CSTC中国评测 见证质量 技术白皮书

移动互联网医疗安全风控白皮书（2020 年）

中国软件评测中心·软件与信息系统测评工程技术中心

2020 年 9 月

序 言

国家高度重视“互联网+医疗健康”工作，近年来出台了一系列政策推动其发展。移动互联网医疗的出现，提升了患者就诊方便性和就医及时性。移动互联网医疗通过移动终端或互联网提供医疗健康服务，由于移动终端应用安全保障机制和系统纵深防御不足，导致其面临新的安全风险挑战。

本白皮书通过分析移动互联网医疗安全风险现状及成因，结合实际应用，提出建立针对移动互联网医疗应用的安全风险监控技术模型和管理机制。倡议成立安全风控联盟，形成政府监管、行业自律、机构自治的三重安全防线。

本白皮书由中国软件评测中心医疗测评实验室撰写，参与人员包括孟晓、赵亮、徐鹏、黄晓培、张春芳、李真、杨令宜、李佳奇，在此特别感谢中心品牌宣传推广部刘喜喜、闫晓丽的编辑及排版支持。限于研究时间有限，领域方兴未艾，报告内容难免存在纰漏，不足之处恳请各方同仁批评指正！

中国软件评测中心

2020 年 9 月 1 日

版权声明

指导组：黄子河　安　晖　刘龙庚　陈渌萍　黄江平
编写组：孟　晓　赵 亮　徐　鹏　黄晓培　张春芳
李　真　杨令宜　李佳奇

目 录

前 言

党中央、国务院高度重视“互联网+医疗健康”工作，习近平总书记指出，要推进“互联网+教育”、“互联网+医疗”等，让百姓少跑腿、数据多跑路，不断提升公共服务均等化、普惠化、便捷化水平。李克强总理强调，发展“互联网+医疗”，让群众在家门口能享受优质医疗服务。

为贯彻落实党中央、国务院精神，国家卫生健康委员会起草，国务院常务会审议原则通过了《关于促进“互联网+医疗健康”发展的意见》，指出要加强行业监管和安全保障，对强化医疗质量监管和保障数据信息安全作出明确规定，保障“互联网+医疗健康”规范有序发展。

移动互联网作为公众生活中越来越依赖的载体，医疗服务机构所提供的服务将更多以移动互联应用模式体现。由于近年来移动互联网安全风险呈现着日益严峻，无论是公众还是服务机构都遭受了安全风险威胁，甚至带来了生命财产的损失。因此，中国软件评测中心根据在多年来移动互联网医疗支撑监管部门及工作经验，对安全风险成因进行分析，提出了针对移动互联网医疗应用的安全风险监控技术模型和管理机制，为推动移动互联网医疗安全风险治理提供参考。

一、移动互联网医疗四类安全风险日渐严峻

随着 5G 的持续推进和移动智能终端设备的深化应用，越来越多的生活服务类数据通过移动应用涌入移动互联网。工信部发布的中国互联网市场移动应用相关报告中指出，截至 2018 年，我国移动市场共检测到移动应用 449 万款，净增数量 42 万款。

作为与公民密切相关的互联网医疗服务发展尤其迅速，各大医院都推出了各自的移动医疗 App，许多第三方机构更是把握市场方向，建立医院、医生和患者三者撮合的第三方移动医疗 App 平台，为公众提供寻医问诊、预约挂号、购买医药产品及查询专业信息等服务，当前市场上已有 2 万多款移动医疗 App 提供医疗相关服务。

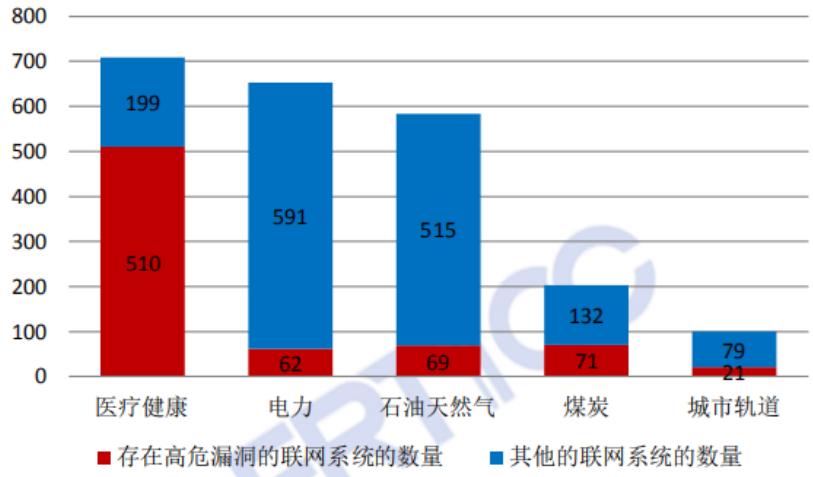
在新型冠状病毒肺炎疫情影响下及近年来国家对“互联网+医疗健康”的鼓励支持下，可以预见移动互联网医疗业务呈蓬勃发展之势。同时，移动互联网医疗应用安全风险也呈现着增加趋势。主要表现在以下四个方面:

（一） 系统安全风险日益增加

由于移动互联网医疗数据中包含患者姓名、年龄、居住地址、电话、银行账户、诊断、检验报告、用药记录、病史等个人敏感信息，蕴含重要财富价值，移动互联网医疗系统成为不法份子所觊觎的重要目标，黑客可通过后台系统漏洞进行攻击从而获得大量的医疗健康数据。

医疗健康行业联网系统高危漏洞需要警惕。根据国家互联网应急中心发布的《2019 年我国互联网网络安全态势综述》报告显示，医疗健康行业存在高危漏洞的联网系统数量最多，安全风险较高。如图 1 所示:

图 1：存在高危漏洞的联网系统数量



图片来源：2019 年我国互联网网络安全态势综述,2019 年

据《2019 医疗健康行业网络安全观测报告》统计数据显示，在被调查的医疗健康行业 15339 家单位中，网络资产评估具有脆弱性的有 9523 家,应用服务端口暴露在公共互联网的有 6446 家，网站存在安全隐患的有 4546 家。

互联网医疗网站被篡改现象依然突出。移动互联网医疗应用通常通过互联网网站提供医疗服务或进行系统管理。根据中国互联网信息中心发布的《第 44 次中国互联网网络发展状况统计报告》统计数据，2019 年上半年国家计算机网络应急技术处理协调中心监测发现并协调处置我国境内被篡改的网站近 4 万个。根据《2019 医疗健康行业网络安全观测报告》统计数据，有 4546 家单位网站

存在安全隐患,其中 261 家单位的网站发现被恶意篡改。

App 漏洞和第三方 SDK 漏洞成为移动医疗领域的主要安全隐患。根据《2019 医疗健康行业移动 App 安全观测报告》统计,88.83%的医疗健康行业 App 存在高危漏洞。攻击者可利用漏洞对 App 进行仿冒、植入恶意程序、非法窃取个人敏感信息等。

医疗健康行业的机构为了给公众提供更多的便民服务,在 App 中集成了第三方 SDK。据爱加密 2019 年发布的《全国移动应用 SDK 市场占有率分析报告》显示，有 25.58%的医疗健康行业 App 引入了第三方 SDK，高于全行业平均水平，平均每款 App 引入了 2.5 个 SDK，同时也指出超过 60%的 SDK 含有多种漏洞。

（二） 应用渠道安全风险不可忽视

移动互联网医疗应用渠道主要分为两类: 一类是 PC 端互联网门户网站，另一类是移动客户端软件下载渠道。

钓鱼网站威胁移动互联网医疗安全。2018 年 8 月 21 日，奥古斯塔大学医疗中心遭遇了网络钓鱼攻击，导致约 41.7 万份记录遭泄露。遭泄露的数据包含患者个人信息以及他们的医疗健康记录、财务记录和社会安全号码。新冠疫情的爆发引发了网络钓鱼和恶意软件攻击的新潮流，不良行为者希望以此流行病为诱饵进行攻击。根据 Checkpoint 的研究，全球超过 4000 个与冠状病毒相关的域名中，3%是恶意域名，5%是非常可疑域名。

移动客户端软件仿冒带来敏感信息泄露问题。由于下载渠道的多样性，以及渠道对移动客户端软件的管理、技术检测等手段

的不足，使得具有钓鱼目的、欺诈行为的移动客户端软件仿冒成为不法者的工具。患者和医生使用仿冒或被篡改的移动客户端软件后，其个人医疗信息和金融信息将被不法之徒获取，给患者和医生带来安全和财产风险。随着移动医疗应用的加速普及，该威胁愈发突出。

（三）违法违规收集使用个人信息问题日益凸显

在中央网信办、工信部、公安部、市场监管总局四部委2019年开展的App违法违规收集使用个人信息专项治理行动中发现移动医疗App存在违规收集个人隐私信息行为，如读取用户联系人数据、读取用户日历信息、读取用户短信内容、允许应用发送短信/彩信导致意外收费、允许应用程序录制音频等超范围收集用户信息的情况，部分存在无用户协议和隐私政策。据爱加密发布的2019年《全国移动App安全性研究报告》，70%以上的App存在违规收集个人隐私信息的行为。

（四）数据泄露事件频发，影响程度加剧

由于很多移动互联网医疗运营机构在安全保障和健康医疗数据生命周期管理措施不足，运行在互联网上的移动互联网医疗系统成为黑客攻击的主要目标。根据国外医疗健康分析公司发布的医疗行业数据安全报告显示，2019年较上一年针对医疗行业黑客攻击事件猛增了48%，受影响的患者数量较上一年增长了两倍，影响范围和程度均加剧。

从2018年到2019年爆发了一系列国内外医疗数据泄露事件:

- 2018 年 1 月，某社区卫生服务中心工作人员，掌握了某市“妇幼信息某管理系统”市级权限账号密码，利用职务之便，多次将 2016 年至 2017 年的某市新生婴儿信息及预产信息导出，累计非法下载新生婴儿数据 50 余万条。
- 2018 年 4 月，MEDantex 旗下的一个门户网站存在泄露患者医疗记录的安全隐患，包含了与 2300 多名医生相关的文件。
- 2018 年 8 月，某 MongoDB 数据库被发现可以通过互联网公开访问，其中包含了超过 200 万墨西哥公民的医疗健康数据，这些数据包括个人的全名、性别、出生日期、保险信息、残疾状况和家庭住址等信息。
- 2019 年 9 月，国内医疗 PACS 服务器泄露近 28 万条患者记录，包括姓名、出生日期、检查日期、调查范围、成像程序的类型、主治医师、研究所/诊所和生成的图像数量等个人和医疗细节。
- 2019 年，我国某第三方预约挂号平台的短信平台存在漏洞，导致大量患者个人信息泄漏。

新冠肺炎疫情的出现，推动了我国移动互联网医疗服务的发展和普及。与此同时，移动互联网医疗安全风险影响深度和广度也在加剧，需要提高警惕并加以应对。

二、移动互联网医疗安全风险成因分析

（一） 移动互联网医疗系统安全纵深防御体系不健全

移动互联网医疗是以移动终端或互联网为载体将医师、患者等联系起来并提供服务。相对于传统的医疗系统来说，移动互联网医疗系统更多地暴露在公网上，不少移动互联网医疗系统安全纵深防御体系尚不健全，主要表现在以下五个方面:

1、网络拓扑结构不安全

网络拓扑结构安全性设计中最重要的因素是根据网络安全区域安全等级的不同，设计不同的网络安全区域，并且避免将重要网段部署在网络边界处，不同安全等级的网络区域之间采取可靠技术隔离手段。

有些移动互联网医疗机构为了部署和管理方便，采用了具有安全风险的网络拓扑结构，一是将 Web 服务器、应用服务器、数据库服务器均部署在同一子网，或 Web 及应用服务器未经过防火墙能直接访问数据库服务器；二是将数据库服务器部署在 DMZ 区域，黑客可通过攻破 DMZ 区域，获取数据库服务器上的敏感数据。

2、入侵防御设施配备不足或配置不合理

移动互联网医疗系统需识别和防范外部和内部的网络攻击行为，尤其是外部攻击行为，如 DDoS 攻击、SQL 注入攻击、跨站脚本攻击等。DDoS 攻击会导致提供的医疗服务无法使用，SQL 注入攻击和跨站脚本攻击会导致医疗健康信息泄露。

多数移动互联网系统未在网络边界处部署入侵防范设备，或者未按照正确的方式进行部署，或者未配置及启用针对常见攻击行为的防范功能，或者使用已过期的规则库。这些都是造成外部攻击行为成功的重要因素。

3、远程传输和接入安全防护措施不健全

对外部使用者来说，患者在注册和使用移动互联网医疗服务过程中，个人健康医疗信息在互联网传输时未进行加密或使用安全通道进行传输，攻击者容易截获敏感数据。

对内部使用者来说,运维人员通过互联网使用 HTTP 或 TELNET 进行远程管理时，未采取安全措施防止鉴别信息在网络传输过程中被窃听，攻击者容易截获鉴别信息和管理信息，获得系统访问权限，盗取更多的敏感数据。

4、安全监控和审计力度不够

建设移动互联网医疗系统时，在安全监控和事件预警机制方面采取的措施力度不够，设计时未充分考虑业务操作监控和审计功能，黑客入侵事件发生概率较高。同时，也未能有效防止内部人员进行违规操作，业务和数据操作不可追溯。

通常攻击者需要经过多次系统渗透或入侵才能获取相应访问权限，从而获得敏感数据。因而，有必要通过安全监控和审计对入侵行为进行分析和预警，可以在入侵事件发生前进行主动防御，阻止攻击行为。

5、Web 应用漏洞的安全防范和客户端抗攻击能力不足

移动互联网医疗系统主要采用 HTTP 协议向服务器提供请求，保障 Web 页面安全是非常重要的。从近几年的安全事件来看，SQL 注入和跨站脚本攻击占大半比例。

大部分机构的 Web 页面均未提供防范 SQL 注入和跨站脚本攻击的安全防护措施，未从代码层面防止漏洞的产生。

同时移动客户端软件未采用代码混淆、代码加壳、检测调式器等有效手段，抵御静态分析、动态调试等操作；未在软件安装、启动、更新时进行完整性和真实性校验，抵御篡改或劫持，导致用户的敏感信息在使用过程中容易被非法获取。

（二） 移动客户端应用渠道安全监测力度不够

移动互联网医疗应用渠道安全风险的主要原因有四个方面：

一是大多数移动互联网医疗应用运营方没有识别移动客户端软件仿冒和盗版应用的手段。

二是由于各渠道发布时间不同，存在版本不一致的情况，用户可能会下载具有安全漏洞版本的移动客户端软件。

三是多数移动客户端软件没有进行安全加固，给用户带来安全风险。

四是渠道对移动客户端软件的管理、技术检测等手段的不足，导致仿冒或篡改的应用存在。

（三） “认证-授权-审计”安全机制薄弱

“认证-授权-审计”（AAA）安全机制包括认证（Authentication）、授权（Authorization）和审计（Auditing），是网络安全中最为重要的安全管理机制，也是防范数据泄露的关键手段。

当前多数的移动互联网医疗系统在认证、授权和审计方面做得不够完善甚至缺失，导致数据泄露影响程度加剧。

从认证机制来看，移动互联网医疗系统应采用“双因素认证”方式和设置复杂口令来保障身份认证的安全性。目前大多数系统采用安全性较差的“用户名+口令”单因素身份认证方式和使用弱口令，容易被不法之徒通过工具暴力破解或被猜测出来，从而导致身份认证信息被盗用。

从授权机制来看，移动互联网医疗系统应合理分配和控制账户权限。目前多数系统未分配用户承担任务最小权限，权限粒度设置过大，未限制默认账户的访问权限，未及时收回账户权限，导致未授权的用户访问系统功能或数据。

从安全审计来看，相对于认证、授权机制，移动互联网医疗系统在安全审计机制建设方面更为薄弱，未提供高频登录、批量登录、关键数据使用等审计功能，甚至缺失基本的日志记录功能，导致无法预防潜在的安全事件发生及事后追溯。

（四） 医疗健康数据生命周期安全保护机制和措施不足

数据生命周期主要包括数据收集、数据传输、数据存储、数据使用、数据销毁五个环节。加强数据全生命周期的安全管理能够有效降低数据泄露的安全风险。目前大多数医疗机构缺少相应的安全管理措施和技术手段。尤其在数据管理方面，未对数据进行分类分级设置并采取针对性的措施进行数据安全保护。

第一，**在数据收集环节**，有些机构未依据最小够用原则收集医疗健康数据，且移动客户端应用软件抗攻击能力不足，在数据收集环节可能导致数据泄露;

第二，**在数据传输环节**，对于涉及数据安全等级较高的医疗健康数据，有些机构未采取加密传输或全通道传输保证传输保密性，数据被窃听的风险加大，同时在数据传输时也未采取校验码或哈希算法确保数据完整性，医疗健康数据被篡改的风险增大;

第三，**在数据存储环节**，对于敏感的医疗健康数据，有些机构未采用足够安全的加密算法进行加密存储，而且未构建安全可控的暂时存储环境，数据泄露风险较高;

第四，**在数据使用环节**，有些机构未建立有效的医疗健康数据脱敏机制，未建立数据分析相关数据源获取规范和使用机制，未明确数据获取的范围、数据量、频率、方式、访问接口、授权机制，通常该环节数据泄露风险最大;

第五，**在数据销毁环节**，有些机构未根据数据的分级分类和数据使用情况，建立合理的数据销毁方式，导致数据泄漏。对于

托管到公有云的移动互联网医疗系统，数据销毁的措施不当，会造成数据泄露情况更加严重。

（五） 行业层面缺乏风险监控管理手段

国务院办公厅在 2016 年和 2018 年先后发布了《国务院办公厅关于促进和规范健康医疗大数据发展行动纲要》和《国务院办公厅关于促进和规范健康医疗大数据发展行动纲要》鼓励“互联网+医疗健康”发展，均要求加强互联网医疗健康的行业监管和安全保障。国家卫健委在 2018 年和 2019 年发布了《电子健康卡建设与管理指南》、《电子健康卡服务应用指南》征求意见稿，均对电子健康卡的应用监测和安全管理提出了要求。但是医疗健康行业仍然缺乏针对移动互联网医疗应用的安全风险监控管理手段。

从行业监管层面来看，需要有效的**安全风险监控管理体系**去实现对移动互联网医疗应用的风险监控、风险评价及处置、风险事件通报，从而提高移动互联网医疗应用安全防护水平。

三、移动互联网医疗安全风险应对思路

为了应对移动互联网医疗应用存在的种种安全风险，为保护公民、法人和其他组织的合法权益，在国家层面陆续发布了一系列的安全政策。面对国家在移动互联网应用方面的监管要求，各级监管机构都在积极探讨和尝试移动互联网应用监管、监控解决方案。

面对移动互联网医疗系统安全纵深防御体系不健全、移动客户端应用渠道安全监测力度不够、AAA 安全机制薄弱、医疗健康数据生命周期安全保护机制和措施不足、行业层面缺乏风险监控管理手段等问题，**通过构建技术模型和管理机制相结合的安全风险监控管理体系**，来实现对移动互联网医疗应用的安全风险管控。

（一） 打造政府监管、行业自律、机构自治的三重安全防线

为了贯彻国家对于“互联网+医疗健康”政策要求，应对移动互联网医疗的安全风险，需要打造政府监管、行业自律、机构自治的三重安全防线，建立分级的风险监控管理模式，并围绕该模式建立事前备案、事中监测、事后追溯的闭环管理机制、风险处置和事件通报机制，降低移动互联网医疗领域的整体安全风险。

移动互联网医疗安全风险控制不是由单一部门来实现的，而是一个分级管理、多方协助的业务逻辑关系，需构建“政府监管、行业自律、机构自治”的管理模式。

一是政府监管。行业主管部门作为风控体系管理的主导者，

发挥规划、指导、行业牵引的作用，建立健全监管协调机制，确保各项监管举措落地实施。

二是行业自律。风控体系管理的实际操作更多地要依靠行业性联盟，通过行业组织的自律行为实现。联盟配合行业主管部门落实相应的管理性和技术性工作，为监管要求落地提供支撑。

三是机构自治。医疗和卫生机构落实风控主体责任，加强安全内控和自我约束，主动接受行业自律和社会监督，建立健全投诉响应、应急处置、风险补偿、安全责任等机制，切实保障用户合法权益。

（二） 构建技术模型和管理机制相结合的安全风险监控管理体系

安全风险监控管理体系见图 2 所示。

图 2：移动互联网医疗应用风险监控管理体系

图片来源：中国评测软信中心，2020 年 9 月

(1) 行业主管部门：行业主管部门作为安全风控管理体系的主导者，明确行业监管目标和监管流程，协调相关资源，制定

相关监管协调机制，完成行业管理模型顶层设计。

(2) 区域监管机构：包含区域有移动应用监管需求的各类组织和机构，通常情况下由各区域或地方卫健委承担该角色，对属地内的移动应用进行风险监测和汇总，收集的数据进行分析统计后向行业管理主体平台进行上报，并接收行业管理主体发放的移动应用风险提示，根据风险提示进行核查。

(3) 终端监控节点：风控监管技术落地单位，包括各类型医院、各种医疗服务机构，他们通过技术和管理手段对所属移动应用按照监控规则进行数据采集并向区域或地方监管机构上报。

(4) 标准支撑组织：本着行业自管、自控、自律原则，倡议在互联网医疗领域成立安全风控联盟，依据行业顶层设计，制定行业风控标准规范，建立**风控汇聚平台**，为技术实现提供依据。

(5) 技术支撑单位：依据行业标准提供多技术维度技术保障解决方案，实现风险管控目标。

移动互联网医疗安全风险监控管理体系从构建技术模型和建立管理机制两个方面来实现**主动**、**持续**、**动态**的安全风险管控，协助各类监管机构建立一个长效的评估体系，对移动互联网医疗应用进行评估和抽查，同步执行发布备案、运行监管等管理措施。通过完善的备案、审核、监督、抽查等业务流程，保障移动应用的安全合规运行。

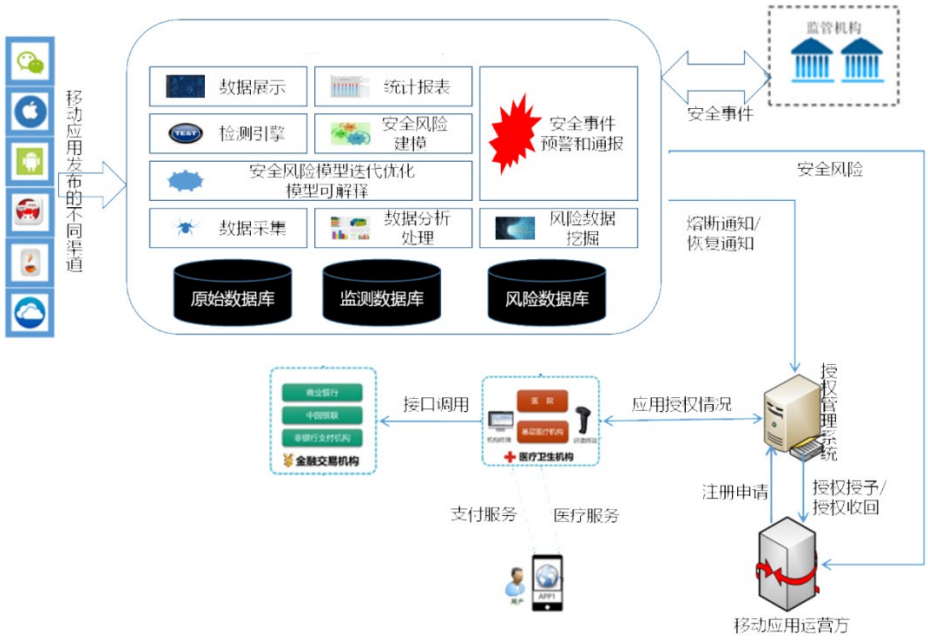
四、风险监控技术模型

为保证接入移动互联网医疗应用在公众使用时的安全性和合规性，对其应用安全风险进行控制，应构建应用安全风险监控技术模型。基于互联网移动应用标识认证技术实现对互联网业务应用的行为监测、行为追溯、移动互联网渠道监测、安全风险监测以及黑白名单管理，监管业务状况和系统风险情况，为管理模型提供技术支撑数据。基于该模型构建的平台应支持与互联网平台业务系统的对接，进而更全面的获取互联网业务平台各运营节点的实时运行数据，通过数据归类和分析，呈现集中监管展示。还可以根据当地主管部门的要求提供相应的数据接口，为互联网政策出台提供决策支撑。

（一） 移动互联网应用安全风控平台技术框架

构建主动、持续的安全风控平台，实现在行业互联网业务场景下，各类移动互联网医疗应用接入的安全风险发现、预警和分析。平台总体框架建议如图 3 所示:

图 3：建议技术框架结构



图片来源：中国评测软信中心，2020 年 9 月

技术要点主要包含以下几方面：

（1）建立数字化监测规则库

监测规则库主要由监测指标和监测规则构成。监测指标来自两方面：一是监管要求，根据国家、行业和主管部门对移动互联网医疗应用相关安全风险监管要求；二是应用本身的安全性数据。监控规则是规定了监控指标经过规则表达式处理后所要求取值范围。

（2）建立安全风险管理模型

该模型主要是在所建设的监测规则库基础上，研究在安全风险中风险所对应的监测规则及其规则直接所存在的相互关系，进而构建移动应用安全风险管理模型，通过所采集的移动应用的监测数据，进行分析计算得到移动应用的安全风险等级；根据安全风险等级，采取相关风险处置措施。

(3) 建立业务监测指标体系

主要针对互联网医疗移动应用建立业务监测指标体系，为核心业务建立全周期行为留痕监控。对互联网医疗应用的处方、处方的审方行为、整个处方开立流程和执行人情况、医嘱、病历书写、药品配送等关键节点数据的留痕情况进行全周期监控。监测指标涵盖医疗服务、公共卫生服务、家庭医生签约服务、医学教育和科普服务、医疗信息互通共享、三医联动等方面。

(4) 基于国密算法的授权管理

采用国密算法的数据安全加密组件，为无证书密钥及认证管理、身份认证服务、监测报告防篡改和审核结果签名等基础数据安全加密服务。

（二） 移动互联网医疗应用风控平台监测内容

监测的内容可包括以下三类:

(1) 资产清查: 管理移动互联网医疗应用清单，包括 App 及 Web 应用数据、渠道数据、SDK 数据和企业数据等，做到对风险对象了然于心。

(2) 应用合法性监测: 实现对移动互联网医疗应用本身在各种流通渠道有无被篡改、仿冒应用等风险监测; 展示发布来源、发布时间、发布版本、下载量、活跃度等统计特征; 进行移动应用关联的开发公司或个人信息、运营公司等的分析。

(3) 安全风险监测: 实现对移动互联网医疗应用在线自动化的常规漏洞扫描、静态安全检测、动态安全检测及恶意行为安全

检测等，通过风控平台从安全防护漏洞和恶意行为安全检测的角度对移动应用进行监测，确保正在使用的移动应用能够持续符合安全要求。

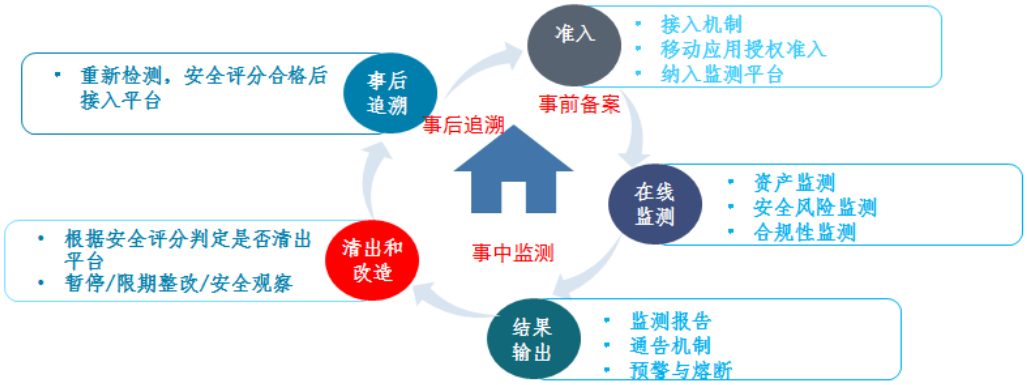
五、风险监控管理机制

通过事前备案、事中监测、事后追溯的闭环管理，安全评价及风险处置，安全风险事件通报这三个方面来构建风险监控管理机制，降低移动互联网医疗领域的整体安全风险。

（一） 建立事前备案、事中监测、事后追溯的闭环管理流程

移动互联网医疗应用风险监控的有效实现，必须建立与业务流程紧密耦合的闭环管理机制，采取事前备案、事中监测、事后追溯的线上、线下管理流程，如图 4 所示。

图 4：移动互联网医疗应用闭环管理流程



图片来源：中国评测软信中心，2020 年 9 月

1、事前备案

只有接入到移动互联网医疗应用安全风控平台的移动应用才能为患者提供医疗健康服务。移动互联网医疗应用建设单位需要向风控平台申请接入，通过审核后方可向风控平台注册并获取授权码，通过授权码纳入到风控平台。

2、事中监测

(1) 在线监测

风控平台定期对纳入的移动互联网医疗应用从各个公开发布渠道对资产、安全风险、合规性三个方面进行安全风险监测。

(2) 结果输出

若未出现安全问题，风控平台持续对其进行监测。通过大数据分析技术形成移动互联网医疗应用安全态势分析，可为主管机构提供决策分析，为出台相关的管理办法提供依据。

风控平台在移动应用出现安全风险时可对应用建设单位进行预警，及时提醒其进行安全防护加固。移动应用出现重大安全风险时，风控平台可采取熔断机制，暂停移动应用与重要后台系统的连接。

(3) 清出和改造

建立移动互联网医疗应用安全风险评价标准，对应用安全性进行评价，如未达到安全要求，则会被清出平台，限期整改。

3、事后追溯

被清出风控平台的应用，需要完成其安全性加固后，并符合安全要求后，方可申请重新接入风控平台进行管理。

（二） 建立移动互联网医疗应用安全风险评价及处置机制

1、建立安全风险评价机制

基于移动互联网医疗应用的漏洞情况、安全防护情况，渠道及版本等因素，构建风险评价模型，首先对风险进行分类，各风险类中包含风险子类或风险项；第二，为各项风险类或风险项按

照其影响程度分配权重；第三，在统计风险值时按照自底向上统计方法，聚合每层节点的统计分数后，形成最终的安全风险评分。

安全风险评分采用定量评分机制，100 分为满分，分数越低代表安全风险越高，评分结果分为 A、B、C 三个级别，评分在 60 分及以下为 C 级，表示移动客户端应用安全风险非常高；评分在 60¯80 分之间为 B 级，表示移动客户端应用存在一定程度的安全风险；评分在 80¯100 分之间为 A 级，表示移动客户端应用运行处于良好安全状态。

2、构建风险处置机制

对移动互联网医疗应用在运行过程中出现重大安全风险问题的处置:

(1) 在监测中发现盗版、近似应用等非法移动应用时，将通过邮件、电话等方式告知应用建设单位。

(2) 在监测中发现监测应用版本与备案版本存在大版本（大版本变更是指版本 x.y 的 x 或 y 发生变化）差异时，暂停该移动客户端应用接入。

(3) 在监测中如移动互联网医疗应用安全风险评分结果在 C 级时，对应用建设单位提出限期整改的通告，如应用建设单位在一定期限内进行整改且安全风险评分结果达到 B 级，继续进行监测；如指定期限内仍未达标，暂停移动客户端应用接入，应用建设单位应进行整改并达到 B 级后再行接入;

(4) 安全风险评分结果在 A 级，保持持续监测。

（三） 建立移动互联网医疗应用安全风险事件通报机制

首先，在接入时应提供相关负责人联系方式，当出现安全风险事件时，通过邮件等方式告知应用建设单位，提示注意相关安全风险并及时对确认的风险进行风险处置措施。

其次，移动互联网医疗应用出现重大风险后，除了告知应用建设单位外，同时会将重大风险情况分别上报给对应的监管机构，监管机构可以通过上报情况，及时对有重大安全风险的应用进行风险处置，减少风险造成的影响；除了重大风险外，定期生成移动互联网医疗应用安全风险统计分析报告，监管机构可及时了解目前移动互联网应用安全态势，制定相关管理办法或技术标准防范安全风险。

六、思考和建议

2019 年相继出台了《网络安全等级保护 2.0》和《信息安全技术 移动互联网应用程序（App）收集个人信息基本规范》等标准规范，加强了对移动互联网应用的安全合规要求，同时也要求在移动互联网应用安全风险监测和控制方面需进一步进行创新和完善：例如，鉴于主管单位的职责定位，如何保持长效的安全风险管理机制；面对新的安全风险和个人隐私保护需求，如何提高安全风险监测水平等。因此我们建议：

1、**成立安全风控联盟。**联盟应包含行业主管的技术支撑机构、第三方评测机构、医疗服务机构、安全服务机构等，统一对移动互联网医疗应用安全风控相关事宜进行管理，制定相关管理制度、技术标准和规范。

2、**制定移动互联网医疗应用备案管理办法。**通过管理措施，加强移动互联网医疗行业自律管理，提高移动互联网医疗应用软件安全水平，保护用户权益。

3、**研究个人医疗健康信息技术保护标准。**制定个人医疗健康信息分类分级和对应的安全保护要求，指导医疗健康行业提升个人信息保护水平。

————————————————

软件与信息系统测评工程技术中心

地　址：北京市海淀区紫竹院路 66 号赛迪大厦 7 层

传　真：86-10-88559332

手　机：86-13488713762（孟晓）

86-15801567456（王金珠）

邮　箱：mengx@cstc.org.cn（孟晓）

wzj@cstc.org.cn（王金珠）