迈瑞产品网络安全白皮书

2026年3月

mindray

目录

执行摘要

在医疗保健和医疗设备领域不断创新迭代的形势下，采取强有力的网络安全措施势在必行。随着行业不断拥抱先进技术和数字化，医疗服务与设备的安全保障需求持续升级，确保其安全可靠、值得信赖，既是我们的基本责任，也是应对技术变革的必然要求。本白皮书阐述了迈瑞在网络安全领域的综合策略，详细介绍了相关原则、价值观和实践。正是这些原则、价值观和实践推动我们不懈努力，保障患者安全、保护客户数据，并持续确保设备运行的稳定性与连续性。

迈瑞在网络安全方面**强调透明可信、责任共担和不懈改进**。我们相信，通过分享我们设备中采取的安全措施、相关风险考量和敏感数据处理流程，赋能利益相关者基于完整信息做出知情、审慎的决策，这是迈瑞进一步建立**信任**的关键。迈瑞将隐私保护和网络安全融入产品开发生命周期的每个环节，以负责任的方式提供产品和服务，从而确保在实现技术创新的同时兼顾产品安全与稳定性。

在迈瑞，**强大的企业信息安全**框架是提供安全可靠的医疗设备和服务的基石。这是我们运营的基础，立足于我们训练有素的**员工**的专业知识和统一愿景之上，正是员工对网络安全的坚守助力我们安全创新。

迈瑞对于保障网络安全的承诺不仅注重**遵守**相关标准和法规，更注重培养一种渗透到我们组织各个方面的安全文化。从最初的概念阶段到上市后的监控，迈瑞将对网络安全的考量融入到产品生命周期的每个环节。迈瑞**获得的认证**彰显了我们对于实现高级别的安全和隐私保护的不懈追求。这些认证不仅是一种荣誉，还是一种力证，证明了我们对卓越的不懈追求，以及对守护患者健康并保障迈瑞设备在运行过程中保护患者敏感数据的承诺。

在责任共担的背景下，迈瑞深知医疗领域的网络安全需要各方共同努力。我们积极与医疗机构、监管机构和其他利益相关者密切合作，打造安全的患者护理环境。这种协作对于识别潜在漏洞、应对各种事件和提升全球医疗环境的安全水平至关重要。我们致力于通过促进开放的沟通与合作，构建抵御网络威胁的强大防线。

迈瑞产品网络安全模型的支柱包括治理和风险管理、安全设计和开发、保护措施和控制、全生命周期管理、事件管理和数据保护，反映了一种应对网络安全多面性的整体战略。其中每个战略。其中每个支柱都是我们网络安全总框架的关键要素，有助于确保我们的设备不仅符合当前标准，并且能够抵御未来威胁。

我们深知，必须坚定不移地全心守护用户对我们和我们设备的信任，这是一项光荣的责任。面对数字化时代的种种复杂挑战，迈瑞将继续坚持诚信、创新、以及对守护医疗行业的坚定决心，与行业携手共进、稳健前行。

领航医疗数字化：安全创新之路

最近几十年来，在技术飞速进步和数字化的推动下，医疗设备和医疗保健行业经历了重大变革。远程医疗、可穿戴健康监控设备和远程诊断工具等创新技术促进了患者护理方式的变革，使其更高效、更准确、更可及。

然而，随着医疗行业越来越依赖互联数字技术，该行业面临的网络安全风险也越来越高。医疗设备与医院网络和云平台的集成使其网络架构更复杂，从而可能产生新的漏洞，这进一步凸显了采取强效安全措施以保障设备可靠性并保护敏感患者数据的重要性。

与WannaCry网络攻击事件类似，近年来许多重大的网络安全漏洞对医疗行业造成了严重影响。例如，斯普林希尔医疗中心的勒索软件事件[1]使医院系统瘫痪，导致一名婴儿在分娩过程中因关键监控系统失效而死亡。

2020年佛蒙特大学健康网络[2]遭到勒索软件攻击，造成严重的运营中断，延误了患者护理并迫使医院恢复使用纸质记录。医疗设备劫持(Medjack)攻击[3]的目标是医疗设备，诸如输液泵和磁共振成像(MRI)设备，利用过时的软件和不完善的安全措施的弱点来控制和入侵更广泛的医院网络。NotPetya勒索软件[4]利用EternalBlue[5]漏洞发起攻击，对关键数据进行加密并引发服务中断，严重影响了全球医疗服务的运营。

这些事件都凸显了网络攻击可能对医疗系统造成的严重影响，如损害患者信息的机密性、破坏基本医疗服务等。

鉴于这些挑战，迈瑞致力于在探索数字化创新和保障安全之间取得平衡。

通过建立严格的标准、遵守国际要求并倡导透明可信、责任共担和不懈改进，迈瑞致力于确保以安全可靠的方式实现创新，在不牺牲安全性的情况下提升患者护理水平。

[1] https://www.healthcareitnews.com/news/hospital-ransomware-attack-led-infants-death-lawsuit-alleges
[2] https://coverlink.com/case-study/uvm-health-network-ransomware-attack/
[3] https://www.trustdimension.com/wp-content/uploads/2015/02/MedJack.4-ilovepdf-compressed.pdf
[4] https://www.cloudflare.com/learning/security/ransomware/petya-notpetya-ransomware/
[5] https://www.avast.com/c-eternalblue

迈瑞网络安全立场

迈瑞深知网络安全威胁的风险日益严峻，并且致力于不断强化我们的流程和体系，将网络安全和隐私保护融入各个方面。

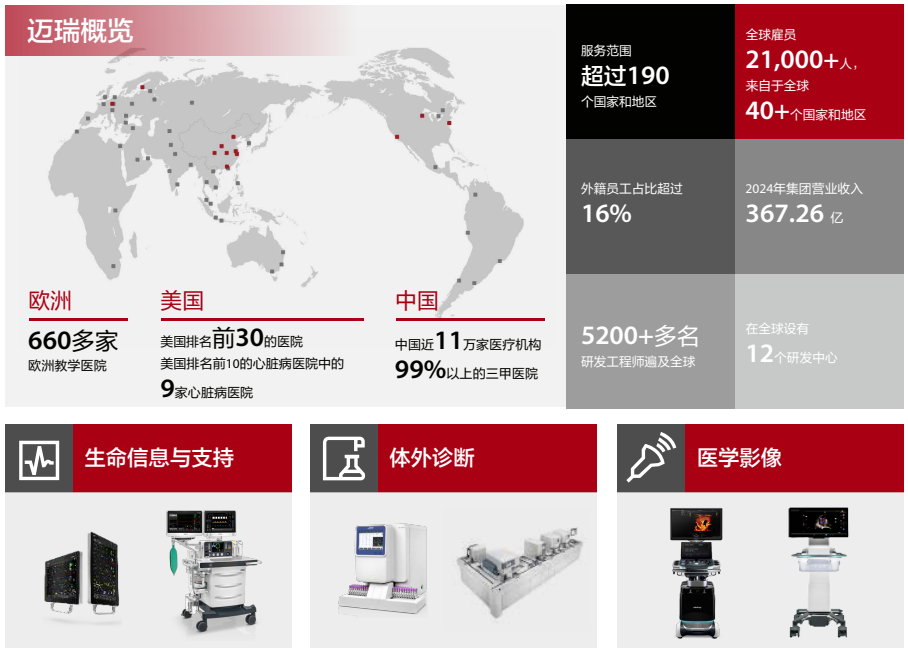
- 卓越引领
- 透明可信
- 组织安全
- 合法合规
- 责任共担

迈瑞网络安全立场

卓越引领

迈瑞是全球领先的医疗设备和解决方案设计者、开发者和制造商，致力于让更多人分享优质生命关怀。自 1991 年成立以来，迈瑞专注于打造三条主要产品线：生命信息与支持 (PMLS)、医学影像 (MIS) 和体外诊断 (IVD)。

迈瑞公司总部位于中国深圳，在全球超40个国家设有64家境外子公司，在全球有约21,000名员工负责为不同的医疗机构提供支持，为社会创造价值。本公司积极致力于创新，在全球设有12个研发中心并且将约 10% 的营业收入用于研发，在创新投资方面处于行业前列。



透明可信

在迈瑞，透明可信是产品网络安全的重要原则。我们对网络安全的态度根植于保障医疗设备的安全稳定和对患者数据的保护中。在国际标准和最佳实践的指导下，我们透明可信、责任共担、不懈改进。

我们的努力旨在创造一个更安全、更可靠的医疗环境，将尖端技术与可靠的安全性相结合，保护并赋能我们所服务的客户。

“信任为合作之基，透明为立信之道。迈瑞以公开透明践行信任，让安全每一步都清晰可见。这让我们的客户决策更安心，因为深知其数据、设备与患者，均由一家看得见、信得过的合作伙伴全力守护。”

吴昊

总裁，迈瑞合规委员会委员

“在迈瑞，安全已根植于我们的每一台设备的基因之中，即使在最严峻的医疗环境中，我们的设备依然需确保稳定性与可靠性。网络安全不仅是一项功能，更是推动我们设计、开发和部署每台医疗设备的核心原则。”

李在文

高级副总裁，迈瑞合规委员会委员

在医疗行业，作为医疗设备制造商，我们始终将“透明度”放在企业原则和价值观的核心位置。我们的愿景超越基本合规要求，体现了对用户知情决策权的深切尊重与责任担当。FDA[6]倡导就设备的网络安全特性及潜在风险建立清晰透明的沟通机制，以便与医疗机构、监管机构和患者建立信任。迈瑞通过白皮书、用户手册、技术文档等多维信息渠道，共享已实施的安全措施、风险考量以及患者敏感数据保护方法，以此践行我们对网络安全透明度的承诺。

我们将“安全融入设计”和“隐私融入设计”嵌入到产品开发生命周期中，确保网络安全与隐私保护从概念阶段就根植于产品的基因之中，从而保障基本医疗服务的连续性，并维护数据机密性。我们缜密的风险管理框架要求不断评估和缓解潜在的安全威胁，确保我们的医疗设备不仅安全可靠，而且具有恢复能力，值得信赖。通过与医疗机构、监管机构和行业合作伙伴密切协作，我们致力于营造一种安全文化，从而推动全球医疗生态系统的信任建设，提升医疗服务与产品的可信水平。

“安全融入设计”和“隐私融入设计”

[6] https://www.fda.gov/media/119933/download

组织安全

在迈瑞，我们的网络安全机制渗透到整体企业文化中，并融入到每件产品和服务内。我们深知，**公司**强大的企业信息安全是建立和维护客户对我们和我们设备的信任的基础。只有被组织充分赋能、且被熏陶有安全使命感的**员工**才能成为能够支撑企业信息安全、守护客户信任的骨干力量，设计并提供安全可靠的服务和**产品**。

统一的安全文化：迈瑞的企业文化建立在安全意识和最佳实践的基础之上。我们在全体员工中培育“安全优先”的理念，覆盖从高管团队到研发一线的所有员工，全面建立安全第一的意识。这种高度重视安全的企业文化是通过频繁的培训计划形成的，这些培训不仅包括“安全融入设计”和“隐私融入设计”的原则，还包括更广泛的信息安全和隐私保护。这种全方位的培训机制有助于将先进的安全和隐私功能融入到日常运营和产品设计中，加强我们的公司和设备的可信度和合规性。

韧性基础设施：我们的企业安全基础设施旨在确保运营稳定性和数据机密性，这对于保障我们业务运营和客户支持的连续性与可靠性至关重要。我们通过保护我们的数据中心、网络和软件架构，防止其发生中断和破坏，从而确保为产品开发和维护服务提供支持的系统始终可用并且安全可靠。

积极主动的事件响应和持续改进：迈瑞的动态事件响应能力和持续的安全评估确保能够在企业和产品层面快速应对潜在的网络攻击和漏洞。这种积极主动的态度不仅可以降低风险，还可以基于真实世界数据和新兴威胁态势促进我们企业和产品安全功能持续改进。

利益相关者的参与和透明度：在迈瑞，我们努力对我们的安全流程和发展状态保持开放沟通。通过对企业和产品安全战略保持透明，我们旨在与客户建立更深层次的信任，向他们保证我们致力于践行更高安全标准、保障患者安全并保护他们的敏感信息。

公司：战略防御

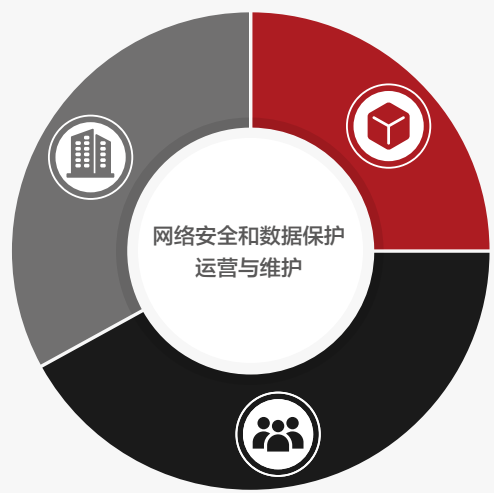
通过全面的事件响应机制和韧性基础设施，构筑企业坚实安全后盾。这确保了运营的稳定性，同时促进保障内部系统和数据方面的持续改进。

员工：获得赋能的强大保护者

通过接受安全实践和隐私标准方面的全方位培训，我们的员工坚持践行“安全第一”的文化并积极推广。

产品：安全创新

从设计到开发，将先进的安全功能融入到每一台医疗设备中，提供客户信任的可靠产品。



合法合规

在迈瑞，我们认同并尊重法律法规、国际标准和认证等要求在确保高水平的产品质量、安全和网络安全方面的重要性和价值。我们坚定地遵守这些要求，不仅为满足法律或认证需求，更为让客户和用户感受到信任与保障。这可以让我们的利益相关者放心，相信我们会以最大的诚信运营，确保产品符合严格的质量和安全基准。这种信任在医疗行业至关重要，因为医疗设备的可靠性和安全性直接影响患者的护理和治疗效果。因此，这些标准和认证印证了我们对保障公司及产品安全的坚定承诺，以及持续成长与改进的努力，推动我们不断提升实践水平。

迈瑞遵循的相关标准和要求包括但不限于ANSI/AAMI SW96、ISO 14971、ISO 31000、IEC/TR 80001-2-2、FDA 上市前和上市后要求及指南、MDCG 2019-16、IMDRF 原则和实践、欧盟《通用数据保护条例》(GDPR)、美国《健康保险可携性和责任法案》(HIPAA) 和《中华人民共和国个人信息保护法》(PIPL)。这些要求指导着我们的流程，涵盖整个产品开发和生命周期管理。通过遵守这些要求，我们确保妥善管理组织风险，并且使产品在设计、开发和维护的全过程都符合最高安全标准。

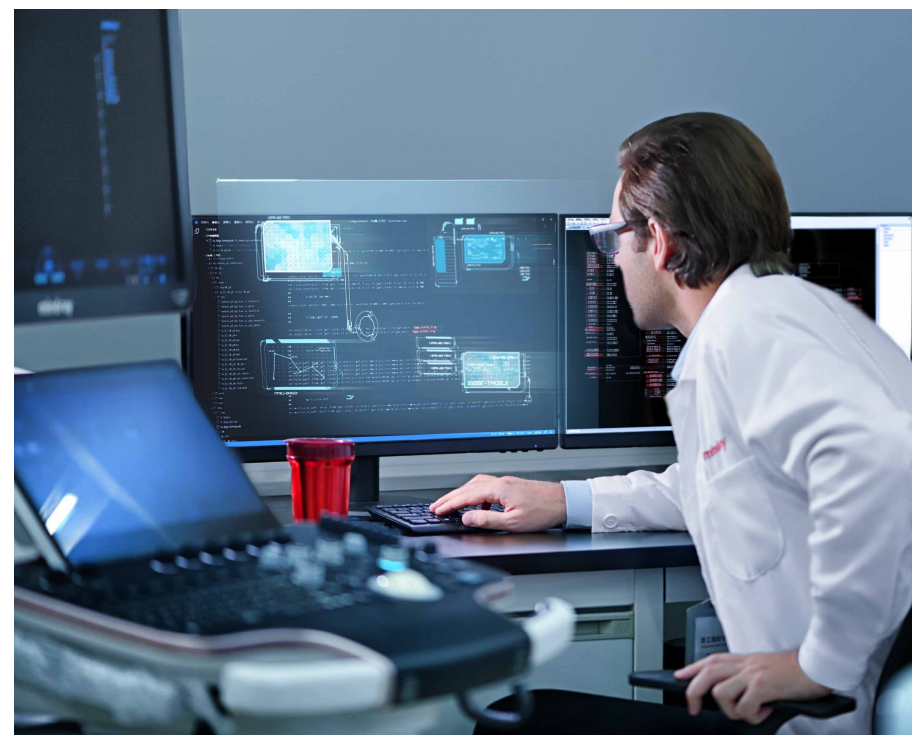
在认证方面，迈瑞已获得多项权威认证，包括 ISO/IEC 27001:2022 信息安全管理体系认证和 ISO/IEC 27701:2019 隐私信息管理体系认证。这些认证涵盖研发、销售、服务、IT等多个运营环节，确保实现全面的合规性和安全性。其他认证还包括医疗信息安全标准NEN7510、针对网络连接设备的UL2900-2-1等。

解决方案

某些要求和认证的适用性取决于具体的产品和销售区域。例如，在美国市场销售的设备严格遵循美国FDA要求，通过510(k)上市前通告等法规途径完成合规认证。我们进行全面深入的研究和监控，确保产品基于目标市场和预期用途满足相关监管要求。

通过达到并保持这些要求和认证，迈瑞努力展示其对追求卓越的坚定承诺，增强企业公信力，并且不断激励创新和改进，确保始终如一地为全球医疗机构和患者提供安全、可靠的医疗设备和服务。

我们坚定地遵守这些要求，不仅为满足法律或认证需求，更为让客户和用户感受到信任与保障。



责任共担

迈瑞认为，医疗保健和医疗设备行业的网络安全是一项共同的责任。医疗设备的互联特性要求制造商和医疗机构之间密切协作，以确保践行强有力的网络安全实践。设备制造商负责遵守行业法规，在设计和开发过程中集成强大的安全功能，进行严格的测试，并及时进行软件更新与漏洞修补来打造安全产品。他们还必须就设备的安全使用提供明确的指引与维护支持。另一方面，医疗机构在其系统内部署设备后，在管理安全性方面发挥着至关重要的作用。这包括实施正确的网络配置、控制对设备的物理访问以及持续监控潜在威胁。医疗机构还必须确保对员工进行充分的安全实践培训，提高其对技术功能的基本理解，并遵循相关规程以保护设备及其处理的敏感数据。通过这种协作，制造商和医疗机构共同构筑安全生态，在技术创新与患者安全及数据保护之间实现动态平衡。

该原则不仅由迈瑞积极倡导，还得到了众多研究机构、学术界和业界同行的支持。国际医疗器械监管机构论坛(IMDRF)[7]指出：医疗设备的网络安全需要设备制造商与医疗机构的紧密协作，强调责任共担原则适用于设备全生命周期。

这一模式能确保所有参与设备使用和管理的相关方都具备防范网络安全威胁的能力，从而提升整体防护韧性。FDA[8] 进一步强调，防护和应对网络入侵是整个医疗设备生态系统的共同责任，包括医疗机构、患者、供应商和设备制造商等都责无旁贷。这种协作有助于识别和缓解风险，且更有效地应对事件并从事件中恢复。

通过推广责任共担的理念，迈瑞致力于与所有利益相关者(尤其是医疗机构) 密切协作，共同提升各方对网络安全挑战的预防与应对能力，最终保护患者的健康和安全。

[7] https://www.imdrf.org/sites/default/files/docs/imdrf/final/technical/imdrf-tech-200318-pp-mdc-n60.pdf
[8] https://www.fda.gov/media/119933/download

迈瑞产品网络安全模型

迈瑞实施内部制定的安全模型，以确保全面保护医疗设备，并以此指导和协调公司内部各团队与各部门的网络安全工作。

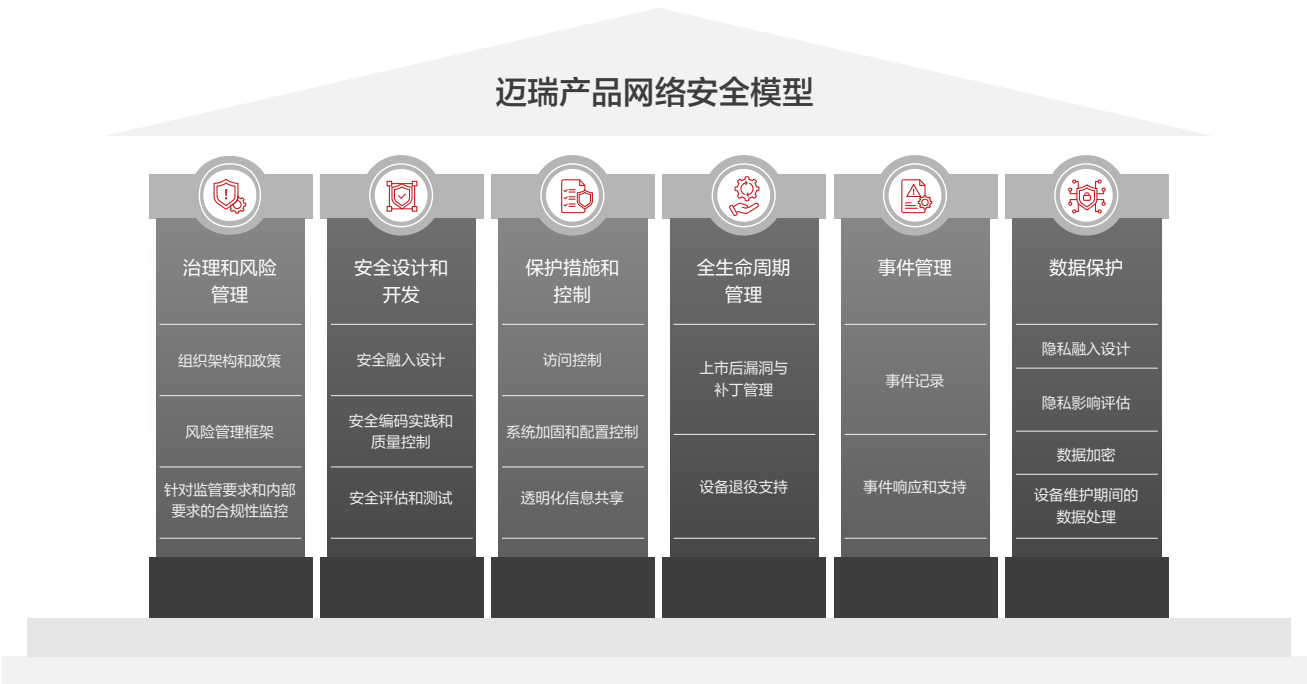
- 治理和风险管理
- 安全设计和开发
- 保护措施和控制
- 全生命周期管理
- 事件管理
- 数据保护

迈瑞产品网络安全模型

迈瑞通过“迈瑞产品网络安全模型”进行产品网络安全治理。该模型是一个内部开发的系统化框架，旨在确保我们的医疗设备得到全面的安全保护，指导并协调迈瑞不同团队和部门的网络安全工作。该模型基于 NIST 网络安全框架 (CSF)[9]的原则构建，涵盖六个核心要素：**治理、识别、保护、检测、响应和恢复**。基于这一权威框架，我们结合迈瑞实际情况形成了适配迈瑞产品的模型，以应对医疗设备行业的挑战和要求。

该模型由六大支柱和十七个要素组成，每个支柱都结合并遵循了国际标准和监管要求，以确保全面覆盖产品网络安全的所有关键要素。

治理和风险管理确保采用结构化方法来管理网络安全风险，并与行业标准和监管要求保持一致。**安全设计和开发**利用安全编码和严格测试等最佳实践，从一开始就将安全实践嵌入到产品生命周期中。**保护措施和控制**是指实施访问控制和系统加固等技术保护，以防御未经授权的访问和网络威胁。**全生命周期管理**侧重于通过有效的漏洞管理和安全退役来持续管理设备安全。**事件管理**是指建立网络安全事件的检测、响应与分析流程，强调迈瑞和医疗机构之间的责任共担。最后，**数据保护**通过“隐私融入设计”、隐私影响评估、加密和一系列合理恰当的数据安全措施来确保患者数据的机密性、完整性和可用性。这一框架体现了我们恪守的承诺，即在整个公司遵循全面的网络安全要求，确保我们医疗设备的安全性和可靠性，全力守护用户及其数据安全。通过该模型，我们不仅努力达到甚至超越全球监管要求和行业标准，也促使迈瑞成为医疗设备网络安全领域的积极领导者。



[9] https://www.nist.gov/cyberframework

治理与风险管理

迈瑞的产品网络安全建立在结构化治理政策、风险管理框架和合规监控方法的坚实基础之上。

治理架构和政策

迈瑞通过精简战略决策和政策执行流程，建立了明确的问责机制和沟通渠道。

合规委员会由公司最高管理层组成，负责指导和监督迈瑞的网络安全工作。该委员会统筹管理多个合规领域，包括决策和批准针对网络安全和隐私保护合规领域的战略和计划。

网络安全和隐私保护委员会负责制定公司网络安全和隐私保护原则及目标。该委员会指导和审查相关内部政策和框架，并管理和监督其在各地区或各业务单位中的全面实施。

合规办公室作为委员会下设的开展合规工作的日常管理机构，负责持续追踪各种法律法规动态，制定及维护公司内部合规政策及制度，建立及完善公司合规体系，推动各项合规制度的落地实施等，其中就包括网络安全和隐私保护合规工作。

产品网络安全管理团队主要负责产品网络安全的技术支持。该团队负责制定网络安全的内部要求和标准。其主要职责包括识别、推广和应用重要的网络安全技术和测试方法，监控和评估网络漏洞，并为漏洞响应和安全 软件开发等关键领域的研发工作提供技术支持。

各产品线作为产品开发的一线主体，负责在整个产品生命周期(涵盖诸如开发、生产、维护等环节)中执行合规委员会、合规办公室和产品网络安全管理团队制定的要求和标准，确保将既定的网络安全措施融合到每件产品中。产品线还需就网络安全相关需求和问题及时向管理层反馈，协同提升集团整体的产品网络安全管理能力。

风险管理框架

科学的风险管理框架是迈瑞网络安全战略的基石，使我们能够在整个产品生命周期中以系统性方式识别、评估和缓解潜在的网络安全风险。

我们的风险管理框架首先要求利用STRIDE威胁建模框架进行详细的威胁分析，通过分类识别与欺骗、篡改、否认、信息泄露、拒绝服务和特权提升相关的潜在威胁，系统性分析可能出现的威胁形式，并评估其对设备安全的潜在影响。

我们的风险管理工作包括制定详细的风险管理计划、建立软件物料清单(SBOM)、开展已知漏洞风险评估，并进行网络安全测试。基于风险管理，我们能够更好地设计风险控制措施，并将其融入到特定的产品安全要求中，从而为后续的设计和测试阶段提供指导。

我们的网络安全风险管理活动并不是一次性的工作，而是一种贯穿整个产品生命周期的持续流程，从而确保及早识别并缓解潜在威胁，降低部署后出现安全漏洞的可能性。

合规性监控

在迈瑞，合规性监控是我们网络安全战略的关键组成部分，旨在确保内部标准符合监管要求和行业期望。

迈瑞持续评估监管要求，并将任何相关变更及时纳入产品开发标准和要求。为了在满足基本合规要求的基础上更进一步，迈瑞根据行业最佳实践进行持续研究和对标工作。这种积极主动的方法使公司的安全措施既强大可靠又与时俱进，能够反映网络安全领域的最新进展和趋势。

为了确保设计的安全标准按预期实施，迈瑞还采用了系统性的“研发网络安全和数据合规矩阵”来验证开发和生产实践是否符合既定的指南和要求。该矩阵作为内部审计的检查清单，为质量控制提供保障。

安全设计和开发

安全融入设计

如前文所述，“安全融入设计”是迈瑞的基本理念，即从一开始就遵循安全原则和要求并将其融入产品开发的各个阶段。这一核心理念通过我们完善的体系和政策得以体现，我们确保从一开始就充分考虑安全规范并使其扎根于产品设计文化中。安全开发生命周期(SDL)活动深度融入整体的产品开发流程，并为我们提供最佳的网络安全开发实践指导。

作为我们所有产品的基础，我们的“安全融入设计”方法的一个关键要素是**纵深防御原则**。这种多层防御策略确保即使一项安全措施失效，其他额外的防护措施仍可保护设备及其数据的安全。

安全编码实践和质量控制

基于“安全融入设计”的原则，我们根据国际电工委员会(IEC)标准、行业最佳实践和自身丰富的软件开发经验，建立了**全面且系统的安全编码标准**。我们的安全编码标准涵盖编码的各个关键要素，包括**输入验证、错误处理和身份认证等**。这些原则使得在编码阶段即可解决潜在的安全缺陷，从而显著降低最终产品携带漏洞的风险。

流程控制和**质量保证标准**也是安全编码的关键要素。迈瑞采取**三步代码审查流程**，包括利用既定基线标准的检查表评估、利用高级工具的静态代码审查和人工代码评审，确保所有软件开发工程师在整个开发流程中严格遵守安全编码标准。

此外，迈瑞强调持续改进，注重研发人员之间的知识共享。所有开发人员都要定期接受有关安全编码技术的培训，及时了解最新的安全漏洞和缓解方法。这种积极主动的方法确保我们的工程师始终具备应对新兴风险的能力。

安全评估和测试

结合安全编码实践，迈瑞也在定期进行安全评估和测试，以确保及时识别和解决潜在的漏洞，并对已实施的安全措施进行测试和验证。

漏洞扫描：
我们利用先进的工具定期扫描产品和系统，识别潜在漏洞，主动高效地识别风险，并根据评估结果及时采取必要的修复措施。

渗透测试：
通过模拟全面网络攻击，测试设备在真实环境中的防护韧性。

第三方安全评估：
聘请独立的第三方机构进行安全评估，提供额外的验证和保障，确保我们的产品符合行业标准和监管标准。

通过将严格的安全评估和测试实践与我们的设计原则相结合，迈瑞致力于实现医疗设备内生安全，有效抵御潜在网络威胁。这种全面的方法印证了我们对交付安全、可靠、合规医疗设备的承诺，并在不断变化的网络安全形势下增强用户对产品安全性的信心。

保护措施和控制

秉承“责任共担”的理念，在医疗设备中配备必要的安全功能与防护能力，是迈瑞作为设备制造商对客户的可信承诺。

访问控制

访问控制（包括**身份认证、授权和审计**等机制）是医疗设备的关键安全措施，确保只有获得授权的用户才能访问敏感信息和系统功能。迈瑞的医疗设备配备**基于角色的访问控制(RBAC)**功能，用于根据组织内各用户的角色分配访问权限。这使得组织可以根据用户的操作需求仅向用户提供最低限度的访问权限，从而降低未授权访问文件或随意更改配置的风险。

迈瑞设备虽型号各异，但均配备多重防护措施以增强访问安全性。这些保护措施包括但不限于：

登录锁定机制	连续错误登录达一定次数后，设备将被锁定，从而防止通过暴力攻击进行未经授权的访问。
自动登出	为防止设备无人值守时发生未授权的访问，系统会在预设的无操作时长后强制终止会话。
密码管理	迈瑞设备允许自定义密码策略。我们还建议用户定期更改密码。
集中化安全认证	迈瑞利用先进、安全的系统来存储凭据和进行身份认证。这些系统采用加密技术来保护凭据数据并管理权限，确保身份认证安全进行，并降低凭据遭到盗窃或滥用的风险。
重大配置变更管控	通过严格的访问控制措施来控制重大变更（诸如操作系统升级场景只允许授权人员执行升级）。

系统加固和配置控制

系统加固是通过最小化攻击面来强化设备安全的另一种关键措施。迈瑞系统加固实践的核心要素可能因型号而异，但通常包括：

操作系统(OS)加固指南	为操作系统的各种功能列出详细的配置方法和要求。这些要求可确保所有开发团队以统一的方式安全地配置操作系统，从而以结构化方式有效落实安全要求。
应用程序和进程白名单	只有经过批准的应用程序和进程才能在设备上运行，从而防止未经授权的软件或活动执行危害系统。
防病毒和恶意软件程序	迈瑞设备经过精心设计，可与符合行业标准的防病毒和恶意软件防护程序无缝协作，实现对恶意软件的持续、高效防护。
防火墙	基于Microsoft Windows系统的迈瑞设备利用内置防火墙来限制外部访问，并控制设备内运行的应用程序。
禁用不必要的风险向量	根据业务需求和具体情况，禁用不必要的服务、端口和功能（诸如远程登录和 USB 自动运行），以最大程度减少遭受潜在攻击的可能性。
Kiosk模式	具备Kiosk 模式的设备通过限制用户仅可访问基本功能、防止未经授权的活动以及最大限度地减少对敏感患者信息的访问，显著减小攻击面。
受控的操作系统和软件升级	操作系统和设备软件的升级仅可通过经过迈瑞验证并发布的受控升级软件包进行。只有授权人员才能执行升级，并且禁止操作系统自动升级，以防止未经授权的更改。

透明化信息共享

迈瑞坚持不懈地践行承诺，提高对设备中实施的安全措施的透明度。我们提高透明度的主要措施包括但不限于：

网络安全白皮书	每条产品线还具备其各自的网络安全白皮书，详细介绍其安全措施、控制手段和实践方法，帮助利益相关者清晰了解我们在网络安全方面所做的努力。请联系迈瑞获取关于特定产品的白皮书。
产品用户手册	我们的用户手册包括对我们产品的网络安全功能的详细描述和建议，以便用户了解现有的安全机制以及如何有效地利用这些机制。
制造商医疗器械安全披露声明(MDS2)	迈瑞根据要求提供MDS2，以帮助医疗机构评估与我们的设备相关的网络安全风险和缓解措施。
软件物料清单(SBOM)	对于适用的设备，我们还可根据要求提供SBOM，以便利益相关者识别可能带来风险的第三方库及依赖项。
协助制定部署计划	我们会协助医疗机构制定部署计划，确保我们设备的安全功能正确集成到所部署的环境中并得到有效管理。这种支持包括安装、配置和日常维护方面的指导。

全生命周期管理

产品上市后的维护，彰显了迈瑞在设备部署到退役全流程中守护患者安全、患者数据及医疗运营连续性的责任担当。

上市后漏洞和补丁管理

迈瑞产品使用第三方操作系统(OS)，诸如 Microsoft Windows 和 Linux。为了管理这些操作系统可能引入的安全风险，我们制定了**全面的补丁管理策略**，以持续监控相关漏洞，评估漏洞对我们设备的影响，并部署补丁以解决问题。

对于在 Microsoft Windows 上运行的产品，我们在知悉新安全补丁后的48小时内对其进行影响评估，判断补丁是需要立即应用还是可纳入计划更新。对于需要紧急处理的关键补丁，我们会提供**详细操作指南**以支持快速更新。其他情况下，补丁通常会在数周内发布并通知用户，保障用户知情权与设备的持续防护。对于基于 Linux 的产品，我们每六个月进行一次分析。鉴于医疗设备中的 Linux 平台通常是针对特定用途定制的，补丁多以完整软件更新的形式发布。

升级软件包会在安装前进行**校验和验证**，确保其完整性和真实性，防止未经授权的篡改。此外，我们的升级过程受到严格控制，仅限授权人员使用迈瑞开发的受密码保护的工具执行操作，并默认禁用操作系统自动升级功能，以避免未授权的变更。

设备退役支持

尽管具体安排可能因市场而异，但当产品达到其使用寿命终点前，我们会主动向客户提供详细的**生命周期终止(EOL)通知函**。通知函包含维修服务终止、零部件供应及技术支持时间表等关键信息，以便客户有充足时间规划设备更换或升级。这种透明的方法确保客户能够充分了解情况并在过渡期间保持运营连续性，体现了迈瑞对提供卓越服务与客户支持的一贯承诺。

对于即将退役的设备，安全、负责任的处置流程至关重要，既要防止敏感信息遭到未经授权的访问，又要确保设备在退役后不遗留任何风险。迈瑞提供有关安全处置实践的现场指导或用户手册（诸如数据擦除操作指南），协助和支持医疗机构安全地实施设备退役。

我们还建议医疗机构遵守当地法规和国际指南，确保以安全和合法的方式处置退役设备。

事件管理

在医疗保健和医疗设备行业，网络安全事件管理被认为是一项共同的责任。只有通过医疗机构和医疗设备制造商之间的协作，才能有效预防和应对网络攻击。迈瑞采取下文所述方法，努力促进网络安全方面的协作，确保自身和医疗机构都具备充分的能力，以应对和缓解潜在的安全威胁。

事件记录

有效的事件记录是医疗设备制造商应具备的关键能力之一。迈瑞的医疗设备配备专门的日志来记录与安全相关的操作，形成全面的活动轨迹——这对后续的事件分析与响应至关重要。我们会与医疗机构紧密协作，根据其具体使用环境与需求，协助开展日志的导出、管理及分析工作。

我们的设备还设计有多种数据备份和恢复机制，确保关键安全信息在系统故障或安全事件发生时仍能被完整保存并恢复。这种韧性设计有助于维护安全日志的完整性和可用性，并且为持续的安全运维工作提供了支撑。

事件响应和支持

迈瑞成立了专门的团队来监督事件响应流程，并持续监控和研究可能影响我们设备的新事件。如果检测到安全事件或收到安全事件报告，这些团队将与业务部门协作以评估风险，制定响应计划并实施补救措施。我们制定了《网络安全事件响应指南》，确保在不同利益相关者之间采用标准化的统一方法。当需要进行监管报告时，我们与相关机构密切合作，确保信息传递的及时性与准确性。在整个过程中，我们与客户保持密切沟通，共同快速评估态势并实施补救措施，以最大限度降低影响、保障设备安全。

作为额外的支持能力，迈瑞的医疗设备具备网络安全事件期间仍能维持业务连续性的设计。虽然取决于具体设备能力，但某些设备采用数据回填、实时同步等机制，确保网络中断期间关键患者信息不丢失。一些设备还采用分层网络设计，可实现设备与医院网络间的风险隔离。此外，通过在冗余的有线和无线网络环境中运行，确保即使其中一台网络设备发生故障，其他设备也可以维持正常运行。

通过协助医疗机构落地系统化事件响应与技术支持，迈瑞致力于支持合作伙伴有效管控、应对网络安全事件并提升运营韧性。

数据保护

隐私融入设计

在企业层面，迈瑞对标国际标准和行业最佳实践，建立了以风险为导向的信息安全与隐私保护合规管理体系。该体系覆盖数据全生命周期（包括收集、传输、使用、共享、存储及删除），遵循合法、公平、诚实、公开和透明的原则，致力于保护迈瑞处理的所有个人数据的**机密性、完整性和准确性**。

通过这一健全的管理体系，迈瑞已获得ISO/IEC27001认证和ISO/IEC27701认证，并持续完善其隐私要求。

基于这样的企业文化和隐私保护意识，迈瑞承诺尊重并保护客户和患者的隐私及数据，并将**“隐私融入设计”(Privacy by Design)**和**“默认隐私保护”(Privacy by Default)**的核心原则融入到产品开发流程中（请详见第6页图示）。

这些原则通过权限管理、日志记录、加密技术、去标识化/匿名化等基线指南，在产品早期概念与规划阶段即得以落实。我们通过将隐私保护前置嵌入设计，确保隐私保护措施并非锦上添花，而是产品架构中不可或缺的一部分，从而主动应对隐私关切、提升用户信任，并满足监管要求。

迈瑞努力将隐私保护作为核心价值观融入其产品开发过程的方方面面。

迈瑞对“隐私融入设计”的承诺使我们得以与医疗机构及患者建立信任，确保用户的敏感数据得到最高标准的保障。

隐私影响评估

对于迈瑞而言，遵守数据保护和隐私法规不仅是一项法律义务，更是协助我们降低数据泄露风险、增强利益相关方信任的基石。为了全面识别隐私和数据保护方面的不足和风险，我们在产品开发过程中引入了**“隐私影响评估”(PIA)**，以确保按照相关合规要求采取有效的控制措施。

PIA流程包括对潜在隐私风险进行深入分析和记录，继而实施相应的风险缓解策略。通过实施严格的评估与管控，迈瑞与客户均能满足**GDPR, HIPAA, PIPL**等法律法规要求。我们还发布了详细的**GDPR白皮书**[10]，阐述迈瑞如何遵循这一国际公认最严格的数据保护标准。该白皮书深入介绍迈瑞的公司治理、内部控制和个人数据处理机制，展现了我们对维护数据安全与隐私高标准的承诺。

[10]https://www.mindray.com/content/dam/xpace/en/legal/GDPR.pdf

数据加密

基于“隐私融入设计”原则，数据加密是迈瑞数据保护方法的基石。作为一种重要的防御机制，数据加密可保护敏感信息免遭未经授权的访问和泄露。迈瑞采用行业公认的标准加密方法，保护传输中的数据和静态数据的安全。迈瑞的每条产品线都采用最适合其自身设备设计和特定业务需求的协议和方法，确保所有数据都得到充分保护。

传输中的数据

数据传输采用DICOM和HL7等标准，支持包括TLS 1.2(AES-256加密) 在内的多种传输加密协议。对于无线通信，迈瑞设备支持WPA/WPA2企业级加密，为Wi-Fi网络数据传输提供强化保护。

静态数据

在最小化个人数据记录与存储的原则下，必要时会采用AES-256等安全算法对静态数据进行加密，以防止未授权访问导致的数据滥用。

显示的数据

监控器显示屏或导出报告中显示的个人可识别信息(PII)可设置为隐藏状态，增强对PII访问管理的灵活管控。

数据导出

对于备份到 USB 的情况，采用带有强加密归档技术来确保数据集得到安全压缩和存储。与此同时，在将敏感数据导出或备份到硬盘时，迈瑞设备还支持匿名化和假名化技术，全方位守护患者隐私。

迈瑞设备采用先进的加密技术并且遵循严格的数据保护标准，使得无论是在传输、存储、显示还是导出数据时，用户始终可以适当地保护数据。

设备维护期间的数据处理

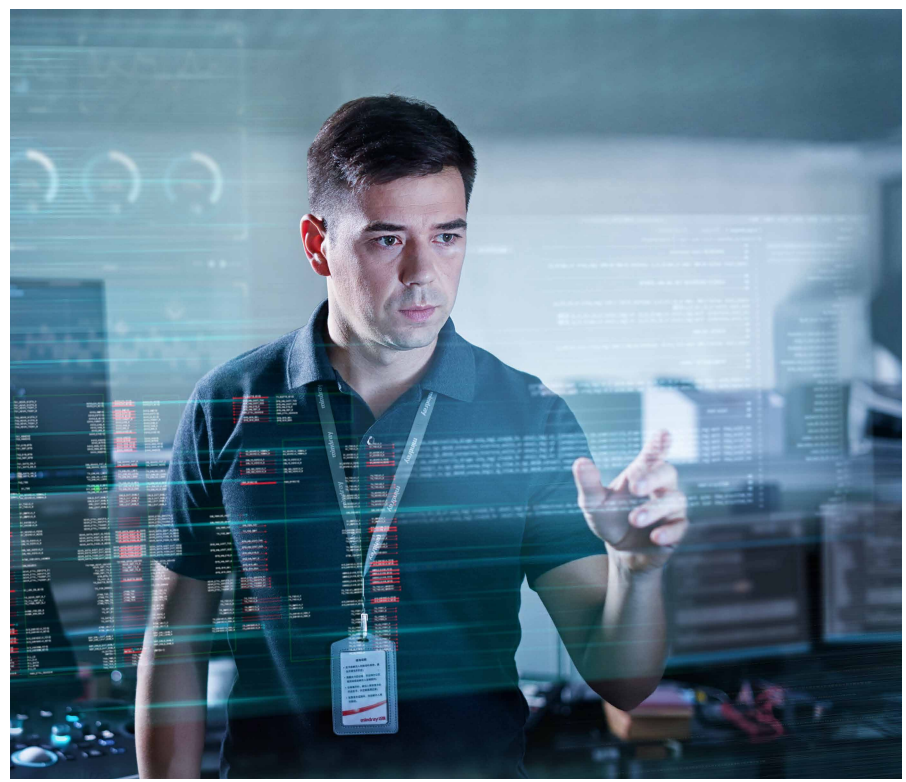
在必要的维护场景中，设备可能需要由我们的人员访问或送往我们的维修机构。针对设备数据未完全擦除、匿名化或脱敏的情况，迈瑞建立了严格的维护期间数据处理规程与内部管理制度，确保敏感信息得到妥善保护或销毁，防止未经授权的访问。

迈瑞为医疗机构提供维护期间安全数据管理的全面指导。作为一项关键措施，设备配备有安全数据擦除功能并建议启用，以确保送修设备不残留任何敏感信息。

在海外各区域，本地团队负责一线评估，判断问题是否可在本地解决。在禁止将设备和日志返回中国的地区，所有问题都在当地解决。若区域法规允许且不可避免需要将设备和日志数据传回中国进行故障排查时，当地团队将进行彻底审查，确认敏感数据已被妥善删除，从而确保遵守国际数据保护和跨境传输法规。在国内，在不可避免需要将设备和日志数据传回迈瑞进行故障排查时，用户服务团队将告知客户提前删除被维修设备中的个人信息，并进行彻底审查，确保敏感数据已被妥善删除。或者，可以采用数据脱敏技术，修改敏感信息以降低数据的可识别性，同时保留其诊断价值。这种方法包括掩盖或更改某些个人可识别信息，通过匿名化测试验证剩余数据无法追溯至个体患者。

同时，我方人员遵循最小权限原则实行严格的访问控制，仅授权人员可访问设备及数据，且其访问范围限于职责所需。所有内部人员或授权第三方人员都受保密义务的约束，确保他们以高审慎态度处理残余数据。

对于远程维护，迈瑞使用经风险控制团队严格管理的安全工具。在执行任何远程维护活动之前，都需要事先获得客户授权并严格遵循最小必要原则，仅访问设备维护所必需的数据，以最大限度地降低数据泄露的风险。我们实施了会话控制和终止流程，确保远程访问会话安全受控，并在维护完成后立即终止。



迈瑞致力于在其医疗设备的全生命周期内保持最高数据保护标准。这种做法不仅守护敏感信息，更赋予设备使用者信任与安心，这正体现了我们在推动医疗技术发展的同时，始终将客户与用户安全置于首位的承诺。

结束语

在不断发展过程中，迈瑞始终坚持以推动医疗技术进步为使命，同时在网络安全方面一直恪守最高标准。我们深知，必须坚定不移地全心守护用户对我们及设备的信任，这是一项光荣的责任。为此，我们不断增强网络安全措施并抢先防范新型威胁，努力提供具有创新性且安全可靠的医疗解决方案。

总之，这份白皮书系统呈现了迈瑞在网络安全方面全面、有效且积极主动的实践方法，重点阐述了我们如何致力于保护患者数据，确保我们医疗设备的完整性，同时营造与我们的使命相契合的安全文化。在应对数字化时代的复杂挑战时，迈瑞将继续坚持诚信、创新以及对守护医疗行业的坚定决心，引领整个行业前行。