人工智能医疗器械创新合作平台
ARTIFICIAL INTELLIGENT MEDICAL DEVICE INNOVATION AND COOPERATION PLATFORM
CAICT 中国信通院

医疗器械数据安全白皮书
(2023 年)

人工智能医疗器械创新合作平台智能化医疗器械产业发展研究工作组

中国信息通信研究院云计算与大数据研究所

通用电气医疗投资（中国）有限公司

深圳迈瑞生物医疗电子股份有限公司

2023 年 10 月

牵头编写单位：

人工智能医疗器械创新合作平台智能化医疗器械产业发展研究工作组、中国信息通信研究院云计算与大数据研究所、通用电气医疗投资（中国）有限公司、深圳迈瑞生物医疗电子股份有限公司、上海长三角医疗装备产业促进中心、杭州安恒信息技术股份有限公司、北京智游网安科技有限公司、深圳华大智造科技股份有份公司。

参与编写单位：

四川大学华西医院、浙江大学附属第一人民医院、上海市医学装备协会、上海申康医院发展中心、上海宝信软件股份有限公司、上海交通大学附属仁济医院、上海市胸科医院、中南大学湘雅二医院、山东大学齐鲁医院、贵州医科大学附属医院、宁波大学附属第一医院、沈阳东软系统集成工程有限公司。

编写组专家：

中国信息通信研究院云计算与大数据研究所：闵栋、李曼、何友斌、李月、魏嵩磊、王凯、赵梓杰、金越、李真真、张斯琴。

通用电气医疗投资（中国）有限公司：黄立，张颖，孙旭光，钟路音，蒋杰，余柳，唐寅如，郑欢欢，孙灵瑶，柴艳秋，陈菁，上官晓清，孙丽萍，秦川。

深圳迈瑞生物医疗电子股份有限公司：张亚帅，汪胜平，吴茂敏，陈松青，薛鹏。

上海长三角医疗装备产业促进中心：张宇鸣。

杭州安恒信息技术股份有限公司：钟诚、张旭辰、张伟琦、徐立松、史坤。

北京智游网安科技有限公司：赵凯，彭浩，闫楠。

深圳华大智造科技股份有份公司：史兴，颜妙丽，苗继业，杨梦，李福斌。

四川大学华西医院：黄进、刘麒麟。

浙江大学附属第一人民医院：冯靖祎。

上海市医学装备协会：杨云。

上海申康医院发展中心：金广予、何萍、尤健、李泽宇。

上海宝信软件股份有限公司：王斌斌、陈玮。

上海交通大学附属仁济医院：张坚、张婧。

上海市胸科医院：顾伟。

山东大学齐鲁医院：刘庆。

贵州医科大学附属医院：罗松。

中南大学湘雅二医院：文劲松。

上海交通大学附属第六人民医院：郑蕴欣。

宁波大学附属第一医院：陈革、吴斌、李征、陆松筠。

沈阳东软系统集成工程有限公司：王华铎、葛长龙。

前言

数字经济时代，全球数据呈现爆发性增长趋势，数据资源已成为国家基础战略性资源和社会生产的创新要素，是决定数字经济发展水平和竞争力的核心资源。然而，数据安全形势日益严峻，高价值数据泄露、个人信息滥用情况突出，加快提升数据安全保护措施和个人信息保护能力迫在眉睫。

近年来，随着《国务院办公厅关于促进和规范健康医疗大数据应用发展的指导意见》《国务院办公厅关于促进“互联网+医疗健康”行业发展的意见》《关于深入推进“互联网+医疗健康”“五个一”服务行动的通知》等政策文件的出台，以及大数据、人工智能等新型技术的发展，健康医疗数据应用、“互联网+医疗健康”和智慧医疗迎来蓬勃发展，新的业务形态不断出现。与此同时，各类新型技术、应用的出现使得医疗行业数据安全治理面临越来越多的挑战。医疗数据天然的敏感性决定了有关方面必须采取有效措施来应对数据安全合规风险和各类内外部风险。

伴随着医疗信息化、智慧医疗的发展，具备网络连接功能以实现电子数据交换或远程控制的医疗器械种类及数量日益增多，互联网可以改善医疗服务，但是相应地也会面对网络安全风险。和其他的计算机系统一样，医疗器械也容易受到安全漏洞的影响。因此在提升诊断效率与质量的同时，带来了遭受网络攻击的风险，医疗器械网络安全逐渐成为国家必须面对的重要问题。

需要说明的是，本文是针对现阶段的行业发展现状总结形成，以

供参考，对于内容中的差错与不足，烦请各界批评指正，我们将充分采纳和吸收各方面的宝贵意见和建议，进一步深入相关研究，持续完善相关内容，并以适当的方式向社会公布。

目 录

第一章 医疗器械数据安全发展概况

一、医疗器械数据概念

根据2022年3月国家药品监督管理局发布的《医疗器械网络安全注册审查指导原则（2022年修订版）》定义，医疗器械中的数据可分为医疗数据和设备数据。医疗数据是指医疗器械所产生的、使用的与医疗活动相关的数据（含日志），从个人信息保护角度又可分为敏感医疗数据、非敏感医疗数据，其中敏感医疗数据是指含有个人信息的医疗数据，反之即为非敏感医疗数据。个人信息是指以电子或者其他方式记录的能够单独或者与其他信息结合识别特定自然人身份或者活动情况的各种信息。如自然人的姓名、出生日期、身份证件号码、个人生物识别信息（含容貌信息）、住址、电话号码等。设备数据是指记录医疗器械运行状况的数据（含日志），用于监视、控制医疗器械运行或者医疗器械的维护与升级，不得含有个人信息。

注册申请人需基于医疗器械相关数据的类型、功能、用途，结合网络安全特性考虑医疗器械网络安全要求。同时，保证敏感医疗数据所含个人信息免于泄露、滥用和篡改，以及医疗数据和设备数据的有效隔离（如访问权限控制等方法）。

医疗器械数据还包括医疗器械研发、产品生产、运输、经营管理、产品使用、产品售后以及相关产业链上中下游等信息。包括但不限于设计图纸，零部件清单、设计软件、客户订单、制造工艺、售后资料等。

医疗数据一是因其数据价值高、敏感程度高、数据体积大、覆盖

范围广、应用场景杂等特点，针对医疗数据的窃取活动呈明显增加趋势，相关数据安全事件频发；二是伴随着网络技术的发展与业务数字化转型的深入，医疗数据逐步从以往局限于内网中使用向外网、云平台等处流通应用，相关数据安全风险进一步增加。

二、医疗器械信息化发展历程

时间	里程碑
1980S	以微处理器为核心的智能仪器（如自动化生化分析仪、血球计数器、免疫分析仪等）进入临床实验室
2000S	医疗信息化开始逐步推进，包括医院管理信息化、医疗设备信息化
2010S	新医改”强调信息化的支柱地位，医疗信息化迎来新一轮发展高峰。
2018-至今	人工智能、大数据等新型技术引入，医疗器械数据安全新高度

三、医疗器械数据安全需求背景与现状

近年来，信息技术与卫生健康行业深度融合，医疗数据体量越来越大。医疗数据是产生于医疗机构诊疗活动关于患者的生理和健康状况的数据。作为电子化信息本身，这些来自广大地理范围内的各类感知数据不可避免地蕴含着患者的大量时间和空间信息，其敏感性较高，一旦泄露可能影响患者个人隐私保护、医疗行业发展乃至国家卫生安全。因此，医疗数据安全至关重要。其中，医疗器械数据作为医疗数据的范畴之一，更值得重视和关注。2022 年 3 月，国家卫生健康委发布《国家三级公立医院绩效考核操作手册（2022 版）》，对大型医疗器械指标进行了修订，进一步强调医疗器械网络安全。

医疗器械是医疗卫生机构资产构成的重要组成部分，也是临床科室完成正常医疗诊治的重要保障。在医改处于攻坚阶段的形势下，大型公立医院虹吸现象仍然客观存在，院内医疗器械均高负荷运转。据调查分析，某医院每台 PET-CT 设备的年均治疗人次达 6000 以上，彩

超机多达 1.5 万人次，产生大量医疗数据。然而，在医疗器械管理领域，针对数据安全的重视程度亟待加强。部分医疗器械仍存在不同程度连接互联网和开启远程控制的现象，尤其很多医疗器械为进口，通过跨境服务器可能导致医疗数据出境，具有较高安全隐患。

3.1 医疗器械网络安全事件频发，引发数据泄露担忧

伴随着医疗信息化、智慧医疗的发展，医疗设备种类及数量日益增多，医疗设备网络安全逐渐成为国家必须面对的重要问题。

2019 年 3 月，某品牌心脏除颤仪所使用的 Conexus 无线遥测协议存在网络安全漏洞，未使用加密、身份验证或授权，可能导致未经授权的个人访问并操纵可植入设备。

2019 年 6 月，某品牌部分型号及版本的胰岛素泵存在潜在的网络安全风险，攻击者可以通过更改胰岛素泵设置的手段，向患者过度输送胰岛素或停止输送胰岛素，导致高血糖和糖尿病酮症酸中毒。

2019 年 7 月，美国国土安全部下属的网络安全和基础设施安全局发布了一份名为《URGENT/11》的网络安全漏洞公告，该公告中记录了由相关安全研究人员在当时使用最为广泛的嵌入式设备实时操作系统 VxWorks 中所发现的 11 个高危漏洞。同年 10 月，美国食品药品监督管理局向患者、医疗器械厂商及相关工作人员通报了该漏洞，该漏洞与在医疗器械中广泛使用的第三方通信组件 IPnet 有关，可导致攻击者在没有用户交互的情况下征用医疗器械，并更改或禁用其相关的功能，主要受影响的医疗器械包含影像系统，输液泵和麻醉机等。

2022 年 6 月，某基因测序仪的本地运行管理软件存在网络安全漏

洞，可以实现对基因测序仪进行远程控制外，还可以影响患者的临床测序结果，从而导致诊断过程中的结果被篡改。

3.2 医疗数据形式多样、数据种类繁杂，用途多样，管控难度加大

医疗器械种类众多，增长迅速。一方面，医疗器械信息化水平相较其他行业存在一定差距，在设计之初缺乏安全考虑，自身安全防护能力薄弱，一旦攻击者接入医疗卫生机构内部网络，医疗器械数据极易泄露或被篡改。另一方面，医疗器械种类与数量都有大幅增长，医疗设备接入医疗机构网络内，连接条件、连接方式、数据类型多种多样，传统数据防护工具无法满足现有医疗环境下数据安全需求，治理难度加大。

医疗器械防护能力较差。医疗器械主要为满足医疗环境下检验检测与治疗需求。因此，医疗器械一般优先满足可靠性、可用性需求，避免了因医疗器械故障造成的安全事故和损失。但在计算、存储、系统以及网络等资源方面存在一定限制，无法部署安装传统网络和数据安全防护工具，容易遭受恶意入侵。

安全建设能力不足，数据安全建设处于起步阶段。在过去的十多年时间，医疗卫生机构已建立以网络安全等级保护定级为基础，围绕制度、组织、人员、建设、运维等安全管理措施，构建了一体化网络安全保障体系。在边界网络防护、攻击风险监测、防病毒、身份认证等方向建设投入大量精力，建设成果丰硕。但在数据安全上，整体来看，尚处于起步阶段，距离《个人信息保护法》《数据安全法》等相关法律要求还有一定差距。

3.3 医疗数据价值日益凸显，数字经济发展进入快车道

随着大数据、人工智能、区块链、云计算等新技术和医疗器械产业快速发展与融合，为传统医疗体系的变革提供契机。可穿戴设备为个人健康提供动态实时监测，助力疾病预防和诊后管理；人工智能技术为医疗诊治效果分析、影像分析以及疾病康复提供了精准支持。

数字医疗规模增长迅速，随着我国人民生活水平提高、人口老龄化不断加剧和居民健康管理意识的增强，我国医疗和健康服务需求不断提高，海量化的数据正呈现爆发式、几何式的增长，数据湖、主数据管理等数据关键技术将逐步规模化应用正在驱动整个医学的发展。我国医疗健康大数据产业规模不断扩大，从 2015 年的 18.67 亿元增长至 2021 年的 212.56 亿元，年均复合增长率约为 50%，初步统计 2022 年我国医疗大数据的市场规模约增加至 301.36 亿元。

数据安全已成为我国总体国家安全的重要组成部分。数据是经济发展的重要生产要素和核心引擎，是开展医疗数字化的关键。《关于构建数据基础制度更好发挥数据要素作用的意见》《数字中国建设整体布局规划》《“十四五”数字经济发展规划》《关于进一步完善医疗卫生服务体系的意见》《关于促进“互联网+医疗健康”发展的意见》等政策文件相继布局数字医疗产业发展，不断加大对数字基础设施的投资，数字医疗产业加速增长。

四、医疗器械数据应用场景

随着人们的健康保护意识不断提升，各种医疗健康设备也不断走向大众视野，根据医疗器械的用途和性质，可将目前医疗器械发展较

快，潜力较大的八类细分领域进行研究：影像设备、体外诊断、监护设备、家用医疗器械、可穿戴设备、高值耗材、口腔设备、医用机器人。

医疗器械重点领域	
类别	主要产品
影像设备	CT、核磁、超声、DR 血管造影机、乳腺机、胃肠机等
体外诊断	基因测序仪、生化分析仪、时间分辨荧光检测仪、酶标仪，和各类配套诊断试剂
监护设备	多参数监护仪、心电监护仪等
家用医疗器械	体温计、氧气囊、轮椅、血糖仪、血压计、急救箱等家用器械
智能可穿戴设备	智能眼镜、智能手表、智能腕带、智能跑鞋、智能戒指、智能腰带、智能头盔等
高值耗材	血管介入类、消化道介入类、骨科植入、颅内植入、起搏器等
口腔设备	口腔综合治疗设备、牙钻机及配件、牙科椅、补牙设备等
医用机器人	手术机器人、外骨骼机器人等

资料来源：九次方大数据研究院

基于医疗器械数据在不同角色之间的流转，可以将以上八大细分领域的医疗器械数据应用安全场景分为以下几类：

4.1 互联互通数据安全

医院等医疗机构为实现跨机构、跨地域的健康诊疗信息交互、共享和医疗服务协同，需要在各医疗机构、医联体信息平台之间实现数据（电子病历、电子健康档案等）的互联互通与信息共享。

在此场景下，医院的医护人员、卫生机构管理人员、医院间联合体及医疗第三方服务机构人员在对相关系统文件、数据库资料以及医疗器械等敏感数据进行访问浏览，以及通过内部信息共享交换系统进行文件数据传输、存储等操作时，均可能导致医患隐私等重要信息面临泄露风险。

4.2 远程医疗数据安全

一方医疗机构为邀请其他医疗机构对其诊疗患者提供技术支持等

医疗活动时，需要运用通讯、计算机及相关网络技术手段，过程中涉及近端/远端医院、患者，以及远程诊疗设备提供者、设备维护管理者、远程诊疗信息发布平台服务提供商、网络运营商等第三方参与。

在此场景下，近端医院需向远端医院出示患者的检验报告、诊断结果、用药信息、既往病史、家族病史、传染病史等涉及患者隐私的个人健康医疗信息。如果远程诊疗网络出现被不明身份人员接入、相关服务器和终端存在病毒或漏洞等问题，则数据在远程诊疗过程中将面临由非法接入、漏洞攻击、病毒感染等导致的敏感数据被非法访问、窃取篡改、恶意上传等风险。

4.3 汇聚中心数据安全

汇聚中心是指区域卫生信息平台、健康医疗大数据中心、学会数据中心、医院内部数据中心等为医生、患者、第三方的“诊疗参考、健康管理、分析利用”相关需求提供数据应用支撑的平台机构。

在此场景下，汇聚中心涉及跨机构数据汇聚，集中存储着包括基本人口学数据、病历数据、健康档案数据等大量数据信息，A 医院医生会通过汇聚中心调阅某患者在 B 医院就诊时的健康医疗信息。如果没有建立对中心数据分级标注以及颗粒度匹配等机制，将面临非法登录、越权访问、异常调阅、冒名查询、批量窃取、明文泄露等数据安全风险。

4.4 健康传感数据安全

健康传感数据是指通过健康传感器收集的如个人身份信息、生活方式等与被采集者个人属性及健康状况相关的数据，主要应用于健康

监测、慢性疾病的治疗、康复护理等领域。一般是具备传感、无线通信等功能的、可直接穿戴在身上的医疗或者健康电子设备，通过软件，可以实现感知、记录、分析、调控、干预佩戴者的健康状态等功能。

在使用的过程中可能涉及对个人数据的处理。例如远程监护，利用健康传感器实时、持续地监测患者的生命体征，再将获取到的数据传送给医护人员，医护人员通过获取的信息可以及时对患者的情况进行判断与处理。在此过程中，会对患者的生命体征数据进行采集、计算和传输。

在此场景下，健康传感数据在采集、存储、使用阶段均存在着不同的安全隐患，应评估各个阶段的安全风险并针对安全风险建立安全防护手段以保证健康传感数据的安全。

4.5 移动应用数据安全

移动应用数据是指通过网络技术为个人提供的在线健康医疗服务（如在线问诊、在线处方）或健康医疗信息服务应用（如个人电子健康档案）中设涉及的个人属性数据、健康状况数据、医疗应用数据、医疗资金和支付数据、卫生资源数据以及公共卫生信息。

在此场景下，用户的隐私信息可能在经应用界面对外展示环节面临数据泄露风险；用户手机丢失、被窃后，其移动应用登录密码设置如过于简单，应用内数据可能被非授权人员登录浏览、截屏导致隐私信息泄露；同时，与应用程序相关的信息系统，因与大量移动设备进行数据传输，亦可能经移动端感染病毒或被植入恶意程序。

4.6 临床研究数据安全

临床研究数据一般是指由医院、学术研究机构和医疗企业发起的，以确认药物、医疗器械、医疗信息系统、诊断和治疗的安全性和有效性为目的的研究中，所涉及的基本人口学资料、检查信息、检验信息、药品医嘱、诊断信息、病例及患者报告等信息。

在此场景下，参与临床研究的医患及有关信息，在通过专线、互联网线路、VPN 等链路进行传输，被临床试验电子系统的用户进行访问或被交由医疗机构进行存储和使用等过程中面临诸多数据安全风险。

4.7 商保对接数据安全

商业保险公司通过与医疗机构建立连接的医疗信息系统，及时掌握个人健康医疗信息主体的诊疗情况及发生的相关费用信息，例如：个人属性信息、健康状况信息、医疗应用信息、医疗资金与支付信息、卫生资源信息等数据，从而根据商业保险机构的核赔规则自动进行支付结算等理赔业务。

在此场景下，投保用户的健康医疗信息将由医疗结构向商业保险机构进行披露，因而在系统对接、数据传输、数据使用、数据存储、数据销毁等环节面临安全风险。如果双方在数据对接的前、中、后三个阶段中，没有形成具有法律约束性的、权责分明的正式协议，没有建立起有效的数据管理机制，则可能导致商保对接数据的泄露。

4.8 器械维护数据安全

医疗器械维护的目标是确保器械安全、有效和功能正常。不同的医疗器械可能涉及不同的数据，影像系统可能涉及病人的影像和影像

诊断报告，检验系统可能涉及病人的检验、检查报告及检验结果；此外，需保存的器械维护历史记录包括：维护的内容、维护的原因、维护的时间、维护的操作人员等信息。

在此场景下，医疗器械厂商在进行远程维护时，可能会读取器械的维护记录和日志报告，用以分析医疗器械失败原因；也可能读取医疗器械产生的数据，用以分析应用的安全性和有效性。在以上流程中，数据将面临非授权访问、不安全链接、隐私数据泄露、维护记录保存不当等安全风险。

根据医疗器械的具体应用场景的不同，梳理了医疗器械中采集、处理数据需要注意的合规要点，通过医疗器械采集和处理患者信息需要获取个人同意，如涉及个人敏感信息，还应遵守《个保法》其他相关规定；医疗器械在远程维护时要做到设备数据和医疗数据的有效隔离以及个人信息去标识化；医疗器械中的医疗数据如涉及出境，须注意本地化存储和进行安全评估审核。

五、医疗器械数据价值日益显著

当前，随着医疗数据价值的日益提升，医疗器械行业对患者数据的采集、合并与分析能力不断进步，包括机器学习能力在内的人工智能技术快速发展，数字医疗软件逐渐成为许多医疗器械产品的重要组件。然而，由于医疗器械数据具有高度敏感性，且许多医疗器械厂商提供患者数据收集、存储与分析等服务， 2021 年 11 月，工业和信息化部、国家卫生健康委、国家发展改革委等 10 个部门联合发布《“十四五”医疗装备产业发展规划》（下称“规划”）。《规划》特别指

出，医疗装备发展要统筹发展和安全，坚持安全第一的基本原则，将安全生产、产品质量作为发展生命线，利用各种安全技术提升产品安全防护能力、信息数据安全保护能力，筑牢风险防范的屏障和堤坝。2022 年 2 月工信部发布《“十四五”医药工业发展规划》提出“医疗器械是关系国计民生、经济发展和国家安全的战略性产业，是健康中国建设的重要基础。”2022 年 3 月，国家药监局发布《医疗器械网络安全注册审查指导原则（2022 年修订版）》。该指导原则重点关注医疗器械产品全生命周期过程中网络安全问题，包括医疗器械产品的设计开发、生产、分销、部署和维护。其中明确指出，医疗器械安全出现问题不仅会侵犯患者的隐私，而且可能会产生医疗器械非预期运行的风险，导至患者或使用者受到伤害或死亡。2022 年 8 月，国家卫生健康委、国家中医药局、国家疾控局联合发布《医疗卫生机构网络安全管理办法》，这个管理办法贯穿了全生命周期管理的主导思想，强调医疗卫生机构安全管理应围绕着顶层设计和制度保障两个要点着力推进。要求建立网络安全管理的制度体系，加强网络安全防护，通过管理和技术手段保障数据安全和数据应用的有效平衡。2022 年 11 月，国家卫生健康委联合国家中医药局、国家疾控局共同印发《“十四五”全民健康信息化规划》，提出加强医疗设备相关网络和数据安全监管，全面落实网络安全管理要求，不断深化在行业治理、智能医疗设备等领域的创新应用。

第二章 全球医疗器械数据安全政策

目前世界各国已针对医疗器械数据安全进行研究，各国监管机构也相继发布一系列政策指导文件，对医疗器械数据安全进行引导和规范。

一、中国数据战略

随着《网络安全法》《数据安全法》《个人信息保护法》以及《关键信息基础设施安全保护条例》等一系列法律法规和标准的出台，党中央、国务院及医疗监管部门相继发布一系列政策指导文件，逐步完善医疗器械网络安全与数据安全体系。

2017 年 1 月国家食品药品监督管理总局（NMPA）发布了《医疗器械网络安全注册技术审查指导原则》，将《中华人民共和国网络安全法》的基本原则应用到了医疗器械领域。自 2018 年起，制造商应根据医疗器械产品特性提交网络安全注册申报资料。制造商应当结合医疗器械产品的预期用途、使用环境和核心功能以及相连设备或系统（如其它医疗器械、信息技术设备）的情况来确定医疗器械产品的网络安全特性，并采用基于风险管理的方法来保证医疗器械产品的网络安全。

2019 年，为进一步加强医疗器械全生命周期的监督管理，创新新模式，国家药监局制定了《医疗器械唯一标识系统规则》（下称“规则”）。《规则》明确了医疗器械唯一标识系统建设的目的、适用对象、建设原则、各方职责和有关要求，由医疗器械唯一标识、唯一标识数据载体和唯一标识数据库组成。医疗器械唯一标识是指在医疗器械产品或者包装上附载的，由数字、字母或者符号组成的代码，用于

对医疗器械进行唯一性识别；医疗器械唯一标识数据载体是指存储或者传输医疗器械唯一标识的数据媒介；医疗器械唯一标识数据库是指存储医疗器械唯一标识的产品标识与关联信息的数据库。《规则》提出，医疗器械唯一标识数据载体应当满足自动识别和数据采集技术以及人工识读的要求。如空间有限或者使用受限，应当优先采用符合自动识别和数据采集技术的载体形式。随着《规则》的发布实施，建立唯一标识系统有利于实现监管数据和共享，创新监管模式，提升监管效能，加强医疗器械全生命周期管理，净化市场、优化营商环境，实现政府监管与社会治理相结合，形成社会共治的局面，助力产业转型升级和健康发展，提升医疗器械管理水平和效能，有力保障公众用械安全有效。

随后2022年，国家药监局器审中心组织制定了《医疗器械网络安全注册审查指导原则(2022年修订版)》。新修订的医疗器械网络安全指导原则针对网络安全概念进行了梳理，重点对网络安全应急响应、网络安全更新、全生命周期质控、数据出境、软件维护与升级、自研软件安全评估与管理等进行修订。

2022年8月，国家卫生健康委、国家中医药局、国家疾控局联合发布《医疗卫生机构网络安全管理办法》，这个管理办法贯穿了全生命周期管理的主导思想，强调医疗卫生机构安全管理应围绕着顶层设计和制度保障两个要点着力推进。要求建立网络安全管理的制度体系，加强网络安全防护，通过管理和技术手段保障数据安全和数据应用的有效平衡。

2022 年 11 月，国家卫生健康委联合国家中医药局、国家疾控局共同印发《“十四五”全民健康信息化规划》，提出加强医疗器械相关网络安全和数据安全监管要求，全面落实网络安全管理要求，不断深化在行业治理、智能医疗器械等领域的创新应用。

文件号	文件名称	发行年份
2017 年第 13 号	医疗器械网络安全注册技术审查指导原则	2017 年 1 月 20 日
2019 年第 66 号	医疗器械唯一标识系统规则	2019 年 8 月 26 日
2022 年第 7 号	医疗器械网络安全注册审查指导原则(2022 年修订版)	2022 年 3 月 7 日
国卫规划发〔2022〕29 号	医疗卫生机构网络安全管理办法	2022 年 8 月 8 日
国卫规划发〔2022〕30 号	“十四五”全民健康信息化规划	2022 年 11 月 7 日

二、美国数据战略

美国 FDA（美国食品药品监管局）是医疗器械网络安全政策制定方面的先驱，发表了这个领域内的第一篇指南也是第一个对器械上市前网络安全管理提出要求的监管机构，它的指南文件“Content of Premarket Submissions for Management of Cybersecurity in Medical Devices”也被很多国家参考。此份指南性文件向行业提供关于网络安全设备设计、标签及 FDA 为可能存在网络安全风险的设备在上市前申报文件中需要体现的建议性内容。FDA 第一次提出了“网络安全物料清单”（CSBOM）的概念，将其定义为可能易受网络安全风险影响的商业，开源和现成软件和硬件列表，认为这可能成为安全漏洞识别工作中的关键性因素，所以在上市前申报文档之中必须包括此安全物料清单。制造商应该利用 CSBOM 更精确的来实施网络安全风险管理流程，以识别其设备，软件和系统的哪些组件更容易受到网络事件或攻击的影响。FDA 将其网络安全要求与美国国家标准技术研究院（NIST）的网络安全

框架紧密联系在一起，后者是全球公认的框架，为制造商提供了公认的风险和影响评估工具，以确定网络安全风险和脆弱性。在 2016 年发布的 Postmarket Management of Cybersecurity in Medical Devices 指南中不仅囊括了新医疗器械和产品，也把上市后和临床上应用的医疗器械纳入其中，即:要求制造商、供应商有能力及时鉴别和处理网络安全所带来的各种技术问题，建立网络安全共管系统，更好地研究新对策和开发新方法。指南还引入了很多新的概念如补偿控制，受控/非受控风险和网络安全预警信号等。此外它还介绍了威胁建模的概念并参考 AAMI TIR57 扩展了有关安全风险管理的建议。在医疗器械产品中网络漏洞的披露和处理上，FDA 鼓励生产商采取自由裁量权，前提是生产商需要遵循 21 CFR part 806 的规定以及 H-ISAC 对于信息披露的指南文件。

文件号	文件名称	中文名称	发布日期
FDA-2020-D-0957	FDA,Guidance for Industry: Cybersecurity for Networked Medical Devices Containing Off-The-Shelf (OTS) Software	行业指南-包含现成（OTS）软件的网络医疗器械的网络安全	2005 年 1 月 14 日
FDA-2013-D-0616	Content of Premarket Submissions for Management of Cybersecurity in Medical Devices	医疗器械网络安全管理上市前提交的内容	2014 年 10 月 2 日
FDA-2015-D-5105	Postmarket Management of Cybersecurity in Medical Devices	医疗器械网络安全上市后管理	2016 年 12 月 28 日
FDA-2021-D-1158	Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions	医疗器械网络安全指南	2022 年 4 月 8 日

三、欧盟数据战略

2017 年 5 月 5 日,欧盟医疗器械法规(REGULATION (EU) 2017/745,

简称 MDR）正式发布，并于 2017 年 5 月 26 日正式

生效。欧盟委员会于 2020 年 4 月 17 日通过关于 MDR 实施日期推迟一年的建议，MDR 生效日期推迟至 2021 年 5 月 26 日。2017 年 5 月 5 日欧盟体外诊断医疗器械法规（IVDR）正式发布，于 2017 年 5 月 25 日正式生效，并于 2022 年 5 月 26 日实施。自实施之日起，IVDR 将取代原欧盟体外诊断设备指令（IVDD）。

欧洲医疗器械协调小组（MDCG）于 2019 年 12 月颁布了 MDCG 2019-16 指导原则“Guidance on Cybersecurity for Medical Devices”，该指导原则旨在就如何满足 MDR 和 IVDR 附件 I 关于网络安全的所有相关基本要求向制造商提供指导。MDCG 的指导原则与其他指南文件的不同之处在于，它是由所有成员国一起撰写，根据 MDR 和 IVDR 法规，欧盟市场上投放的医疗器械需确保满足网络安全风险相关的技术挑战的新要求。因此，提出了针对含电子编程系统和软件（本身就是医疗器械）的医疗器械新的基本安全要求。制造商需要按照要求在考虑风险管理原则（包括信息安全性）的同时，根据最新技术开发和制造其产品，并就 IT 安全措施（包括防止未经授权的访问）制定有关的最低要求。指导原则涵盖了上市前和上市后网络安全的要求，并概述了与每个类别相对应的活动。文中提到一些重要的网络安全要求在 MDR 中并未明确表述，尤其是与医疗器械使用相关的数据的隐私和机密性，这些要求需要与其他法规，如通用数据保护条例（GDPR）一起考虑。我们熟知 ISO 14971 是对单个医疗器械风险管理的指导，它提出了一个概念叫“合理可预见的滥用”，规定了制造商应在合理可预见的情况

下评估风险，而对于涉及网络安全的风险，制造商更要考虑这些风险会不会被作为恶意攻击的对象，概率大小。指南的第三部分着眼于设计控制和生产过程，其中产品设计控制，需要考虑充分实现“设计安全”和“纵深防御”的理念，制造商可以参考工业界被广泛运用的 IEC 62443 系列标准和 IEC/ISO TR 80001-2-2。另一个对于实现网络安全至关重要的方面是风险控制，在指南的 3.5 章节、MDR Annex I 都有详细的说明，医疗器械网络风险管理的对象是整个医疗 IT 网络，当制造商在进行风险-收益分析时候，一定要合理的平衡安全性、有效性、网络信息安全性，需要在它们之间作出取舍时，应以病人利益为核心进行优先级的安排，即安全性具有最高优先级，有效性次之，信息安全再次。指南的 3.6 章节规范了生产商 IT 系统最低配置要求，这与 MDR Annex I 中针对 IT 环境设置的要求一致，包括了明确系统整体需求，设立对硬件设施，网络环境和安全措施的要求。对比美国和欧盟针对网络安全的要求，FDA 监管深入到产品级，要求制造商根据风险对产品组成部分划分不同风险级别，属于主动防御，而欧盟相对要宽泛，属被动防御。

文件号	文件名称	中文名称	发行年份
法规 2017/745	Medical Devices (MDR): Regulation (EU) 2017/745	欧盟医疗器械法规	2017 年 5 月 26 日
法规 2017/746	In-vitro-Diagnostic Medical Device Regulation (IVDR): Regulation (EU) 2017/746	欧盟体外诊断医疗器械	2017 年 5 月 5 日
MDCG 2019-16	MDCG 2019-16 Guidance on Cybersecurity for medical devices	医疗器械网络安全指南	2019 年 12 月

第三章 医疗器械数据安全存在风险和挑战

随着技术发展，医疗器械联网设备激增，分布广泛，应用场景多样，并展露出类型多、型号多、远程运维方式多的“三多”趋势，直接导致安全风险暴露面的增加，原有的安全手段难以应对，由此引发的医疗网络安全风险和挑战与日俱增，主要体现在几个方面：

一、医疗器械数据安全治理尚在初期

经过等保的推动和落地，大部分医院系统都具有明确的网络安全规范要求，依赖于等保评估的网络安全整改，医院在宏观系统的网络防护层面建设相对成熟。

但聚焦于医疗器械场景下，目前现有的医疗器械网络安全防护体系主要参考《指导原则》，但基于《指导原则》中针对医疗器械网络安全能力建设，仅给出22种网络安全能力的简要说明，尚未明确与医疗器械（类别：一类、二类、三类）风险等级（低、中、较高）相匹配的网络安全能力建设标准，再加上部分医疗器械厂商关注业务正常运行的考量而忽略其网络安全能力的建设，导致医疗器械在初期设计研发中缺少实现数据保护功能的相应组件，尤其是在数据存储机密性和传输机密性等方面，缺乏相对应的安全防护机制。

同时，医疗器械数据安全缺少能够贯穿整体数据生命周期的管理规程和标准，相应的数据安全监管措施无法得到落实，考核体系也无从建立，距离建立符合《个人信息保护法》、《数据安全法》以及《网络数据安全管理条例（征求意见稿）》的成熟数据安全体系还相差甚远。

二、医疗器械采集的数据具有临床性质

区别于日常网络系统的数据安全治理，医疗器械往往存储着大量的患者个人信息（如身份证号、医保卡号、家庭住址、银行卡号等）以及医生数据诊疗信息（病症处方、检验结果）等医疗数据，同时医疗器械数据还具有其独特的临床性质，即大部分医疗器械中存储着检查、检验过程中具体的化学药物用量或相关设备数据，该部分数据直接作用或间接影响着医生的实际诊疗过程。

因此，如果医疗器械未能做到有效的数据安全防护，从而导致敏感信息泄露，不仅仅会造成医患信息泄露，对患者的个人隐私保护造成侵害，同时还有可能影响到医疗器械本身的使用，即攻击者通过特殊手段恶意篡改医疗器械底层数据，导致其无法正常运行，更有甚至会直接影响医院的正常运作。

三、医疗器械数据传输缺少足够的机密性保护

数据传输本质上就是数据从一个实体传输到另一个实体上的过程，由于目前远程医疗服务、互联网诊疗服务等医疗卫生服务新模式、新业态的发展，越来越多的医疗器械可以通过包括以太网通信方式、蓝牙、串口通信方式等多种渠道完成数据的远程传输。

由于传输方式的种类较多，部分医疗器械在其使用前并未针对其数据传输接口开展必要的渗透测试、漏洞扫描等工作，导致其上线后不具备数据传输的完整性、机密性和可用性的安全保障，可能会导致以下风险：

1、额外端口或服务的透出：部分医疗器械在生产过程中会预留端

口或服务用于相关组件的开发或测试，而在医疗器械上线使用之后，该部分端口仍然继续保持开放，此类端口可能会被作为攻击入口进行恶意渗透，进而控制整个医疗器械。

2、未进行严格的双边身份认证：部分医疗器械厂商自行研发协议进行数据交互，而其中一些协议可能不具备严格的双边身份认证流程，无法确保数据交互的双方是完全可信的，从而扩大数据泄露的风险。

3、敏感数据未加密传输：医疗器械在传输敏感数据时如果未采用有效的加密方案，则会让医患敏感数据直接明文“裸露”在外。

4、医院内网与互联网交叉使用导致无法形成有效的内网隔离：部分医疗器械在涉及到医院内网数据交互与互联网数据交互时，未采用有效的控制方式进行内外网数据传输模式的隔离，导致医院内网环境暴露在外，进而影响整个医院内网环境的网络安全。

四、医疗器械数据的存储缺乏明确规范

医疗器械从大类上可以分为诊断设备类、治疗设备类和辅助设备类，具体细分可涵盖影像类、检验类、窥镜类、激光类、手术类、辅助治疗类等几十个小类，医疗器械涉及到的数据又可以进一步划分为结构化数据、半结构化数据和非结构化数据。在不同的场景下，所涉及到的医疗器械数据的种类也各不相同，如病历相关医疗器械多存储为数据库中的结构化数据、以 XML 格式为主的半结构化数据以及 PACS 系统上存储的 DICOM 非结构化医学影响文件数据。

由于医疗器械的种类繁多，同时缺少明确的管理规范，因此很多医疗器械缺少统一的梳理，大部分医院不具备医疗器械的数据资产表，

对于医疗器械资产的统计具有滞后性，往往在其发生数量、种类的变化后，无法准确得到相关的信息，进而无法对新增医疗器械进行实时的感知，从而导致无法对其分发对应的责任人、存储空间位置、访问日志记录等，使其游离在网络安全管理体系范围之外。

同时，目前大部分医疗器械及其业务的运维、安全能力多依赖于外部厂商，而由于未能存储相关运维人员的访问行为、操作审计记录，导致医院及相关技术人员无法第一时间通过异常行为流量判断是否为正常业务交互，可能会出现外部厂商的运维人员监守自盗，恶意窃取医疗器械中存在的敏感数据。

五、医疗器械使用时安全意识薄弱

医院中涉及到的医疗器械的种类和数量均较多，关联的科室、部门和人员更为繁杂。相关资料和案例统计显示，很多安全事件的发生都是由于人为因素，缺少对工作人员以及相关医院机构安全教育的普及。

例如医疗器械厂商在设置医疗器械初始化时，多数默认系统账号的密码安全性较低，部分系统未强制要求使用人员更改初始密码，导致很多系统管理员账号密码仅为简单数字组合，除此之外，部分医院相关部门管理人员为了方便使用，未设置复杂度较高的密码，甚至将用户名和密码以明文便利贴的形式贴在公共工作区域，还市场出现医疗器械主机未上锁或钥匙未妥善保存的场景，很容易被有心之人通过暴力破解、物理破解等方式进行攻击，相关部门管理人员网络安全意识的不到位，则造成了很多线下数据泄露事件的发生。

再从医院对于医疗器械使用的整体体系来看，多数医院对于医疗器

械的网络安全方面并不重视，没有有效的医疗器械数据使用安全策略和操作流程；医疗器械归属设备、医工等部门管理疏忽数据安全，管理侧重点在于医疗器械的应用与质量控制；信息中心对医疗器械未进行管理，医院整体缺少对医疗器械的统一集中管控，故针对医疗器械的网络安全防护尤其是医疗器械的数据防护，或缺少安全管控或已有传统的网络安全设备存在防护“盲区”，无法有效精准地识别到医疗器械数据中所携带的病毒攻击等，甚至有些医院中设置具有高权限的特权账号，却并未对其进行使用、访问的限制，造成特权账号的滥用，从而导致数据的泄露。

六、医疗器械数据委托处理缺少有效隔离措施

数据委托处理指的是由于医疗器械本身及其业务运维的必要性，需要将其中涉及到的设备数据回传给第三方外部厂商的动作。由于医疗器械本身需要定期进行系统性的运维，再加上目前大部分 CT、核磁设备供应商均为国外厂商，故此需要通过远程运维交互的方式传输相关的数据。如果医疗器械在投入使用之前未能进行有效的隔离检查，则可能会出现患者数据未经有效的加密手段直接与设备数据混用的场景，从而导致大量患者数据随同设备数据流入到国外厂商所属的服务器上，未采用有效隔离的数据混合也会对后续安全风险的溯源造成极大的阻碍。

第四章 医疗器械数据安全发展规划

一、建立医疗器械数据安全管理体系

随着云计算、5G、物联网、人工智能等创新技术的发展，数据向云、网、端等应用场景不断延伸，数据跨网络边界、业务部门的流转成为常态，单点的安全防护手段缺乏协调联动能力，安全策略全面性弱、一致性差、管控效率低，难以发挥贯穿数据处理全流程的整体防护能力。在国家《“十四五”数字经济发展规划》的不断推进下，为实现大规模的数据共享和业务协同，数据安全必须与业务进行体系化融合，实现全场景、全流程、全链路的安全保障，通过统一的管控平台，推进产品、技术和管理的协同治理，形成数据安全综合治理体系。

1.1 建立数据安全组织架构

依据数据安全相关法律法规、标准规范等国家和行业合规要求，结合医疗卫生机构与医疗器械厂商的数据安全现状，规划、构建统一的协调、沟通、管理机制，设立决策小组、管理小组、执行小组、监督小组四层组织架构。各团队职责划分清晰，推进相关制度文件的落地执行，并形成考核评价机制。同时，可将医疗器械数据安全管理制度分设 4 级，便于后续统一管理。制度的定制可设为战略类、数据生命周期管理类、通用管理三大类，按需建设、补充，针对管理制度体系完善对应管控流程建设。

1.2 健全数据安全管理制度

为了加强数据的保密管理，保障数据的完整性和可用性，规范数据的合法使用和交换，医疗卫生机构与医疗器械厂商都应建立健全数

据安全管理制度，责任到人，提升整体安全意识，强化责任分工，使医疗器械厂商相关人员有规可守将监管方式分为自检、抽检和巡检，提高监管频率，严查一切违反安全规定的行为。最后，医疗卫生机构应增加数据安全建设预算和投入，建立信息安全保障平台，构筑计算机网络安全环境，确保医疗器械的安全正常运行，防止恶意软件或病毒漏洞感染。针对医疗器械备数据安全，使用科室相关人员均应签署医疗器械网络与数据安全协议，明确未经审批授权不得擅自接入介质、终端或导出数据，并建立相关责任追究制度。

在数据安全建设中，医疗卫生机构与医疗器械厂家需梳理数据应用重要业务场景，评估其数据安全现状，在数据分类分级的基础上，分段实施、体系规划、面向数据访问域、存储域、流动域，落实覆盖数据全链路的数据安全技术防护体系。

在数据存储方面，对敏感数据或重要数据进行加密存储，防止黑客拖库、磁盘丢失、备份文件被盗等原因造成敏感信息泄漏；对重要终端、数据库服务器、应用服务器、文件服务器等重要系统部署勒索软件防范勒索攻击；同时借用数据灾备保障业务连续。

在数据访问方面，通过数据库防水坝对运维人员的权限进行细粒度的操作权限控制，实现 DBA 权限分离控制、防止越权，实现 DML/DDL 操作指令控制，防止误操作；通过数据库防火墙防范黑客通过 SQL 注入漏洞和数据库漏洞进行网络攻击和数据窃取；采用 DLP 数据防泄漏系统对重要文件的处理、传输进行管控；通过数据库审计实现数据库访问的各类操作行为的监控和记录、审计溯源。

在数据流动方面，通过静态脱敏、水印溯源、API 监测与访问控制等能力，加强数据流动场景下的安全保障和风险监测，实现数据可控流动。

安全是一个不断变化的过程。为了应对变化，医疗机构与器械厂商应对数据安全进行持续优化改进与运营，以看见驱动安全，从全局视角提升对数据安全威胁的发现识别、理解、分析和响应能力，实现资产全域可管、风险全域可视、策略全域联动，充分盘活整体数据安全防护能力，最终形成一体化的数据安全管理、安全监控和安全运营体系，实现数据安全统一运营。

1.3 加强数据安全培训

为确保医疗器械进入临床使用时合法、安全、有效，各医疗器械厂商应对设备管理人员、运维人员以及监管人员加强宣贯数据安全的宣教力度、监管力度，以多种形式定期进行培训，加强员工对数据安全的认知和意识。在制定医疗器械安全策略时关注设备质量和完整性，并权衡风险提出合适的设计和功能并实施反恶意软件，也必须考虑数据加密、数据传输、软件维护和更新等问题，

为加强医疗器械临床使用安全管理工作，降低医疗器械临床使用风险，提高医疗质量，保障医患双方合法权益，各医疗卫生机构应加强数据安全教育培训，组织安全意识教育和数据安全管理制度宣传培训，结合医疗卫生机构业务实际情况，建立完善数据使用申请及批准流程，遵循“谁主管、谁审查”、遵循事前申请及批准、事中监管、事后审核原则，严格执行业务管理部门同意、医疗卫生机构领导核准

的工作程序，指导数据活动流程合规。

1.4 数据安全技术工具

1.4.1 模拟系统攻击面，保障安全设计

在医疗器械产品设计阶段，可以通过减小攻击面和威胁建模的方式保障产品设计的安全性。

减小攻击面本质上与威胁建模相同，不过其切入角度不同，减小攻击面采用尽可能缩小攻击者利用的漏洞范围来降低可能出现的风险，在医疗器械下主要包括：关闭或限制系统接口、服务的访问；通过最小权限原则的方式设定不同的账号体系以约束其触达的数据范围；医院内网与互联网进行隔离分层尽可能减少直接攻击者直接触达医疗器械的可能性。

威胁建模是在识别和评估一个系统中的威胁，基于工程和风险的方法，用于识别、评估和管理安全威胁，以便采取适当的措施来减轻威胁的影响。旨在开发和部署符合企业组织安全和风险目标的更好软件和 IT 系统。威胁建模通常是在系统开发的早期阶段进行，以确保安全性被嵌入到系统的设计和架构中。当然在开发后的威胁建模也是有意义的，帮助识别系统中的漏洞和弱点，并提供相应的修复建议。

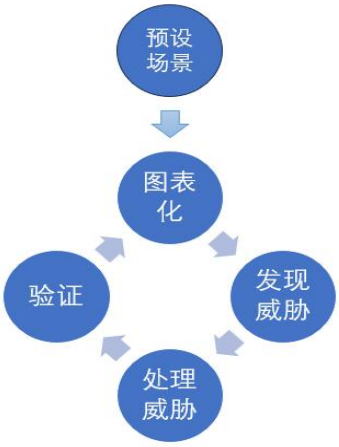


图 1：威胁建模的方法流程

a) 目标和定义：分析系统中可能出现的威胁，包括黑客攻击、病毒感染、木马、钓鱼、社会工程学等，在系统开发早期发现 Bug、理解安全需求等。

b) 适用范围：可应用于任何类型的预期接入 IT 网络的医疗器械。

c) 测试对象：IT 网络、系统、应用程序。

d) 测试方式：需要对医疗器械的整体系统进行梳理，确定系统的主要部件、交互方式和流程。然后根据梳理结果，结合常见的威胁模型（如 STRIDE）和攻击路径（如 ATT&CK），识别可能存在的威胁和攻击路径。

e) 威胁评估：评估每种威胁的概率及影响程度，以确定其重要性。

f) 测试结果：包括系统的威胁模型、安全漏洞、弱点和建议的安全措施等。

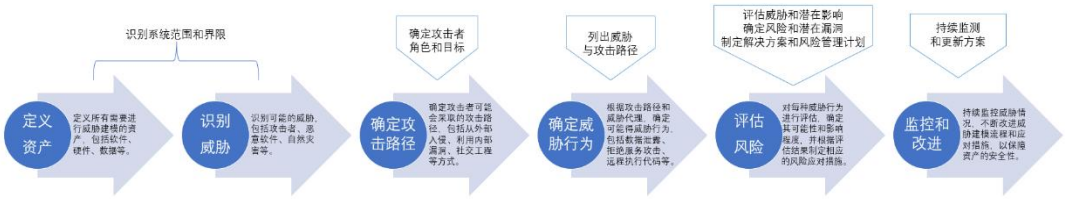


图 2：威胁建模实施流程

1.4.2 静态白盒扫描，减少代码漏洞

静态白盒扫描是指对源代码进行静态分析，识别程序中的安全漏洞和不安全的函数和 API。它适用于对特定的代码进行评估，不安全的编码规范会导致程序漏洞百出，不经意的为黑客留下程序的后门。

a) 目的：分析软件源代码，发现静态的安全漏洞和潜在问题。

b) 适用范围：可应用于任何类型的预期接入 IT 网络的医疗器械，因为它是一种

针对源代码的静态分析。这意味着代码审计可以用于任何类型的程序，无论是桌面应用程序、Web 应用程序还是嵌入式软件。

c) 测试对象：软件源代码，包括其编写的语言、算法、逻辑等。

d) 测试方式：对软件源代码的分析，进行白盒测试。

e) 测试结果：一份详细的代码审计报告，包括发现的静态漏洞、潜在问题、代码规范问题及修复建议等。

1.4.3 动态渗透测试，模拟外部攻击

渗透测试指的是通过模拟真实的攻击行为，评估系统或应用程序的安全性能和弱点，发现并利用漏洞，进而提供系统和应用程序的安全建议。它适用于对系统进行全面的、深入的评估，从而找出潜在的风险和漏洞，以便提高系统和应用程序的安全性能。

a) 目的：模拟攻击者的行为，从实际运行中发现安全漏洞，漏洞包含已知的安全漏洞和特有的 0day 漏洞。

b) 适用范围：适用于所有类型的医疗器械。

c) 测试对象：已部署的软件系统及其环境中的开放服务和应用程序，包括其运行时环境（Runtime environment）、网络拓扑等。

d) 测试方式：模拟攻击者的行为，进行黑盒测试，通过使用自动化工具、人工测试进行系统性的黑盒测试。

e) 在不知道目标网络的情况下，模拟黑客攻击，使用各种主流测评攻击及自主开发的内部测试工具，参照相应的安全性能指标标准进行安全检测。渗透测试服务用于验证在当前的安全防护措施下网络、系统抵抗黑客攻击的能力。

f) 测试结果：一份详细的测试报告，包括漏洞的类型、位置、危害程度及修复建议等。

g) 在模拟测试前，需提前制定测试时间计划和测试用例范围。

1.4.4 交互模糊测试，挖掘隐藏漏洞

模糊测试是一种专注于输入模式的动态分析，通过故意向目标发送大量的随机数据或特定格式的数据包来尝试造成目标系统的故障，比如缓冲区溢出漏洞、拒绝服务漏洞等，在医疗器械场景下，拒绝服务漏洞也可能会造成重大的风险，如攻击者传输特定格式的 DICOM 文件以触发目标器械的拒绝服务漏洞，造成器械故障无法正常运转工作。

a） 目的：通过对输入数据的随机生成和变异，可以检测应用程序或系统的完整性和安全性，从而帮助开发人员修复漏洞并提高应用程序或系统的安全性。

b） 适用范围：可应用于任何类型的预期接入 IT 网络的医疗器械，特别适用对于输入的数据检查较为松散的（loosely validated）医疗器械。

c） 测试对象：各种输入端口、输入参数、文件格式等。通常，模糊测试会对输入数据进行随机生成和变异，以测试应用程序或系统对异常、无效或恶意输入的响

应能力。

d) 测试方式：使用自动化工具生成异常数据进行测试，比如使用 fuzz 工具对输入端口进行模糊测试。

e) 测试结果：一份详细的测试报告，包括发现的漏洞、异常情况和潜在问题等。同时需要提供产生异常的测试用例，以便开发人员进行漏洞修复和代码改进。

f) 在模糊测试之前，需提前制定测试时间计划和测试用例范围。

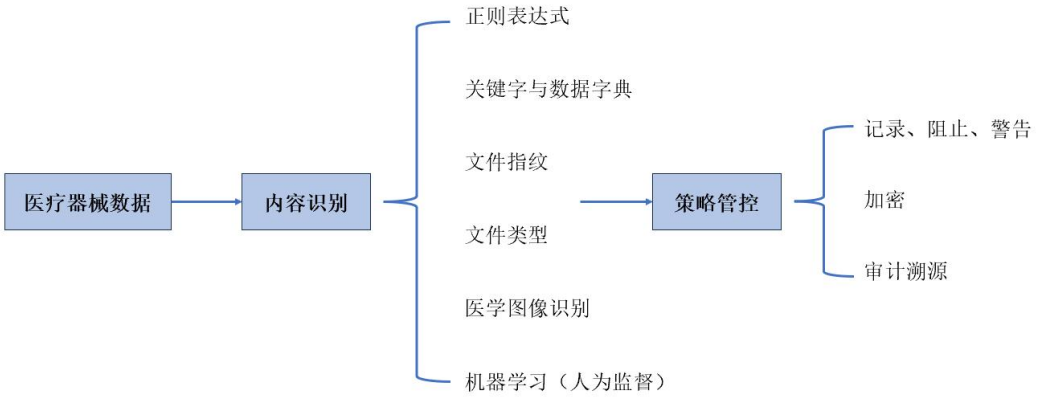
1.4.5 数据泄露防护，保护数据安全

数据泄露防护系统是基于内容识别技术，针对医疗器械中所存储的静态数据和动态数据进行数据安全保护，防止其通过 U 盘拷贝、打印、QQ 外发等途径泄露数据，对潜在的泄露数据行为进行记录、告警以及阻断，减少人为数据泄露的可能性。

a) 目的：通过对医疗器械中存储的敏感数据以及拷贝、打印、QQ 外发等数据邪露通道进行策略管控，做到事前主动防御，事中策略控制，事后行为审计的全链路数据安全防护。

b) 适用范围：可应用于任何类型的预期接入 IT 网络的医疗器械。尤其是具有医疗器械操作或使用权限的系统终端。

c) 防护手段：采用关键字匹配、图象识别、指纹识别、人为监督的机器学习等内容识别技术，结合记录、阻断、告警等管控策略，减少数据泄露风险。



1.4.6 集中身份认证，确权互联双方

集中身份认证平台是通过访问控制一体化的能力，实现账号、密码

统一分配和管理，完成非授权人员无法登录，授权人员最小权限授权登录，不同权限角色间的权限有效隔离的防护手段，避免出现部分低权限员工或运维人员在不当账号授权下获得高敏感权限的场景，提高医疗器械及其相关联系统中的账号安全性，确保完成数据交互的双方都为可信用户。

a) 目的：通过对具有医疗器械操作、使用、运维权限账号的管理、认证、审计和授权动作，完成不同角色账号之间的权限隔离以及交互双方的可信性保证。

b) 适用范围：可应用于任何类型的预期接入 IT 网络的医疗器械。尤其是具有账号体系的系统终端。

c) 防护手段：采用数字证书、USB Key、动态口令、LDAP 等技术确认账号身份及其对应的权限，完成多账号的安全管理和权限授权。

1.4.7 安全信息和事件管理，监控异常日志

安全信息和事件管理主要包含安全信息管理和安全事件管理，通过医疗器械及其关联系统的广泛事件数据日志的实时收集和存储，利用数据模型对其进行安全风险事件的关联与分析，完成实时数据安全事件监控以及安全告警，能够及时的发现渗透进入医院内网的攻击者及其留存的恶意后门程序。

a) 目的：通过对医疗器械及其关联系统的数据日志进行数据模型的关联与分析，清理历史留存漏洞后门程序，并及时告警实时攻击行为。

b) 适用范围：可应用于任何类型的预期接入 IT 网络的医疗器械。

c) 防护手段：采用日志分析、数据模型建模等手段，为医疗器械的网络安全保驾护航。

1.4.8 实时态势感知，预测安全风险

态势感知是利用大数据、机器学习等技术方法对海量数据进行提取并进行关联分析，做到对潜在安全风险的趋势预测。态势感知区别于

安全信息和事件管理最重要的一样便是态势感知重点对于潜在发生的安全风险进行预测，而安全信息和事件管理则更偏向于对实时和历史日志的分析，以获取当前已明确发生的安全事件和风险。

同样，态势感知往往会依赖一些医疗行业的威胁情报，结合相关领域专家的实操经验，来构建基于特定场景的感知系统，感知系统需要持续不断的进行维护和更新，以确保能在与时俱进的攻防对抗中保持主导地位。

a) 目的：提前预测、监测到潜在的复杂高级攻击，针对性的对医疗器械组件或系统进行安全能力的布控。

b) 适用范围：可应用于任何类型的预期接入 IT 网络的医疗器械。

c) 防护手段：利用大数据、机器学习技术，结合海量威胁情报数据，预测潜在的安全风险，做到风险的事前预防。

二、夯实医疗器械基础数据安全

2.1 医疗器械网络安全管理

随着《网络安全法》《数据安全法》《个人信息保护法》《关键信息基础设施安全保护条例》以及《医疗器械网络安全注册技术审查指导原则》等一系列法律法规和标准的出台，医疗器械网络安全越来越受到重视。伴随医疗云计算、远程医疗、人工智能技术的普及，越来越多医疗器械具备网络连接功能以进行电子数据交换或远程控制，这在提高医疗服务质量与效率同时也面临着网络攻击的威胁，导致患者隐私和生命安全受到威胁。据不完全统计，医疗器械越来越成为恶意网络攻击的目标，不仅导致数据泄露，还会增加医疗保健服务成本，并最终影响患者的健康状况。

为落实国家及行业主管部门关于医疗器械网络安全管理工作要求，医疗器械企业应加强网络安全管理，一是结合医疗器械预期用途、使用场景、核心功能确定不同类型产品安全风险类型；二是评估威胁和脆弱性对于医疗器械和患者的影响以及被利用的可能性，确定风险水平并采取充分、有效、适宜的风险控制措施；三是加强医疗器械全生命周期质控工作，要做好上市前后各个阶段的质控工作，上市前结合质量管理体系要求和医疗器械产品特性开展网络安全质控工作，上市后根据网络安全更新情况开展更新请求评估、验证与确认、风险管理、用户告知等活动。四是开展网络安全测试工作，定期开展医疗器械网络安全测试工作，包括源代码审核、漏洞扫描、渗透测试等，并将必要的网络安全相关信息以及应对措施告知用户，五是及时清理过时医疗器械，进行网络隔离消除关键漏洞。

因此，在目前医疗器械日益数字化的趋势下，网络安全问题迫在眉睫。各大医疗器械企业应该高度重视网络安全问题，加强医疗器械网络安全管理，不断提高医疗器械的网络安全性能，以确保医疗器械的稳定性和可靠性。

2.2 医疗器械数据安全治理

企业应加强数据安全治理工作，围绕数据战略、数据标准、数据质量、数据架构、数据应用以及数据全生命周期开展治理工作，推动企业建立数据统一标准，促进数据应用，进一步提升数据资产价值创造。同时，数据全生命周期建立数据安全管理策略，针对数据收集、传输、存储、使用、交换和销毁等环节，采取相应的数据安全管控措

施，强化数据全生命周期安全防护能力。

数据收集阶段，明确数据收集的目的和用途，确保满足数据源的真实性、有效性和最少够用原则要求，并明确数据收集渠道、规范数据格式以及相关的流程和方式，从而保证数据采集的合规性、正当性和一致性。在采集过程中采用数据加密、数据脱敏等技术手段，确认用户身份真实性和合法性，并确保数据收集过程中全流程可审计。

数据传输阶段，采用适当的加密保护策略和数据安全防护措施，防止传输过程中的数据泄露，并加强数据传输过程中接口安全控制，建立满足数据传输安全策略相适应的数据安全控制技术方案，包括通道安全、可信通道等。

数据存储阶段，根据组织内部数据存储介质的访问和使用场景，以及业务特性和数据存储安全要求，提供有效的技术和管理手段，防止对存储介质的不当使用而可能引发的数据泄漏风险，实现对数据逻辑存储、存储容器等的有效安全控制。选择合适的数据存储架构和介质在 境内存储，采用敏感数据分类分级、数据库漏洞扫描、数据存储加密、身份权限控制、数据备份等安全防护措施防止数 据在存储时被非授权获取、篡改以及破坏。

数据使用阶段，采用终端防泄漏、数据安全访问控制、数据静态脱敏等技术 ，确保数据在使用过程中的安全，同时采用数据安全审计技术对数据的操作与访问等进行全方面的审计，确保使用过程留痕，以便事后溯源。

数据交换阶段，采用终端防泄漏、API 审计、网络 DLP、水印技

术、隐私计算、数据库访问控制技术等，实现数据敏感性识别、数据泄漏溯源、高危操作拦截等，保证数据使用安全和数据流向的可知可管可控。

数据销毁阶段，通过制定数据销毁机制，实现有效的数据删除管控，防止因对存储介质中的数据进行恢复而导致的数据泄漏风险。采取磁盘数据删除、加密数据删除和物理介质报废等技术，确保数据无法还原。

2.3 加强数据安全审计

应结合医疗卫生机构自身内部审计的需求，采取实现内部审计全流程管理、加强信息数据安全管理工作、建立内部审计信息化执行规范等一系列措施，提升公立医院内部审计信息化建设的质量。加快数据安全审计与监督检查机制建设 ，推动将数据安全审计纳入行业机构内部 风险防控体系，明确数据安全审计开展的方式、频率、审计重点、审计程序等内容，定期开展数据安全审计工作，评估审核数据安全组织机构、数据生命周期安全。

2.4 提升数据安全应急响应能力

医疗器械企业应加强数据安全风险评估、风险监测与事件处置，从数据安全事前防御、事中监测和事后处置环节出发，建立数据安全应急响应管理机制。一是明确数据安全事件管理和应急响应工作指南，定义数据安全事件类型，明确不同类别事件处理流程，制定有针对性的应急预案，按照医疗器械安全风险分级，制定相应的数据安全应急预案；二是建立对数据安全事件管理及执行的有效性量化评估规则，

向管理层呈现数据安全事件应急处置效果，并建立数据安全事件复盘机制，总结应急管理经验；三是在企业内部加强对应急响应、数据安全事件处置工作制度、策略和防范等方面工作培训宣传，培养相关人员的基本应急响应意识。

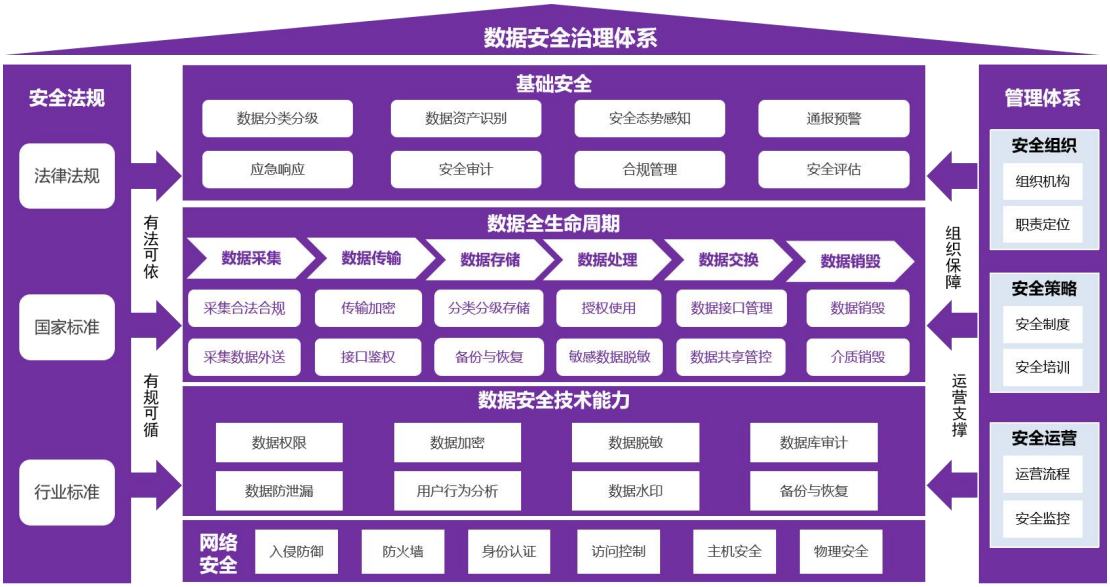
第五章 医疗器械数据安全行业应用实践

一、数据安全合规管理体系

GE 医疗作为全球领先的医疗技术、药物诊断和数字化解决方案的创新者，高度重视数据安全工作。经过体系化数据安全治理工作，形成以保障核心信息系统及医疗器械数据安全为主要目标的数据安全合规管理体系。

1.1 GE 医疗数据安全体系框架

GE 医疗依据法律法规、国家标准及行业标准，围绕基础安全（包括数据资产识别、数据安全态势感知、数据安全审计、数据分类分级等）、数据全生命周期安全（包括数据采集、传输、存储、处理、交换、销毁等生命周期技术安全）、网络安全（包括入侵防御、防火墙、身份认证等），进一步提升数据安全管理、技术和运营三大方面能力，形成覆盖多业务类型的数据安全管理体系，在满足安全合规的基础上，实现数据有序流动，推动数据价值创造。



图：GE 数据安全治理体系框架

1.2 GE 医疗数据安全管理能力

GE 医疗从组织、制度、流程等方面加强数据安全治理力度，有效推动数据安全管理目标落地实施。组织方面，GE 医疗建立了包含决策层、管理层和执行层的三层组织架构。安全制度层面，以 GE 数据管理规划、数据管理办法等纲领性文件为指导，以数据安全规范、指南、细则等制度为基础，建立 GE 数据安全管理制度体系。数据安全管理流程层面，以数据安全制度为基础，进一步建立包括账号权限申请、数据提取、数据归档、数据安全应急响应等相关流程，实现数据安全闭环管理。

1.3 GE 数据安全技术能力

GE 基于数据全生命周期安全防护要求，重点开展数据资产管理、数据权限、数据加密、数据脱敏、数据审计、数据防泄漏、数据备份恢复等安全技术能力建设，将数据安全技术嵌入到数据全生命周期管理全过程。在数据保护方面，开展数据分类分级工作，建立数据分类分级管理流程，并将智能化数据分类分级工具纳入数据安全管理重点工作内容。数据加密保护方面，加强数据存储和传输过程中安全管控，采用数据加密保护技术，为数据存储和传输过程提供安全通道，保护数据安全。在数据访问控制方面，建立数据访问控制矩阵，明确主体访问数据范围，并通过技术手段对主体建立标签体系，建立形成以用户为中心的访问权限表。

图：GE 数据全生命周期安全技术防护能力

二、数据安全全生命周期管理

迈瑞医疗器械在全球范围内的销售和装机已扩展至 190 多个国家和地区，为了满足多个区域对医疗器械病人隐私保护和数据安全的需求，迈瑞生产的医疗设备采取了一系列的安全措施。

2.1 管理体系

首先是建立合规基线，基线内容来源于中国，美国和欧洲等不同区域的法律法规及行业监管要求分解，内部建立跨部门的网络安全和数据保护团队，将法律法规和行业最佳实践分解成为可以执行和追溯的产品需求清单。

2.2 设计研发

在产品设计过程中，注重采用行业最佳实践来进行网络安全和隐私数据保护。

a) 保存到设备永久存储介质中的数据，都加密后再保存，目前主流产品都采用 AES256 加密算法；

b) 所有无线 WiFi 设备都支持企业级加密认证，设备之间的通讯采用 TLS1.2 传输数据，支持医院导入自己证书；支持批量导出迈瑞设备的 MAC 地址，用于医院对接入设备进行网络认证；

c) 支持对接医院权限管理系统,对访问设备关键功能和核心数据进行权限认证，并提供可供审计的数据访问记录；

d) 只采集必要的隐私数据,对隐私数据提供多种可配置的显示方式，如脱敏显示，或者要求鉴权后再显示，提供快速清除所有隐私数据的能力；

迈瑞的产品研发遵循网络安全开发流程（Security development lifecycle，SDLC）开展活动，产品网络安全管理不仅是上市前产品开发的需求输入，也在产品上市后的全生命周期得到全面及时维护。迈瑞遵循各种法律法规进行网络安全需求分析活动,并通过威胁建模识别与我们的产品相关的任何潜在安全风险。基于需求分析结果和所发现的安全风险，将风险控制分解到产品需求，用于后续的设计和测试跟踪，这些风险控制措施也包含在产品风险管理报告中。网络安全风险分析活动贯穿于产品上市前的整个开发过程。

迈瑞建立了产品的漏洞管理策略，补丁管理策略，应急响应策略等，在产品发布以后，通过这些措施来定期评估已发布产品的安全风险，协调统一的响应，并根据我们的产品安全策略框架跟进以调查和解决安全事件。同时迈瑞建立产品安全团队，负责所有产品的安全测试。这些测试包括漏洞扫描，渗透测试，网络安全需求验证等活动。

2.4 运营管理

迈瑞的产品网络安全管理由产品网络安全委员会负责，该委员会独立于迈瑞的各个事业部，从机制上协同不同事业部的产品网络安全管理，形成迈瑞统一的产品网络安全管理策略。产品网络安全委员会与集团合规办公室共同确定迈瑞的整体产品网络安全工作指导原则，并定期向集团管理层呈现公司在产品网络安全方面的规划与进展。产品网络安全委员会按照迈瑞三条产品线分别设置各个事业部的产品网络安全技术专家，并由产品网络安全委员会组织各技术专家，从产品的设计、开发、验证、维护等各个环节，进行统一和持续迭代更新的产品网络安全管理。产品网络安全委员会持续研究网络安全关键技术，并调动迈瑞的软件开发委员会和软件测试委员会进行关键技术研究和人员培养。

三、数据安全建设框架

医疗行业数据安全基础较为薄弱、随着医疗器械数据参与生产与使用场景增多，数据开放城程度加深，数据安全的隐患逐步增加。

为保证数据安全流通，安恒信息提供安恒数盾数据安全解决方案，聚焦于身份安全、数据流通、数据保护、咨询规划四个方向，建立数据风险核查、数据梳理、数据保护、监控预警的 CAPE 数据安全能力模型。构建覆盖数据采集安全、数据存储安全、数据交换与传输安全、访问控制安全、数据加密安全、数据备份与恢复、数据使用申请与管理以及数据回收与销毁等生命周期的数据安全治理体系。

图：安恒 CAPE 数据安全能力框架

在契合数据要素流通市场的基础下，安恒提出应以“数据内外循环为视角，客户核心痛点为中心，数据使用场景为抓手“的理念，提供”2 平台+3 体+N 场景”的数据安全技术能力体系。在数据对内部循环使用时，提供加密、脱敏、审计、识别等多版块安全保障能力。在数据交易、数据开放等不可控环境的数据外循环场景下，安恒信息提供了原始数据不可见、计算模型授权可控的隐私计算方案，实现“数据价值传递”、“数据可用不可见”、“数据可用不可取”。同时，安恒信息提供了咨询前期数据安全顶层规划、咨询中期数据安全治理落地、咨询后期数据安全持续运营的闭环服务。

在医疗场景下，安恒信息提出了医疗数据安全建设整体框架，构建以身份安全、数据保护、数据流通、咨询规划为核心的数盾数据安全解决方案，真正实现从“基于威胁的被动保护”向“基于风险的主动防控”转变，提升整体数据安全能力，形成数据安全保障闭环，数据的安全可控。帮助企业“让业务放心大胆地使用数据，创造更大的

商业和社会价值”。

四、医疗数据自动化分类分级

随着业务发展，医疗行业类系统对数据使用的方式日渐复杂，存在数据管理、用途授权控制粗放、敏感数据外泄等数据安全风险。需从数据本身的特性出发，基于数据权属和流动特性，识别数据可能面临的风险和威胁，了解数据安全现状和存在的安全问题。

爱加密深度学习了主管部门关于数据分类分级、数据安全相关要求，开展数据安全基础现状、数据安全风险评估、数据资产梳理，摸清核心数据资产家底，开发医疗数据分类分级自动化系统。

a）全面识别数据安全风险

通过对关键数据进行安全风险评估，总结数据安全的薄弱点，并形成评估报告和整改建议，协助业务整改。

b）建立并推行数据安全运营管理体系

结合法律法规和行业经验，建设数据安全管理体系框架和管理策略，形成管理体系框架。

c）数据资产的梳理

在了解自身和所处行业数据特性的基础上，有效的识别现有数据资产，避免因数据类型定义不清造成的数据违规收集、数据开放与隐私保护风险。数据资产识别梳理应通过技术手段实现工具化。

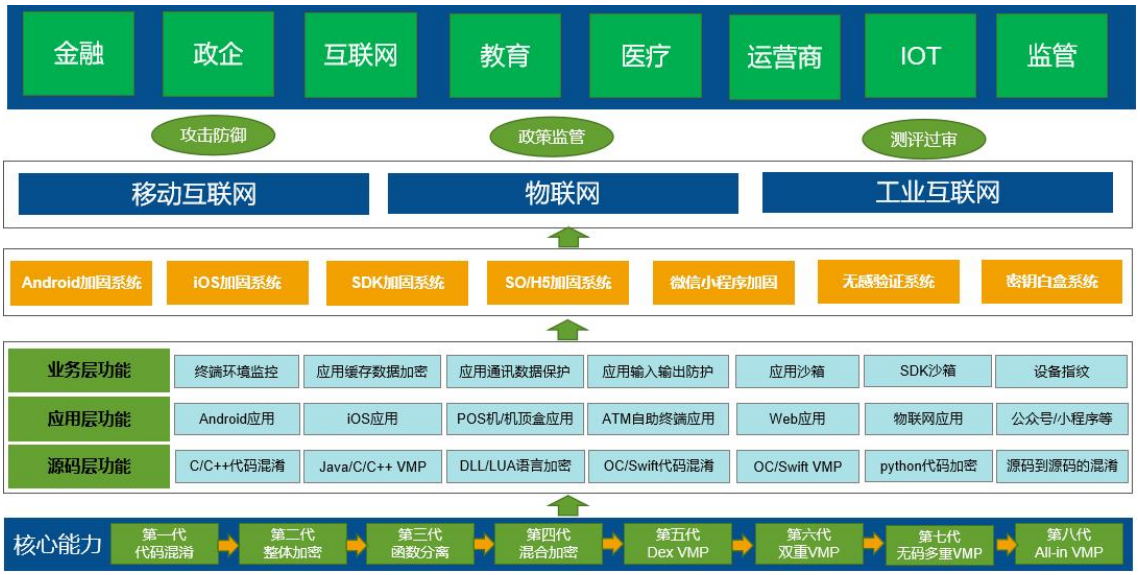
五、移动客户端安全防护

5.1 移动端安全加固平台

1）产品定位：

爱加密移动应用安全加固平台为开发者提供全面的移动应用安全加固技术，包括 Android 应用加固、iOS 应用加固、H5 文件加固、微信小程序加固、SDK 加固、so 文件加固和源对源混淆加固技术，从根本上解决移动应用的安全缺陷和风险，使加固后的移动应用具备防逆向分析、防二次打包、防动态调试、防进程注入、防数据篡改等安全保护能力。

2）产品架构：



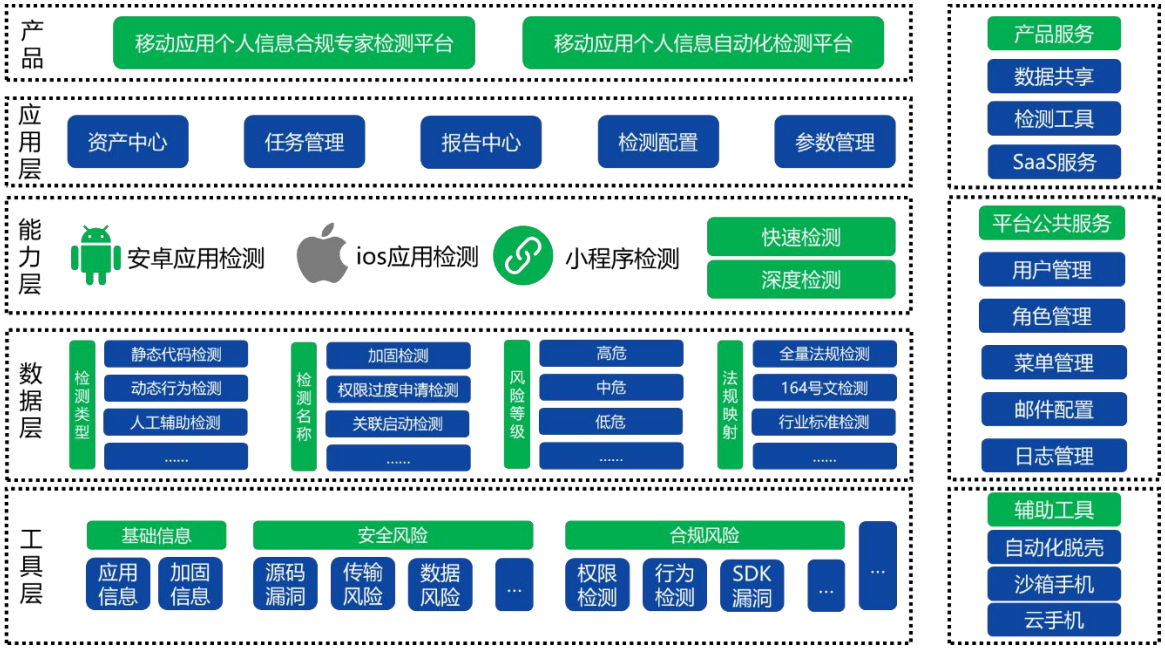
5.2 移动端个人信息保护检测平台

1）产品定位

爱加密移动应用个人信息安全检测平台是针对移动应用、SDK 和小程序中出现个人信息的非法收集、滥用、泄露等严重问题，结合相关法律法规和监管要求，为监管机构、测评机构、应用开发企业等推出的合规检测平台。该平台针对移动应用的基本信息、漏洞信息、收集和使用个人信息行为、通讯传输行为、软件和技术供应链情况、技术脆弱性、隐私政策规范性等进行多维度安全检测和合规检测，并出

具专业的个人信息安全报告。帮助监管机构准确、有效地提供行政执法依据；帮助测评机构出具专业的个人信息测评报告；帮助应用开发企业在应用发布前评估个人信息的安全性和合规性。有效降低 APP、小程序违规收集使用个人信息的风险，助力 APP、小程序和平台长久运营。

2）产品架构

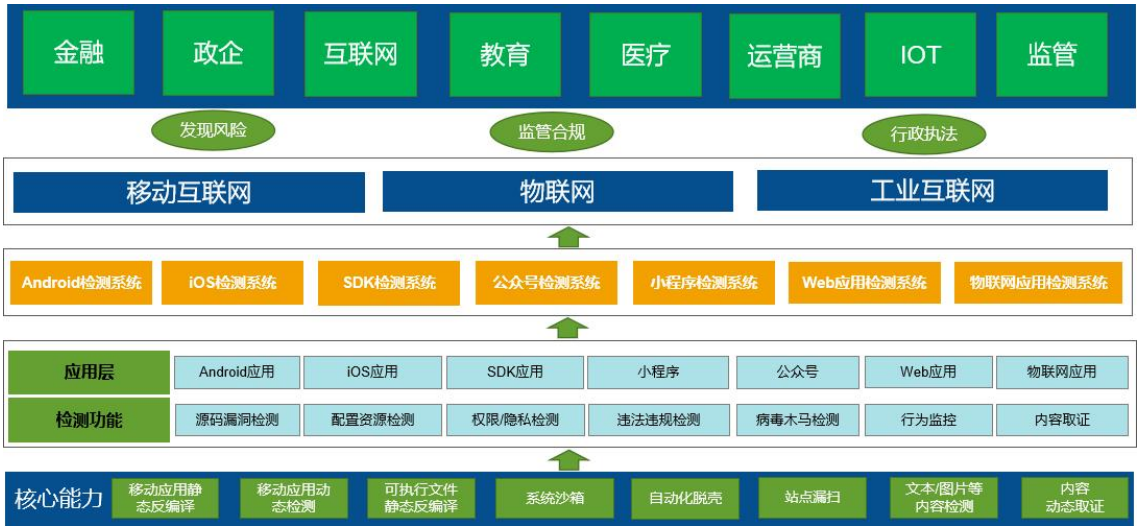


5.3 移动客户端安全检测平台

1）产品定位

爱加密移动应用安全检测平台通过静态检测技术和动态检测技术，检测 Android 应用、鸿蒙应用、iOS 应用、Android SDK、微信公众号、微信小程序、IoT 固件存在的安全风险、漏洞，对发现的安全问题给出解决建议，并且提供准确、完整的安全检测报告，帮助开发者了解并提高应用的安全性。

2）产品架构



第六章 医疗器械数据安全发展展望

一、明确要求，推动医疗器械数据安全发展

（一）从行业主管部门层面，提出医疗器械数据安全注册指导原则，推动发展。

一方面，数据安全注册指导原则可有效促进医疗器械企业切实提升数据安全意识，增强主观能动性，切实做好医疗器械数据安全相关工作。另一方面，医疗器械产业发展涉及多行业主管部门，要进一步加强各部门的沟通协调、协作配合，出台专门的数据安全政策要求，共同做好医疗器械数据安全管理、监督、考核，促进产业合规发展。

（二）从产业层面，建立健全医疗器械数据安全标准体系，规范发展。

以医疗器械数据安全全生命周期为导向，从生产规划、设备建设、临床应用、运行维护、停服退网等关键环节，重点研究医疗器械漏洞挖掘、威胁情报收集、远程运维管理、安全评估评测等核心技术，制定相关标准，推动落地实施，规范产业链有序发展。

二、鼓励创新，提升行业数据安全管理水平

（一）探索医疗器械数据安全管理新思路。

云计算、区块链、AI 大模型等新技术新理念快速发展，鼓励从医疗设备应用发展趋势着眼，以满足数据安全需求，解决安全风险为导向，创新安全防护新思路和新方法，推动医疗器械数据安全产业发展。

（二）推动新思路落地实施，谋求革新发展。

通过对医疗器械供应链资产识别，自动开展安全漏洞和威胁情报关联分析，通过建设 AI 风险分析模型，实时快速发现安全威胁，及时通知整改，为重大活动提供专项检测、实时监测、应急处置等能力，提升行业数据安全管理水平。

三、产业聚焦，打造产业健康生态

医疗器械数据安全健康可持续发展，离不开产业链的鼎力支持、合力推动和全力配合。在行业主管部门指导下，中国信息通信研究院云计算与大数据研究所，聚集医疗器械企业、网络安全企业、医疗卫生机构等相关单位，联合开展医疗器械数据安全研究工作，在数据安全研究方面达成共识、形成合力，共筑医疗器械数据安全新生态、共谋新发展。