用户意外或恶意共享可能给组织带来风险的数据。数据丢失防护软件和工具可监控端点活动，过滤企业网络上的数据流，并监控云中的数据，以保护静态、动态和使用中的数据。DLP 还提供报告功能，以满足合规性和审计要求，并识别弱点和异常情况，以便进行取证分析和事故响应。

环境安全

对设施和受保护信息资产的物理访问仅限于授权人员。Medidata 维护了一份当前的授权人员名单，这些人员有权访问包含信息系统的设施，并发放相应的授权凭证（例如，胸牌、身份证、智能卡）。组织内的指定官员至少每年审查和批准一次访问列表和授权凭证。

在设计上，任何区域都不对公众开放。物理访问名单由建筑物管理员维护，但会由设施安全团队定期审查。要访问数据中心，必须按正确顺序将生物识别、智能卡和 PIN 码结合起来。对于访问名单的增加必须经过高级管理层的批准，然后才能提供无陪同进入权限。

Medidata 监控信息系统的物理访问，以检测和应对发生的物理安全事件。物理访问会被自动记录并可供查看。摄像头用于记录实际进出情况。

Medidata 通过在授权访问设施之前对访客进行身份验证，来控制对信息系统的实际访问。访客访问前须先提出访问申请，并经 Medidata 相关人员批准。所有访客都有专人陪同进入设施。

Medidata 公司制定了正式的信息安全政策，并将有关安全区域和设备实体安全的程序记录在案。

安全规划

Medidata 以 ISO 27001 为基础，实施持续的安全计划改进流程。Medidata Clinical Cloud 实施了 ISO 27001 认证的信息安全管理系统以及符合 NIST 标准的系统安全计划。 这些计划每年更新一次，以纳入新的和不断变化的安全和隐私架构要求，并确保 Medidata 强大的安全能力。这种方法可确保将所有安全和隐私架构变更纳入安全计划、鉴定文件、工程文件、产品文件和托管文件。

人事安全 - 人力资本

根据员工行为标准聘用员工，并考虑与背景筛选程序相关的背景调查的结果。所有人员在访问 Medidata 系统之前都必须阅读、确认并遵守《商业行为准则》。Medidata 的学习管理系统会记录完成情况。这些人员安全程序也适用于第三方承包商和顾问。

产品和服务资格认证

Medidata 实施了一项全面的采购流程，该流程每年都会进行规划、记录和审批，同时也会考虑到安全和隐私的需求。这包括为渗透测试提供资金、FISMA 评估、ISO 审计、SOC2 审计、欧盟-美国数据保护框架（Data Protection Framework, DPF）认证以及其他与安全相关的活动。在规划中，也包括为整合新的安全与隐私特性至系统软件所需的加密产品和软件配置相应的资金支持。信息安全和隐私团队参与采购过程，以确保采购过程中包含所有安全和隐私要求。

系统和信息完整性

Medidata 通过使用自动化工具、单系统、补丁管理系统和质量保证流程，在整个组织中实施系统和信息完整性保障，以监控、扫描和修正 Medidata 系统整个生命周期内发现的问题。恶意代码保护在企业范围内应用时，对其进行集中监控和管理。整个环境都采用完整性监控工具，以确保 Medidata 系统的完整性。Medidata 系统内的信息在静态和传输过程中都经过加密。此外，Medidata 还持续监测国家脆弱性数据库。

第三方风险管理(Third Party Risk Management, TPRM)

Medidata 使用第三方和次级服务提供商，作为提供服务的一部分，这些第三方和次级服务提供商可代表 Medidata 访问和处理数据，偶尔包括个人信息（Personally Identifiable Information, PII）。

Medidata 隐私办公室（Medidata Privacy Office, MPO）与业务领域、主题专家和控制职能部门合作制定合同，其中包括概述参与处理参与者个人信息的第三方必须做出的隐私承诺的条款。MPO 和法律团队负责审查和批准新的第三方合同，以确认其中包含符合 Medidata 标准的隐私条款。

全球合规与战略部（Global Compliance & Strategy, GCS）与 MPO、信息安全部（Information Security, InfoSec）和业务部门合作，确保所有新供应商都要接受对访问 Medidata 系统和环境的第三方供应商进行的风险评估。Medidata 公司定期对第三方供应商进行风险评估，重点是那些访问、使用和/或存储参保者个人信息（PII）的供应商，并对评估结果进行分析，如有必要，还将进行风险评估、制定成文计划，以评估因风险评估而被视为高风险的第三方供应商。供应商评估按照规定的 Medidata 供应商评估政策和程序进行。供应商评估结果记录在案。

供应商评估和审计

所有建议用于支持 Medidata SDLC 或向 Medidata、Medidata 客户或 Medidata 合作伙伴提供服务的第三方供应商，均应接受 Medidata 人员的安全评估。Medidata 对供应商进行初始评估和定期评估，以确保基本的运营安全指标符合 Medidata 的要求。定期对供应商进行评估：关键供应商在上次评估后的 12 个月内进行评估；主要供应商在上次评估后的 12-24 个月内进行评估；次要供应商在上次评估后的 24-36 个月内进行评估。

无论审计和/或问卷调查的频率如何，供应商审计和/或问卷调查可能会因有关供应商的突发事件而安排。在供应商状态/日程表中保存供应商审计信息，包括公布日期、审计日期和完成日期。

反病毒和反恶意软件保护

除了入侵检测系统（Intrusion Detection System, IDS）和防火墙之外，Medidata 还使用一系列扫描工具，在数据中心网络穿越之前对所有数据进行进一步净化。这些扫描工具会在发生恶意事件时通知我们。通过我们的防御系统，并可能试图访问我们的系统。Medidata的网络安全理念遵循一条古老的格言：“预防胜于治疗，一盎司的预防比一磅的治疗更为重要。”在这种情况下，恶意软件扫描就是一种预防措施。已安装端点安全软件所有生产和验证系统，包括反恶意软件、端点检测和响应。服务器防火墙、日志检查和入侵检测与防御模块。

数据加密

包括 PHI 和 PII 在内的所有数据均采用最新的高级加密标准算法（Advanced Encryption Standard, AES-256）加密存储和传输，并定期进行可恢复性测试。

传输中的数据加密

系统使用传输层安全 TLS v.1.2 对传输中的数据进行加密。TLS v.1.2 允许客户端计算机与服务器建立可公开访问的连接，但只有客户端和服务器能够解密或以可解释和可用的形式查看传输的信息。TLS 1.3 已成为技术主流。

静态加密

加密在存储单元级别启用，并通过硬件受到影响。对于 Rave EDC 数据存储，PureStorage 存储区域网络使用专有密钥管理系统，使用 256 位 AES 密钥。对于多租户系统，我们也使用 AES-256，但使用亚马逊（Amazon）的 KMS 产品。

系统加固标准

Medidata 在所有 MCC 组件上实施 CIS 基准加固指南以及其他加固技术。

远程连接

默认情况下，Medidata 只允许来自 443 端口的入站流量。防火墙和 IDP 可阻止源端口和目的端口，并确保流量安全。全球网络运行中心（“GNOC”）全天候运行，以确保始终有人监控环境。此外，Medidata 还聘请了第三方安全管理服务提供商 (Managed Security Service Provider, MSSP) 提供全天候的安全环境覆盖，并有权采取行动保护环境，服务级别协议（SLA）为十五（15）分钟。

隐私计划

Medidata 隐私办公室（“MPO”）根据 Medidata 在代表客户处理个人数据方面的职责，执行全球隐私计划中的隐私原则。Medidata 公司的客户作为“数据控制者”，负责在 MCC 公司内提交和处理其签约服务的个人数据。数据控制者（或适用法律中定义的类似实体）是指确定个人数据处理方式和目的的实体。也就是说，当 Medidata 的客户利用 MCC 进行临床试验时，他们充当自己数据的控制者，决定收集、提交、处理、披露、保留和/或销毁哪些个人数据，以及这些活动的目的是什么。Medidata 的角色是“数据处理者”，即执行数据控制者指令的实体，以实施已决定的处理方式和目的。

Medidata 公司作为数据处理者，主要负责实施有效的数据安全措施，并在上述责任范围内遵循客户的指示。

在客户合同/协议中记录并传达对用户实体的隐私承诺。此类隐私承诺包括但不限于以下内容：

- 根据适用的协议、法律和法规，制定数据保留和处置政策与程序，以妥善处理和安全维护、处置和销毁系统硬件和敏感数据。
- MPO 实施全球隐私计划，按照适用法律和最佳做法，规范客户个人数据的收集、访问、使用、存储、披露和处置。
- 用户实体在使用 MCC 登录时，作为“使用条款”的一部分，会收到关于 Medidata 处理个人数据实践的通知。
- Medidata 对 MCC 的每个产品版本进行“隐私设计”评估，以评估对个人数据处理的影响/任何重大变更。
- Medidata 维护客户数据管理计划，以验证对客户个人数据的适当访问和使用。
- Medidata 应客户要求（根据适用的监管/法律要求）归还或删除客户个人信息。
- MPO 制定了隐私事件响应计划，用于识别和评估未经授权披露客户个人数据的行为。

设计隐私保护

Medidata 正式记录了应用程序和数据清单，上面记录了整个 MCC 个人身份信息的来源和位置。应用和数据清单由每个产品团队编制，是“隐私设计”流程的一部分。每个业务流程领域都记录并维护一个标准模板，规定收集哪类数据、该业务流程中的相关隐私风险，以及为降低该流程中发现的隐私风险而采取的控制措施。

作为设计隐私保护流程的一部分，产品所有者评估那些会导致对现有流程产生新的或变更的项目，这些变更涉及到访问、使用和/或存储参与者个人信息，以评估对个人信息及相关控制措施的影响。如发现此类变化，MPO 将评估与 MCC 中个人身份信息处理方式的任何变化相关的风险。在设计隐私保护流程中识别出的控制缺陷会被记录下来，并制定并执行纠正措施计划以解决这些缺陷。

安全设计

安全编码标准

Medidata 以 OWASP 为基础，将安全应用程序开发纳入其 SDLC 流程。它有正式的编码标准和编码指南，并受版本控制，因为它们都存储在我们的源代码库中。

软件开发生命周期

MCC 提供端到端技术和数据分析解决方案，旨在管理整个临床开发过程中的各项活动。作为一个 SaaS 环境，Medidata 平台可以根据客户的需求进行扩展和伸缩。Medidata 通过坚持以敏捷（Agile）开发原则为驱动的文档化 SDLC 流程来实现这一目标，并在整个流程中提高质量。Medidata 生产的软件位于合格的基础设施上，符合客户要求，发挥预期功能，并支持遵守适用的 GCP、数据保护/数据隐私和电子记录/电子签名（Electronic Records/Electronic Signatures, “ERES”）法规和指南。我们的软件开发和发布程序中记录了 SDLC 要求和流程。托管环境架构管理文件中记录了 IT 基础设施的资质要求和流程。

SDLC 活动由研发部门负责。研发部门下设职能部门，每个部门都对 Medidata 软件的设计、开发、测试、验证、部署和运行支持负有管理责任和权力。软件发布类型包括 alpha 版、beta 版、功能版、标准软件发布和紧急软件发布。

漏洞识别和管理

Medidata 漏洞评估是对信息系统潜在安全弱点的系统性审查。它评估系统是否易受任何已知漏洞的影响，为这些漏洞指定严重程度，并在必要时随时提出补救或缓解建议。

应用程序安全漏洞评估

Medidata 对软件进行安全漏洞评估的主要目标是Medidata 为客户提供的服务是识别系统、网络和应用程序安全控制中的漏洞，这些漏洞可能会被利用来访问系统和指定数据，而未经授权的用户是无法获取这些数据的。评估包括动态（Dynamic Application Security Testing, DAST）和静态（Static Application Security Testing, SAST）代码分析安全扫描。Medidata 将在规定的测试参数范围内，尝试识别和利用已识别的任何系统、网络和应用程序漏洞，以实现上述目标。

不会试图伪装任何攻击，因为这不是隐形安全评估。需要注意的是，真正的攻击对于系统管理员来说可能并不那么明显。测试过程可以是手动的，以限制一般漏洞评估中使用的扫描仪和核对表方法得出的通用结果。此外，还可使用自动工具进行应用程序映射和潜在漏洞识别。这样，测试人员就可以集中精力对应用程序进行基于逻辑的定向测试。

网络安全漏洞评估（渗透测试）

Medidata 的网络漏洞评估将包括服务器、交换机、路由器和工作站等资源，这些资源可从 Medidata 网络外的测试地点到达。Medidata 将采用经首席信息安全官（Chief Information Security Officer, CISO）批准的、精心编写的测试方法对网络和组件进行测试。《参与规则》规定，任何测试都不包括对非 Medidata 所有和/或运营的互连网络组件的测试。

此外，测试不应包括有意导致任何系统服务拒绝（Denial of Service, DoS）或故意损坏任何遇到的可利用目标系统的行为。外部漏洞评估将从 Medidata 物理位置/网络以外的位置进行。

Medidata 对其环境和相关控制进行多次独立评估，包括定期漏洞评估和渗透测试。这些测试分别每周和每季度在整个环境中进行一次。信息安全部评估为“严重”或“高度”的所有安全问题，除非得到信息安全主管的书面认可，否则应在发现后三十 (30) 个日历日内进行补救。所有安全问题除非信息安全主管书面同意，否则应在发现后 180 个日历日内对信息安全评估为“中度 ”的情况采取补救措施。

独立测试和审查

只有客观的观察者认为安全才是最好的。因此，除了我们对客户和监管机构的评估之外，我们还使用多个独立的实体进行定期轮换，以防止自满，并确保我们引入客观性、尖端技术和新兴技术，以确保我们客户的知识产权及其患者的信息得到妥善保护。

SOC2 是由美国注册会计师协会（American Institute of CPAs, AICPA）制定的服务机构自愿合规标准，规定了机构应如何管理客户数据。该标准基于以下信任服务标准：安全性、可用性、处理完整性、保密性和隐私性。SOC2 报告是根据每个组织的独特需求量身定制的。根据其特定的业务实践，每个组织都可以设计遵循一个或多个信任原则的控制措施。这些报告为企业及其客户、监管机构、业务合作伙伴和供应商提供了有关企业如何管理数据的重要信息。

SOC2 报告有两种类型：第 1 类描述组织的系统以及系统设计是否符合相关的信任原则。第 2 类详细介绍了这些系统的运行效率。

Medidata 维持 SOC2+ 类型 2，以展示 Medidata 对于安全和隐私（“适用的信任服务标准”）的承诺，这些标准载于 TSP 第 100 节，即《2017 年安全、可用性、处理完整性、保密性和隐私的信托服务标准》（AICPA，《信托服务标准》），以及 Medidata Solutions, Inc.确定的与开发和部署、质量保证以及电子记录和签名相关的附加标准。

SOC 评估每 6 个月进行一次，以 12 个月的滚动人口时间框为基础。Medidata 还为 Medidata 平台临床试验管理系统（Clinical Trial Management System, CTMS）网站支付产品维护 SOC-I 类型 2。

ISO/IEC27001

ISO 27001 是一项安全管理标准，它按照 ISO 27002 最佳实践指南，规定了安全管理最佳实践和全面的安全控制措施。这是一个得到广泛认可的国际安全标准，Medidata 的客户对此表现出极大的兴趣。

标准认证要求我们：

- 系统地评估我们的信息安全风险，同时考虑到公司威胁和漏洞的影响。
- 设计并实施一套全面的信息安全控制和其他形式的风险管理，以应对公司和架构的安全风险。
- 采用总体管理流程，确保信息安全控制措施持续满足我们的信息安全需求。

该标准认证的关键在于有效管理严格的安全计划。该标准所要求的信息安全管理系统（Information Security Management System, ISMS）定义了我们如何以整体、全面的方式持续管理安全。ISO/IEC 27001 认证专门针对 Medidata 的 ISMS，衡量我们的内部流程如何遵循 ISO 标准。认证意味着第三方认可的独立审计员已对我们的流程和控制措施进行了评估，并确认我们的运营符合全面的 ISO/IEC 27001 认证标准。

ISO/IEC27701

ISO/IEC 27701 认证与 ISO/IEC 27001 认证配套使用，涵盖了建立、实施、维护和持续改进隐私信息管理系统（Privacy Information Management System, PIMS）的要求。

ISO/IEC27017

ISO/IEC 27701 是适用于云服务的信息安全操作规范。它是 ISO/IEC 27001 和 ISO/IEC 27002 的扩展，为云服务提供商和云服务客户提供额外的安全控制。

ISO/IEC27018

ISO/IEC 27018 是一项安全管理标准，规定了云计算环境中隐私信息的安全管理最佳实践和全面安全控制。该标准是对 ISO/IEC 27001 和其他安全框架的补充，以保持对隐私相关信息的有效管理。

与 ISO/IEC 27001 认证一样，ISO/IEC 27017 和 27018 认证意味着第三方认可的独立审计员已对我们的流程和控制措施进行了评估，并确认我们的运营符合全面的 ISO 27018 认证标准。

FISMA 中等级别

Medidata 帮助美国政府机构客户实现并持续遵守《联邦信息安全管理法案》（Federal Information Security Management Act, FISMA）。FISMA 要求联邦机构根据美国国家标准与技术研究院特别出版物（National Institute of Standards and Technology Special Publication, NIST）SP 800-53 第 5 次修订版，为其数据和基础设施开发、记录和实施信息安全系统。FISMA 要求 Medidata 实施和运行一套全面的安全配置和控件。这包括记录用于确保物理和虚拟基础设施安全的管理、操作和技术流程，以及对既定流程和控制措施的第三方审计。Medidata 每年都会接受评估，以确保我们的软件即服务符合 FISMA 合规性要求，并已获得多家美国政府机构颁发的运营授权（Authority to Operate, ATO）。

欧盟-美国数据隐私框架（DPF）及相关框架

欧盟-美国数据隐私框架以及相关框架，如英国对欧盟-美国 DPF 的扩展和瑞士-美国 DPF，为 Medidata 提供了从欧盟、英国和瑞士向美国传输个人数据的可靠机制，同时确保数据保护符合欧盟、英国和瑞士的法律。参与欧盟-美国 DPF 和相关框架的组织可从以下方面接收个人数据：(1) 从欧盟接收，自 2023 年 7 月 10 日起生效，这是欧盟委员会对欧盟-美国 DPF 充分性决定的生效日期，(2) 从英国接收，自 2023 年 10 月 12 日起生效，这是实施英国扩展的充分性法规的生效日期，以及(3) 从瑞士接收，在瑞士对瑞士-美国 DPF 的充分性认可生效之日。欧盟-美国 DPF 和相关框架对美国公司规定了保护全球欧盟、英国和瑞士公民个人数据的严格义务。

这在实践中意味着什么？

Medidata Solutions

- 遵守欧盟-美国 DPF 原则（通知、选择、向前传输的责任、安全、数据完整性和用途限制、访问、追索、执行和责任）。
- 每年进行自我认证，证明我们符合欧盟-美国 DPF 的要求。

对于 Medidata Solutions 的欧洲、英国和瑞士客户

- 提高向美国转移个人数据的透明度，加强对个人数据的保护。
- 可以通过访问欧盟-美国 DPF 网站 https://dataprivacyframework.gov 来验证 Medidata 对欧盟-美国 DPF 的自我认证。

FIPS 140-2

《联邦信息处理标准》（Federal Information Processing Standard, FIPS）第 140-2 号出版物是美国政府的一项安全标准，规定了保护敏感信息的加密模块的安全要求。为支持客户满足 FIPS 140-2 要求，Medidata Private Cloud 端点和 Medidata 中的终端负载平衡器使用经 FIPS 140-2 验证的算法运行。在 FIPS-140-2 合规模式下运行确实需要在用户浏览器端的连接上具备可比的能力。虽然我们不使用经 FIPS 140-2 认证的硬件，但我们使用的是经 FIPS 140-2 全面认证的软件的同类品牌和型号。

健康保险便利与责任法案（HIPAA）

根据 Medidata 提供的特定服务的要求，Medidata 使受美国《健康保险便利与责任法案》（Health Insurance Portability and Accountability Act, HIPAA）保护的实体及其业务合作方能够利用安全的 Medidata 环境来处理、维护和存储受保护的健康信息。

关闭

我们认为，Medidata 的安全实践是世界一流的，由最优秀的人才、流程和技术负责。我们认真负责，每天都在赢得客户及其患者的信任。我们为自己的工作感到自豪，并乐于展示。

除本文件外，我们还在 https://www.medidata.com/en/trust-and-transparency 上发布漏洞摘要、渗透测试结果、认证、审计和其他安全相关事项，以便让我们的客户及其网站可以放心，保护措施符合患者的期望。

如有任何疑问或澄清，请随时联系 Medidata 信息安全框架团队，电子邮件：asksecurity@3ds.com

免责声明

本《安全白皮书》所载信息仅供参考

本文件中的任何内容或口头转达给任何客户的任何内容，均不得视为对该客户与 Medidata 或 Medidata 子公司或附属公司（统称“Medidata”）之间任何书面协议的条款和条件的修正、修改或取代。

Medidata 不向客户承诺或保证本《安全白皮书》中描述的任何方法或建议将恢复客户的系统、解决与任何恶意代码相关的任何问题或实现任何其他声明或预期的结果。客户自行承担使用或不使用本《安全白皮书》中所述任何指导的所有风险。