上海联影医疗科技股份有限公司
Shanghai United Imaging Healthcare Co., Ltd.

上海市嘉定区城北路 2258 号，邮编 201807
咨询电话 | +86（21）- 67076666
售后服务 | 4006 - 866 - 088
www.united-imaging.com

联影官方微信号 | lianyingyiliao
扫一扫关注联影微信

联影医疗于 2011 年成立，总部位于上海，同时在美国、马来西亚、阿联酋、波兰等地设立区域总部及研发中心。

公司致力于为全球客户提供全线自主研发的高性能医学影像诊断与治疗设备、生命科学仪器，以及涵盖医疗数智化和贯穿「基础研究 - 临床科研 - 医学转化」全链条的创新解决方案。

以「成为世界级医疗创新引领者」为愿景，以「创造不同，为健康大同」为使命，联影医疗通过与全球高校、医院、研究机构及产业合作伙伴深度协同，不断突破科技创新边界，加速推进精准诊疗与前瞻科研探索，持续提升全球高端医疗设备及服务可及性。

网络安全声明

数字浪潮同行 · 安全共赢共生

版本号 | 91000116-CSD-SCN-02, 2025 年 6 月

外部环境变化

数字经济时代，数据要素已成为各行业新技术发展的核心驱动力。随着大数据、云计算、医疗物联网（IoMT）等技术的快速发展与深度融合，医疗健康行业正经历着前所未有的信息化变革浪潮。医疗健康设备、诊疗一体、智慧医疗等新势态出现，医疗健康行业数字化、智能化、互联化发展的趋势已不可阻挡，但同时行业和企业也面临着更严峻的网络与数据安全风险及挑战。

为了回应频发的数据和网络安全威胁，全球监管体系加速完善。多个国家或地区已颁布立法，全面实施数据安全保护措施。例如，中国《中华人民共和国数据安全法》、（中华人民共和国网络安全法），美国《健康保险流通与责任法案》(HIIPAA)《加州消费者隐私法案》(CCPA)，欧盟《通用数据保护条例》(GDPR) 等

各国医疗监管机构也陆续发布了关于医疗器械的网络安全方面的行业标准或指南。中国 NMPA《医疗器械网络安全注册审查指导原则》(2022 年修订版）明确要求企业建立纵深网络安全防御体系；美国 FDA 发布《医疗器械中的网络安全：质量体系注意事项和上市前提交内容》（2023 最终版）等均进一步强调医疗器械网络安全。

我们在行动

联影关注外部环境的变化，高度重视网络安全与合规，从始至终产品与服务的安全合规都是联影的重点发展战略之一。

联影关注各个国家和地区的合规要求并积极响应，回应所有利益相关方和行业的安全与合规需求并保障客户利益。

为此，联影于 2012 年成立信息安全部，2016 年成立信息安全监督管理委员会，2017 年基于风险管理和行业最佳实践构建了企业安全内控体系，并在 2017-2024 年先后通过海内外不同国家、地区、乃至国际上都具有广义认可度的安全合规认证和检测

时间线

2011
联影医疗成立

2012
联影信息安全部成立

2013
第一代产品上市

2014
美国：医疗器械网络安全管理上市前提交内容

2016
美国：医疗器械网络安全上市后管理

2017
ISO/IEC 27001:2013 首次认证

2018
发布《产品网络安全程序》

2019
NIST CSF 1.0 符合性评估良好

2021
引入安全开发生命周期管理理念

2022
ISO/IEC 20000:2018 认证
CCRC 二级认证

2024
ISO/IEC 27001:2022 升版认证
CCID 评估 一级五星
NIST CSF 2.0 符合性评估优秀
ITSS 三级认证
“工赋砺网”护网行动 零失分并荣获优秀蓝方称号

安全认证与最佳实践遵从

联影建立并运行符合 ISO/IEC 国际标准的信息安全管理体系 (ISMS) 及隐私保护管理体系 (PIMS)。在 ISO/IEC 27000：2022 系列的基础上，将美国国家标准和技术协会 (NIST) 发布的企业网络安全框架（CSF 2.0）融入体系，动态识别各国、各地区的信息安全和隐私法规要求及最佳安全实践，遵循 PDCA 方针持续改进。确保可以为客户提供安全合规的产品与服务，满足不同地区、国家客户的安全与合规需求。

ISO 27000 系列

ISO/IEC 27001

信息安全管理体系

是一套获得业界广泛认可的安全管理体系标准，一直被认为是国际最权威、最严格的信息安全体系（ISMS）认证标准，被全球广泛接受。

联影通过此项认证意味着我们在信息安全管理领域已经与国际标准对标，具有充分的信息安全风险识别和控制能力，可以为全球客户提供安全可靠的服务。

ISO/IEC 27701

隐私信息管理体系

是首个真正意义上构建出具有 PDCA 完整运行闭环的隐私信息管理体系（PIMS）标准。其详细规定了建立、实施、维护和不断改进隐私信息管理系统的各项要求，在信息 安全保护的基础上将处理个人可识别信息（PII）所需的隐私保护措施纳入考量。联影是全球首批获得该认证的医疗器械制造企业之一，联影获得此项认证，有助于确保在为客户服务过程中隐私合规。

ISO/IEC 27017

云服务信息安全管理体系

提出特定于云的信息安全控制机制实施建议，补充了 ISO 27002 和 ISO 27001 标准的指导。此标准针对云服务提供商提供了更多信息安全控制实施指导。联影通过此项认证，意味着我们在云服务类产品和服务等方面已经达到国际标准。

ISO/IEC 27018

公有云隐私安全管理体系

是首个专注于公有云中个人信息保护的国际认证标准，基于 ISO27002 信息安全管理实用规则，并针对适用于公有云个人可识别信息（PII）的安全控制体系提供了实施指南。

联影通过此项认证，意味着我们在保护企业数据、保障用户个人信息安全、防止信息泄漏等方面已经达到了业界实践的高标准。

ISO 27799

医疗健康安全管理体系

是一套特别关注医疗健康部门面临挑战的医疗健康安全管理体系（ISMH）标准。其关注个人健康信息的保密性、完整性和可得性，并确保对这些信息的获取可以进行审计和问责。有助于防止医疗实践中的错误， 同时确保医疗服务的连续性的。

联影是较早关注该认证的医疗器械制造商企业之一。联影获得此项认证，意味着我们通过遵守 ISO 27799 的框架和原则，为您提供安全协作的产品和服务，有助于您能安全采用协作技术来提供医疗保健服务显著改善医疗结果。

安全认证与最佳实践遵从

NIST 网络安全框架 CSF （2.0）

是一套美国国家标准和技术协会 (NIST) 网络安全框架 (CSF 2.0)，它包含用于管理网络安全相关风险的标准、指南和最佳做法。NIST CSF 参考了全球公认的标准，包括部分 NIST SP 800-53 信息系统和组织的安全和隐私控制。

2019 年，国际上具有广义认可度的第三方评估机构基于 NIST CSF(1.0) 对联影展开全面测评，得分良好，2024 年，NIST 发布 CSF(2.0) 正式版本，联影再次接受基于 2.0 版本的全面测评，得分为优秀。说明联影产品有能力为客户提供良好的网络安全保障，且联影的安全建设在不断优化和发展中。

网络安全等级保护三级

《GB/T 22239—2019 信息安全技术 网络安全等级保护基本要求》简称网络安全等级保护，是中国国家标准化管理委员会发布的信息安全标准，是中华人民共和国信息安全保障的一项基本制度。联影采用了三级等保的保护策略，并通过了专业测评机构的测评。说明联影产品在安全事件的发现、应对能力，信息系统受到破坏时的恢复能力方面已达到业界最佳实践水平。

密码应用安全性评估

是在等级保护基础上，对密码应用安全性提出的更加严格的要求。它对全局密码应用技术管理、物理环境、网络通信、设备计算等八个方面的安全性、规范性和有效性进行量化评估，联影产品开展了关于密码应用安全性评估，并通过了专业测评机构的测评。说明联影产品和服务有能力帮助您更规范的使用密码和管理密码，为维护您的网络和信息系统密码安全，切实保障网络安全与数据安全。

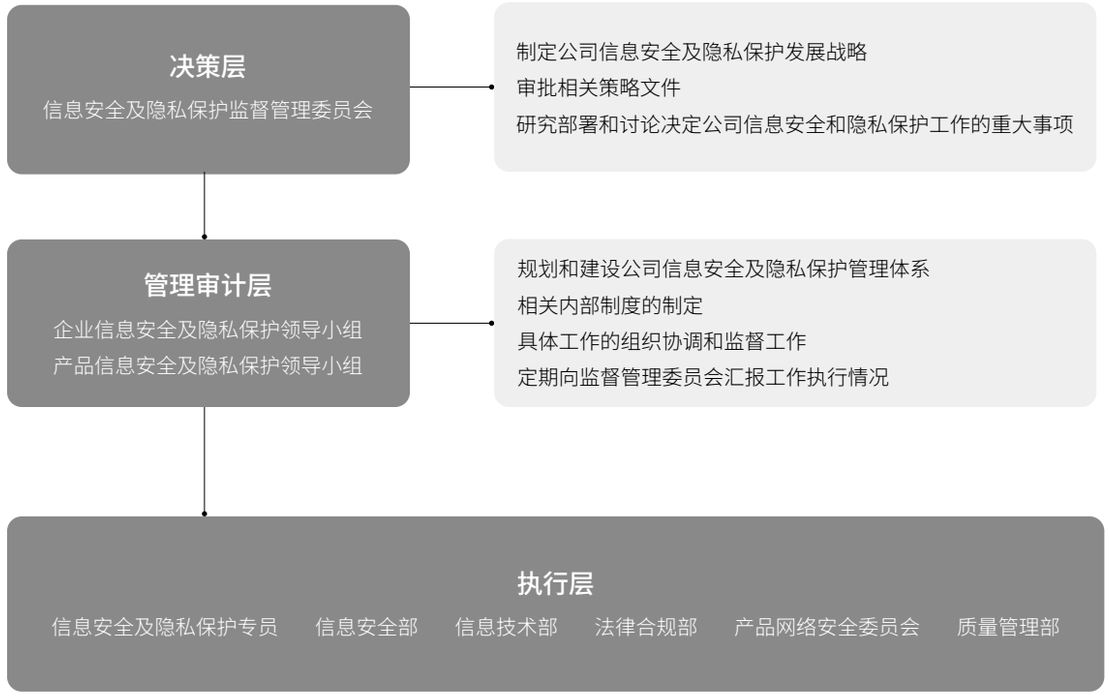
联影积极跟进国内外对产品安全性合规性的要求，通过安全管理与合规团队对接各级监管机构，确保提供的产品和服务符合行业标准。并配备专门的隐私保护团队，对产品的隐私保护设计、隐私政策、用户隐私数据的收集与使用进行审查，确保用户的隐私数据被妥善使用和处理，并对用户保持合理的透明度。

信息安全治理组织架构

治理组织

通过系统化的信息安全治理组织与机制建设，联影可以为客户提供符合信息安全及隐私保护国际标准规范的服务。联影建立信息安全及隐私保护监督管理委员会统筹负责公司信息安全及隐私保护建设工作

联影信息安全治理组织架构



【决策层】信息安全及隐私保护管理委员会作为决策层，负责制定公司信息安全和隐私保护的战略方向及目标，研究、部署、审议公司信息安全和隐私保护工作的规划及重大事项。委员会由公司高层组成，深度参与企业安全治理工作。

【管理审计层】企业信息安全及隐私保护领导小组和产品信息安全及隐私保护领导小组共同构成管理审计层。

企业信息安全及隐私保护领导小组和产品信息安全及隐私保护领导小组分别负责企业运营、产品产研中的安全与隐私保护建设，两者相对独立又共同协作。

管理审计层负责落实公司安全战略、明确公司运营与产品安全基线、参与公司安全重大事项的讨论。结合外部环境变化与利益相关方的期望实时更新公司安全管理制度，将安全要素与公司日常运营工作和产研流程相结合，推动其落地实施。

【执行层】信息安全部、法律合规部、信息技术部、质量管理部、各业务部门的信息安全与隐私保护专员共同构成安全治理的执行层。通过规划、执行、监测、改进，实现企业运营与产品产研全过程的安全可控，确保企业安全与隐私保护政策被有效执行。联影通过自上而下推进、自下而上反馈的双线循环，确保企业信息安全与隐私保护战略与目标在得到贯彻实行的同时，不断发展与更新。

信息安全治理组织架构

人员管理

为规范员工在入职、在职、离职时的信息安全行为，减少因人为原因造成的信息安全风险，联影构建了全公司范围内的人员安全管理规定与流程，通过多种途径推动人员安全管理要求落地实施。包括但不限于：

制度约束

制定并发布《人员信息安全管理规定》明确组织在人员管理层面的安全要求

任用前背景调查

确保人员背景和经历符合职位、客户要求

签订保密协议

明确关键岗位的保密义务

明确人员管理职责分工

对于人员管理的所有关键职责，明确到最小化执行单元，确保安全要求得到实施

访问权限控制

通过审批赋权、权限复核审计、离转岗权限清理等手段确保人员权限符合最小必要原则，保障数据安全

信息安全治理组织架构

安全培训

联影为加强全体员工对信息安全及隐私数据保护的关注开展信息安全培训

安全意识培训

联影每年都会通过线上、线下讲座等方式开展信息安全意识培训，涉及办公环境安全、密码设置安全、识别和防范钓鱼邮件、保护商业秘密及差旅中的信息安全等关键内容。培训员工覆盖率达 100%

定期演练

定期开展钓鱼邮件和信息安全事件演练，提升员工信息安全意识，提高员工对信息安全攻击的警惕性，及时发现和上报各类信息安全事件

常态化审计

定期对账号弱口令开展审计并整改，部署并实施密码强度管理系统，降低因弱口令带来的安全风险

信息安全月

每年开展“信息安全月”主题宣传教育活动，邀请网络安全与隐私数据保护领域的专家举办专题讲座，提升员工对信息安全了解的积极性

信息安全与隐私保护技术建设

联影建立纵深防御（Defense-in-Depth）的安全技术体系，
提供多层安全防护

安全技术体系

数据安全防护

- 数据完整性及真实性保护
- 敏感信息匿名
- 硬盘数据加密
- 数据传输加密

应用安全防护

- 用户认证与授权
- 用户访问安全保护
- 支持紧急访问
- 应用白名单
- 审计日志
- 安全扫描

主机安全防护

- 操作系统安全加固
- 防病毒软件
- 病毒库定期更新
- 安全补丁定期更新
- 可信认证
- 密码管理系统

网络安全防护

- 防火墙
- 安全加密连接
- 网络白名单
- 网络准入机制
- 7*24 小时监控值班
- 态势感知
- 威胁情报系统

信息安全与隐私保护技术建设

信息安全事件管理流程

联影建立了信息安全事件监测与应急响应机制，持续监测与产品和运营有关的网络安全风险，响应和处理内外部的信息安全事件。

分析软件供应链和安全相关方发布的漏洞预警及安全补丁。及时响应风险并升级安全防护策略，始终与客户共同应对网络安全威胁。

网络攻防实战演练

联影积极参加各类网络安全实战演练活动，通过攻防实战检验提升网络和数据安全防护、应急处置能力，推进公司网络和数据安全保障体系建设。

2024 年，联影医疗积极参与由上海市经济和信息化委员会组织的“工赋砺网”护网行动，及由上海市通信管理局举办的“磐石行动”安全护网活动，通过模拟攻击检验，提升企业的信息安全风险防御能力。在为期一个月的 7*24 小时安全防护期间，联影医疗凭借零失分的优异成绩，荣获“工赋砺网”主办方颁发的优秀蓝方称号，充分证明联影医疗在信息安全领域的专业实力和坚固防线。

安全合规 携手共赢

联影高度重视客户的网络安全及隐私保护， 我们将通过持续保持警惕并识别不断变化的网络安全威胁，与客户共同创建网络安全和隐私安全环境。 在医疗数字化的浪潮中， 联影与客户携手共赢未来。