智慧健康医疗行业网络安全体系研究综述

智慧健康医疗行业背景简介

1） 智慧健康医疗行业定义

智慧健康医疗是对数字健康、智慧医疗、“互联网+”等概念的统称，简单来说就是利用新一代信息技术、网络技术、物联网技术等，对健康医疗业务供给产生重大影响的新兴业务模式、新技术应用、新产品服务、新监管方式等，进一步完善全民健康信息服务体系，打造健康档案区域医疗信息平台，强化健康医疗大数据应用，规范数字智能医疗技术应用，创新互联网健康医疗服务模式，全面推动公共卫生、医疗健康、个人生活以及社会活动深度融合，实现患者与医务人员、医疗机构、医疗设备之间的互动，逐步达到健康医疗的网络化、数字化、智慧化。

2） 智慧健康医疗行业背景

健康医疗关乎民生福祉，数智技术重塑全球健康医疗未来。全球新冠疫情爆发背景下，以大数据、云计算、人工智能、互联网、物联网、区块链为特征的新一轮科技革命和产业变革正在加速演进，全球迎来数字化发展浪潮，卫生健康领域正在经历一场深刻变革。立足数字中国战略和健康中国理念，智慧医疗、数字健康、“互联网+健康医疗”等成为促进卫生健康行业高质量发展的关键词，既关乎人民健康，也关乎经济发展，已经成为数字经济时代国家综合竞争力的重要组成部分。“后疫情”时代，随着“健康中国”建设和深化医改的推进，健康医疗行业信息化建设正快速发展，新兴技术和健康医疗行业的深度融合带来了具有行业特点的新业务新场景，网络信息系统已经成为健康医疗行业提高决策水平、管理效率和运营能力的倍增器，伴随着“十四五”的到来，全民健康信息化建设迈入了新征程，健康医疗行业的网络化、数字化、智慧化进程明显提速。与此同时，随着网络联通范围的扩大和数据共享应用的深入，“互联网+”打破了行业的内外网边界，医疗联合体的建设增加了互联网暴露面，新技术发展导致各类新型网络安全风险层出不穷，行业信息安全防护体系亟待完善，数据应用安全问题日益凸显，网络安全面临新的威胁和挑战。

3） 智慧健康医疗研究目的

为贯彻落实习近平总书记全民健康战略思想，促进智慧健康医疗行业网络安

全能力建设和发展，本报告从智慧健康医疗行业背景出发，解读国内外有关健康医疗政策演进情况，总结“大卫生、大健康”理念下的智慧健康医疗发展成果和主要趋势，深度研究智慧健康医疗行业的主要安全问题，给出了行业网络安全体系针对性的思考和建议，为中国健康医疗行业的未来网络安全发展决策提供参考，为行业高质量的数字化安全转型升级提供可期的解决思路。

智慧健康医疗行业政策演进

随着健康医疗数字化转型已成为全球发展的共识，智慧健康医疗上升至全球战略，国内外发布了一系列政策文件支撑智慧健康医疗行业发展。

1） 智慧健康医疗全球政策

世界卫生组织（World Health Organization，WHO)智慧健康医疗政策。世界卫生组织发布的政策主要有：2016 年的《监测和评估数字卫生保健干预措施的指南》主要指导各国政府开展数字卫生保健技术评估。2018 年的《数字卫生保健分类标准 1.0》用于统一和规范数字技术在医疗健康领域应用的通用语言。2019 年的《全球数字卫生保健战略 2020- 2024》、《关于加强卫生体系数字技术应用的建议指南》正式号召全球各国积极制定国家层面数字健康建设与转型计划。2020 年的《卫生体系数字技术应用投资指南》、《数字卫生保健全球战略草案 2020- 2025 年》，为各国和地区制定数字健康建设和转型提供系统化指南，并提出一系列推进举措和行动框架。

国外主要经济发达体在智慧健康医疗方面的政策。美国发布《21 世纪医疗法案》《数字健康创新行动计划》等政策，美国食品药品监督管理局（Food and Drug Administration，FDA）成立数字健康卓越中心，旨在推动智慧健康医疗体系建设。欧盟发布《通用数据保护条例》、《评估医疗服务数字化转型的影响》、《欧洲数据战略》、《数字服务法》《数字市场法》等，重在智慧健康医疗市场行规范建设。德国出台《电子卫生法》、《数字供应法案》，推性智慧健康医疗服务先行。英国出台《2020 年个性化医疗与保健：行动框架》、《英国数字化战略》、《设计评估：数字健康产品评估指南》、《数字健康和数据驱动型医疗技术指南》等，发布了系列智慧健康医疗技术指南。

2） 智慧健康医疗国内政策

党中央、国务院高度重视智慧健康医疗行业发展。

2013 年，国务院发布《关于促进健康服务业发展的若干意见》（国发〔2013〕

40 号）中提出要推进健康服务信息化。一是制定相关信息数据标准，加强医院、医疗保障等信息管理系统建设，充分利用现有信息和网络设施，尽快实现医疗保障、医疗服务、健康管理等信息的共享。二是逐步扩大数字化医疗设备配备，探索发展便携式健康数据采集设备，与物联网、移动互联网融合，不断提升自动化、智能化健康信息服务水平。由此，我国进入互联网医疗时代。

2014 年，国家卫生计生委（国卫医发〔2014〕51 号）印发《关于推进远程诊疗的建议》允许医疗机构提供远程医疗服务。

2015 年《国务院关于积极推进“互联网+”行动的指导意见》（国办〔2015〕40 号）中提出推广在线医疗卫生新模式，发展基于互联网的医疗卫生服务，支持第三方机构构建医学影像、健康档案、检验报告、电子病历等医疗信息共享服务平台，逐步建立跨医院的医疗数据共享交换标准体系。

2016 年《关于促进和规范健康医疗大数据应用发展的指导意见》（国办发〔2016〕47 号）中指出以“互联网+健康医疗”模式，进一步推进网上预约分诊、检验结果获取及上传、医保联网等便民惠民应用，发展智能化远程健康医疗设备。

2016 年 10 月，中共中央、国务院印发《“健康中国 2030”规划纲要》，提出了大健康的发展理念，确立了以促进健康为中心的“大卫生、大健康”理念，提出要完善全民健康信息服务体系建设，全面建成统一、权威、互联互通的人口健康信息平台，规范和推动“互联网+健康医疗”服务。互联网+健康医疗第一次上升到国家战略层面，是我国健康现代化建设的一个里程碑政策。

2018 年 4 月，国务院办公厅印发《关于促进“互联网+医疗健康”发展的意见》，提出了促进互联网与医疗健康深度融合发展的一系列政策措施。一是健全“互联网+医疗健康”服务体系：从发展“互联网+”医疗服务，创新“互联网+”公共卫生服务，优化“互联网+”家庭医生签约服务，完善“互联网+”药品供应保障服务，推进“互联网+”医疗保障结算服务，加强“互联网+”医学教育和科普服务，推进“互联网+”人工智能应用服务等七个方面，推动互联网与医疗健康服务融合发展。二是完善“互联网+医疗健康”支撑体系：加快实现医疗健康信息互通共享，健全“互联网+医疗健康”标准体系，提高医院管理和便民服务水平，提升医疗机构基础设施保障能力，及时制订完善相关配套政策。三是加强行业监管和安全保障：强化医疗质量监管，保障数据安全。

2020 年，国家卫生健康委先后印发《关于加强信息化支撑新型冠状病毒感染的肺炎疫情防控工作的通知》《关于在疫情防控中做好互联网诊疗咨询服务工作的通知》《关于深入推进“互联网+医疗健康”“五个一”服务行动的通知》等系列文件，充分发挥“互联网+健康医疗”的作用，为疫情防控、精准施策、惠民服务等提供有力支撑，为推进互联网医疗、电子健康卡、全面健康信息平台、医防融合等提供重点保障。特别是《关于深入推进“互联网+医疗健康”“五个

一”服务行动的通知》，通过推进“一体化”共享服务、“一码通”融合服务、“一站式”结算服务、“一网办”政务服务、“一盘棋”抗疫服务等 5 个方面、14 项重点举措，切实提升了“互联网+医疗健康”便民惠民服务水平，深入推进了新一代信息技术在医疗卫生健康行业的融合发展，加强了线上监管，进一步优化了资源配置，提升了服务质量效率。

2021 年 7 月，国家发展改革委、国家卫生健康委、国家中医药管理局和国家疾病预防控制局共同编制了《“十四五”优质高效医疗卫生服务体系建设实施方案》，从总体思路、公共卫生防控救治能力提升工程、公立医院高质量发展工程、重点人群健康服务补短板工程、促进中医药传承创新工程、资金安排、保障措施方面做了具体要求，进一步推动了优质医疗资源扩容和区域均衡布局，提高了全方位全周期健康服务与保障能力。

随着健康医疗行业新模式新业态新场景蓬勃发展，健康医疗大数据加快推广应用，物联网、大数据、人工智能、区块链等新技术与卫生健康行业进一步融合，智慧健康医疗在方便群众看病就医、提升医疗服务质量效率、增强经济发展新动能等方面将发挥越来越重要的作用。

智慧健康医疗行业发展趋势

“互联网+”时代，随着大数据、人工智能、云计算、物联网、区块链和 5G 等新兴技术在健康医疗应用的进一步落地发展，智慧健康医疗在健康信息化、医院信息化、医疗信息化等正呈现出新的发展态势。

健康信息化方面，依托顶层设计引领区域平台从点及面发展，通过区域卫生信息化建设基本形成了四级平台互联互通体系，跨部门数据共享比例不断提高，截至 2020 年底，基于国家全民健康信息平台的数据服务总调用量超过 700 亿次，共覆盖全国 8 亿人口。

医院信息化方面，以电子病历为核心的医院信息化平台和系统建设不断完善，智慧医院建设成为医院发展的方向，致力于为患者、临床、科研、管理提供全方位智能服务。医院信息化步入数字化、智慧化转型轨道，预约服务、自助服务、自主支付、智能候诊、患者定位等惠民功能普遍开通，医疗服务、医技服务、移动医疗、运营管理、医疗协同等数字业务普遍展开。

医疗信息化方面，基于物联网的数据收集、大数据和云计算的数据分析和 5G 网络的数据传输和分析下，我国的健康医疗行业呈现出更智能的发展，智慧健康医疗成为医疗信息化的最终目标。医疗的全面信息化也是智慧医疗的重要支柱，在物联网、5G、大数据和 AI 的赋能下，我国医疗信息化的建设正向着标准化、集成化、智能化、移动化和区域化方向发展。

“十四五”时期健康医疗信息化工作需要适应新时期网络化、数字化、智慧化的健康发展新需求和人民新期待，2021 年举办的中国卫生信息技术/健康医疗大数据应用交流大会通过系统回顾我国卫生信息化、医院信息化、医疗信息化的业务领域发展历程，提出了我国健康医疗行业的十大发展框架思路，具体可总结如下图所。

智慧健康医疗安全现状分析

智慧健康医疗行业创新发展为卫生部门和医疗机构以及公众带来更加便捷服务的同时，也同步面临网络安全的痛点难点问题，主要体现在以下方面。

1）安全合规有待完善

整个医疗行业的网络安全等级保护工作开展情况一般。在 CHIMA《2018-2019 年度中国医院信息化调查报告》中，参与调查的 839 家医院中仅有 43.95%通过了等级保护测评，其中三级医院比例明显大于三级以下医院，三级以下医院中 75%未开展过等级保护测评。即使通过等级保护测评，但行业化的网络安全制度和规范还有待健全，基础设施比较薄弱，防护技术措施比较单一等。如中国评测网安中心分析了 35 家开展网络安全等级保护测评的医疗信息系统案例后发现，部署网络准入系统的有 0 家，对接入网络的终端基本没有进行 IP 限制，也没有必要的认证机制。可以看出医院对网络安全愈发重视，但整体推进态势仍显缓慢。

2）数据安全方兴未艾

近年来，国内外由于医疗信息系统被入侵而导致的信息泄露事件多次发生。数据泄露成为家常便饭，医疗行业网络安全形势日益严峻。中国评测网安中心分

析了 35 家开展网络安全等级保护测评的医疗信息系统案例后发现，在数据保护方面 38%的系统没有数据库审计，只有 2%的单位具有灾备服务器，60%的医疗信息系统数据备份机制不健全，包括无异地备份机制、备份策略不合理等问题，72%的医疗信息系统在数据存储和传输过程中未采取加密措施，大部分医疗信息系统没有完善的数据保护机制。随着数据安全法的出台，健康医疗大数据作为国家重要的基础性战略资源，如何提出推进数据汇聚和发掘，深化大数据在健康医疗行业中的安全创新应用，推动健康医疗大数据信息安全互通和共享开放，行业化的数据安全治理之路道阻且长。

3）**隐私保护来势迅猛**

随着健康医疗行业互联化、移动化、在线化的服务模式普及，暴露在互联网中健康医疗信息系统漏洞急剧增多，涉及公民个人信息的数据库数据安全事件频发，数据安全与个人隐私面临严重挑战。CNCERT 在《2019 年我国互联网网络安全态势综述》中，对电力、石油天然气、医疗健康、煤炭、城市轨道交通等 2249 套重点关键基础设施行业暴露的联网监控管理系统进行了漏洞威胁统计分析，医疗健康行业监测 709 个系统，存在高危漏洞的系统达 510 个，占比高达 71.93%；监测的系统存在高危漏洞的 733 个，医疗健康行业贡献的存在高危漏洞的系统数占比高达 69.58%。随着 2020 年新冠肺炎疫情在全球的暴发和蔓延，有组织的 DDoS 攻击、钓鱼邮件攻击等网络攻击呈高发频发趋势，随着个人信息保护意识加强和监管驱严，预计未来智慧健康医疗行业隐私保护形势不容乐观。

4）**新兴技术面临挑战**

智慧健康医疗行业信息化建设由分散到整体、由系统到集成的发展过程中，信息服务体系的应用持续快速发展，新技术与医疗卫生服务融合持续加速，健康医疗大数据成为新的行业生产要素，健康医疗领域广泛运用大数据、人工智能、区块链、5G 等数字技术，辅助卫生管理决策，加强健康数据共享交换，创新诊疗服务模式，扩展医疗服务空间，推动优质医疗资源流动等。新技术在为行业带来便利和动能的同时，如何安全融合数字技术和业务场景，面临新的安全挑战。

5）**密码应用困难重重**

随着密码法和密码应用制度成为合规要求，编制密码应用方案，配备密码设施，通过密码应用测评成为健康医疗信息化系统的标配。而由于智慧健康医疗行业长期以来并未深入考虑国产密码的应用，基础设施不够健全，业务应用系统庞杂，业务应用厂商众多，基于目前的行业信息化现状通过密码测评，基本不太现

实，实现智慧健康医疗行业化的国产密码应用困难重重。

6）**安全人才比较匮乏**

智慧健康医疗行业信息化发展过程中，人才队伍建设不足主要体现在信息技术管理机构编制数及工作人员数量不足，特别是网络安全人员严重缺乏，既懂行业又懂安全的高水平人才更是极度匮乏。据有关统计，近五年来，省级卫生健康统计信息技术管理机构编制数量和在岗人员数量无明显增加。部分省（自治区、直辖市）甚至出现减少现象。智慧健康医疗行业政策要求高，专业性强，新型信息技术迭代快，现有网络安全人才队伍远远不能满足发展需要。

智慧健康医疗安全体系思考

面对网络安全新形势、新挑战，智慧健康医疗行业需要坚持以习近平总书记关于网络强国的重要思想为指导，坚持总体国家安全观、树立正确的网络安全观，强化顶层设计和标准研制，从网络安全的基础合规、数据安全、密码应用、业务融合、实战攻防等方面进行全面的体系化思考，打造最硬核的行业化网络安全体系，有效提高行业网络安全保障能力。

1）**以政策合规为核心基础的网络安全体系**

以全民健康信息化的深化应用和创新发展为主线，针对关键信息基础设施要求有组织、有目的、高强度网络攻击愈加明显的趋势，进一步落实网络安全等保和关键基础设施保护制度，建设持续合规的网络安全防护体系，提升抵御网络攻击威胁的能力，构建全适应智慧医疗健康行业化建设和健康医疗大数据应用发展的网络和信息安全保障体系

2）**以数据安全为核心目标的网络安全体系**

以数据安全法为契机，加强行业数据安全治理和个人隐私保护，出台数据安全和隐私保护制度，深度融合数据、隐私等安全技术和医疗健康行业场景，完善数据安全防护体系，并针对性的提供解决方案；建立行业化的个人信息和重要数据安全监管技术体系，常态化开展数据安全审查评估，深入贯彻行业数据安全和隐私保护合规建设。

3）**以密码应用为核心支撑的网络安全体系**

行业主管部门协同密码主管部门出台配套政策，进一步推进信创集成建设和

运维，制定行业化密码测评制度标准，在行业中全面推进密码测评工作，全面构建行业网络可信体系，加强数据安全融合利用监管，强化全民健康数据隐私保护，发挥国产替代、国产密码、安全认证、检测防护的集成整合作用，保障网络、设备、业务系统的运行安全和医疗健康数据信息安全。

4）**以业务融合为核心方向的网络安全体系**

在疫情影响下，远程医疗、互联网医院、智慧医院等新模式得到快速发展，5G、AI、大数据、区块链、物联网等新技术场景得到落地应用，需要加大对新技术新场景的网络安全融合技术研究，借鉴金融、互联网等行业成功安全举措，在保障网络信息和数据安全前提下，促进行业创新发展。

5）**以实战攻防为核心能力的网络安全体系**

智慧健康医疗行业的信息安全人才培养机制和手段比较匮乏，应结合行业属性和特点，构建以威胁情报为中心的行业安全防卫评估体系，打造行业专属的网络安全实战攻防演练平台，利用多方力量开展专业化的内在风险和成熟度评估，实现安全理论与行业实战的充分结合，壮大行业网络安全人才队伍，形成行业网络安全的新能力。