《基于 GB/T 22239-2019 的医院网络与信息安全保障体系建设指南》（征求意见稿）

编制说明

一、任务来源

根据广东省网络空间安全协会《关于批准团体标准<等保 2.0 医院网络与信息安全保障体系建设指南>立项的公告》编制团体标准《等保 2.0 医院网络与信息安全保障体系建设指南》（以下简称“项目”），项目的负责单位是广东省网络空间安全协会，项目的提出单位为广东省网络空间安全协会医疗信息安全专业委员会。

二、制定标准的必要性和意义

随着我国各级各类医院信息化建设及应用的不断深入发展，为医院服务患者和运营管理带来了极大的便利，大大提高了医疗服务质量和医院的管理水平。与此同时，信息技术的广泛应用也带来了信息安全问题，医院信息安全事件时有发生并见诸报道，不仅严重影响医院的正常运作和管理，而且还威胁着患者的健康和隐私，给社会带来不安定的因素。

在 2019 年 5 月 13 日的国家标准新闻发布会上,《GB/T 22239—2019　信息安全技术 网络安全等级保护基本要求》（以下简称“等保 2.0”）正式发布，实施时间为 2019 年 12 月 1 日。等级保护范围涵盖的主要行业有能源、金融、交通、水利、医疗卫生、环境保护、工业制造、市政、电信与互联网、广播电视及政府部门，同时又适应了当前云计算、移动互联、物联网、工业控制和大数据等新技术的应用场景。

在全球网络空间安全面临新挑战、新风险，全国医疗行业信息化面临

新任务、新机遇，信息安全领域面临新等保、新管控要求的形势下，广东省网络空间安全协会、广东省医疗行业信息安全标准委员会组织行业专家和安全企业，集专家和一线技术人员的聪明才智，采用科学的系统工程方法和问题导向法，遵循《中华人民共和国网络安全法》和等保 2.0 标准体系，联合编制了本标准，以帮助医疗行业尤其是三级医院根据等保 2.0 的标准和要求，实施网络信息系统等级保护工程，建立相对完整的医院网络与信息安全保障体系。

三、主要起草过程

（一）前期工作

在等保2.0系列国家标准正式发布之前，项目前期工作组于2月28日起开展了多次专题调研，一是搜集国内外相关标准资料，认真研读对比；二是开展行业调查，通过走访医疗机构和网络安全企业，对我省医疗机构信息和网络安全保障体系建设的现状进行分析，对如何达到等保2.0系列标准的要求进行探讨；三是对新一代信息技术在智慧医院应用中的安全问题进行研究，对医疗云在网络资源、计算资源、存储资源各层面的安全问题进行分析，研究了移动互联网在医疗行业的应用场景及其可能带来的安全隐患，讨论了基于RFID、视频监控、红外传感和可穿戴设备等物联网技术的安全风险，对利用工控机、可编程控制器（PLC）或其它工控系统同类型技术建立起来的医院工控系统做了初步调研，对医疗大数据带来的隐私保护问题以及AI辅助系统可能受到的网络攻击、病毒感染、木马威胁等风险问题进行了探讨；四是进行多次研讨，在2019年5月9日之前共计召开了9次会议，涉及议题包括：三甲医院安全保障体系应达到的等级保护功能和性能要求，

对应的安全产品及安全管理手段，对等保2.0标准中的通用安全、云计算安全、移动互联安全、物联网安全、工业控制系统安全部分与《全国医院信息化建设标准与规范（试行）》中的相关条款进行一一对应，安全管理者与运维服务者的角色定位、责任分工，等等。旨在为医院信息化建设编制一部基于等保2.0网络安全要求的具有医疗行业特色的网络安全建设指南。

（二）起草过程

5月16日，项目启动会在广州举行，项目负责单位正式成立标准编制工作组，由饶坚任组长，王景保、胡江波任副组长。编制工作组成员来自天融信、安恒、广州市信息安全测评中心、赢领科技、中科慈航、轩辕网络等单位。

启动会明确了工作组成员的责任和任务，并按照团体标准管理办法规定，制定了标准编制工作计划，确定了标准名称、基本框架、时间进度，落实了编制组成员的具体分工。

启动会后，编制工作组各成员按照分工，分别编写标准的各部分内容，经5次内部讨论修改，形成标准讨论稿。

7月1日，项目负责单位邀请深信服、浪潮、蓝盾、绿盟、奇安信、亚信、网宿科技等国内知名网络安全服务企业参与讨论，征求各企业对标准讨论稿的修改意见。

7月25日，项目负责单位和提出单位共同邀请中山三院、暨大附属一院、省中医院、南方医科大附属三院、珠江医院、中山六院、肇庆市第一人民医院等医院信息中心负责人参与讨论，征求医院信息主管部门对标准讨论稿的修改完善意见。

8月2日，根据标准编制专家的建议，本标准名称由《等保2.0医院网络与信息安全保障体系建设指南》修改为《基于GB/T 22239-2019的医院网络与信息安全保障体系建设指南》，标准分为3部分：第1部分为技术要求，第2部分为管理要求，第3部分为软硬件系统符合性功能要求。

编制工作组汇总并采纳各方意见，经过多次修改完善，形成标准征求意见稿。

四、制订标准的原则和依据，与现行法律、法规、标准的关系

（一）编制思路

以往，国内各行业、各领域在落实等保要求所采取的相关措施，主要是从选择安全设备或软件层面去开展规划设计、提供解决方案，但忽略了网络和信息安全领域的“三分技术，七分管理”的规律。

本标准运用符合性设计思路，针对等保 2.0 和全国医院信息化建设标准和规范的要求，从技术（硬件设备及软件系统）和管理（管理方及运维服务方）两个维度给出解决方案和具体措施，也可以视为安全软硬件系统、管理侧措施、运维服务侧措施等三个维度。

本标准以三级医院遵循等保 2.0 的保护要求为基础进行设计，将等保二级和三级信息系统的保护要求也分别做了设计。

编制本标准的目的就是要解决安全体系建设方、实施方和运维方理解等保 2.0 要求“是什么”，明确“怎样做”、“谁来做”、“什么时候做”等问题。

（二）编制依据

本标准主要以信息安全、网络安全服务方面的国家标准、行业标准、地方标准和医疗系统信息化建设方面的技术规章，以及行业实际情况为依

据。

本标准编制的格式符合 GB/T1.1-2009《标准化工作导则第一部分：标准的结构和编写》的规定。

五、主要条款的说明

（一）本标准的主要框架

本标准主要框架如下：

前言

引言

1 范围

2 规范性引用文件

3 术语和定义

4 缩略语

5 等保 2.0 标准符合性措施设计

6 产品功能和性能指标设计

7 技术实现

附录 A 云计算安全

附录 B 移动互联安全

附录 C 物联网安全

附录 D 工控系统安全

附录 E 网络与信息安全软硬件系统（产品）基本功能和性能指标

（二）主要条款的说明

本标准以对照表的形式，将等保 2.0 的要求逐项列出，同时将全国医院信息化建设标准与规范中的信息安全条款与之对应。

本标准从三个维度（软硬件系统、管理视角、运维服务视角）分别给出对应的解决方案和采取的措施。

六、重大意见分歧的处理依据和结果

本标准在编制标准讨论稿及征求意见稿过程中没有发生重大分歧。

七、作为推荐性或强制性标准的建议及其理由

本标准作为推荐性标准。

八、贯彻标准的措施建议

（一）由网信、卫生、工信、公安网安、政数、财政等相关部门联合发文，引导医疗机构重视医院网络与信息安全保障体系建设。

（二）加强宣传力度，提高政府部门和医疗行业的网络安全意识，鼓励医疗机构主动依照本标准要求建设网络与信息安全保障体系。

（三）建议政府有关部门、医疗机构将网络与信息安全保障体系建设纳入政府信息化建设采购项目中同步建设，按照本标准要求建设网络与信息安全保障体系，规范医院信息化系统建设和管理，促进产业的良性发展。

（四）建议由医疗行业主管部门出台具体的实施细则，在全省各地推广，促进标准的落地实施。

九、其他应说明的事项

本标准计划编制 3 部分，本部分主要内容为医院落实等保 2.0 技术要求的措施；第二部分为落实等保 2.0 管理要求的措施；第三部分为落实等保 2.0 技术要求的软硬件系统符合性功能。

二〇一九年八月二十八日