



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

基因测序数据安全 研究报告 (2025 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

2025 年 7 月

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、深圳华大智造科技股份有限公司、深圳华大基因股份有限公司、北京惠泽智信科技有限公司、苏州吉因加生物医学工程有限公司、北京优迅医疗器械有限公司。

编写组专家：

中国信息通信研究院云计算与大数据研究所：李曼、崔伟男、赵阳光、徐冰心、崔日宏、金越、赵梓杰、赵靖如。

深圳华大智造科技股份有限公司：颜妙丽、史兴、苗继业、李福斌。

深圳华大基因股份有限公司：向嘉乐。

北京惠泽智信科技有限公司：薛新华、宋平、车宇洋、赵红姣。

苏州吉因加生物医学工程有限公司：田超。

北京优迅医疗器械有限公司：张静波。

目 录

一、基因测序概述	1
(一) 基因测序技术线路多元, 各类技术各有千秋	1
(二) 基因测序应用场景广泛, 市场拓展潜力巨大	4
(三) 基因测序链路环节相连, 数据类型复杂多样	6
(四) 基因测序数据体量激增, 数据安全不容忽视	7
二、全球基因测序仪数据安全现状	9
(一) 美国持续加强基因测序仪数据安全	9
(二) 欧盟对基因测序仪数据安全进行严格监管	13
(三) IMDRF 不断发布医疗器械网络安全新指南	17
(四) IEC 积极制定医疗器械数据安全标准	18
(五) 我国基因测序仪的数据安全管理在不断加强	19
三、安全风险挑战	24
(一) 身份验证和访问控制不足造成的风险挑战	24
(二) 第三方供应链安全风险挑战	25
(三) 数据传输过程的安全风险挑战	26
(四) 数据存储、计算过程的安全风险挑战	27
(五) 数据意外丢失或损坏造成的安全挑战	27
(六) 基因组数据共享的隐私安全挑战	28
四、安全技术与措施	28
(一) 身份识别与权限控制	29
(二) 系统安全加固	29

(三) 安全日志审计	30
(四) 漏洞管理和网络安全补丁升级	31
(五) 密码学的应用	31
(六) 软件供应链管理	32
(七) 实施数据保护与备份	33
五、案例研究与分析	34
六、总结与建议	36
(一) 基因测序数据网络安全至关重要	36
(二) 基因测序数据网络安全发展建议	37
附 录	39
一、基因测序网络安全相关政策	39

表 目 录

表 1 不同基因测序技术对比 4

一、基因测序概述

(一) 基因测序技术线路多元，各类技术各有千秋

基因测序技术 (DNA Sequencing) 是指获得目标 DNA 片段碱基 (包括腺嘌呤 A、胸腺嘧啶 T、胞嘧啶 C 与鸟嘌呤 G) 排列顺序的技术,它是基因组学的核心技术,也是现代生命科学研究中最广泛应用的重要技术之一。科学家们提出基于基因组学的两个重要理念:“生命是序列的”和“生命是数据的”,基因测序技术能够帮助科学家获得人类基因组以及其他许多动植物和微生物物种的完整 DNA 序列以至于更加深入地了解生物体。随着技术进步,该技术已经逐渐应用于分子诊断领域。

基因测序技术大致经历了从“前直读”到“直读”、从手工到自动化、从平板电泳到毛细管凝胶电泳再到大规模并行高通量测序四个阶段。

第一代测序技术: Sanger 测序。始于 1977 年弗雷德里克·桑格 (Frederick Sanger) 发表的双脱氧核苷酸末端终止法,因而被称为“Sanger 测序”。Sanger 测序因为检测准确度高,至今依然被称为基因检测的金标准。该方法的原理为: 核酸模板在 DNA 聚合酶、引物、4 种 dNTP(其中的一种用放射性 P32 标记)存在条件下复制时,在四管反应系统中分别按比例引入四种 ddNTP,因为双脱氧核苷缺乏 3'-OH,所以只要双脱氧核苷掺入链末端时,该链会停止延长,若链端掺入单脱氧核苷,链就可以继续延长。如此每管反应体系中便合成以各自的双脱氧碱基为 3'端的一系列长度不等的核酸片段。反应终止后,分四个

泳道进行凝胶电泳，分离长短不一的核酸片段，长度相邻的片段相差一个碱基。经过放射自显影后，根据片段 3'端的双脱氧核苷，便可依次阅读合成片段的碱基排列顺序。**Sanger** 测序因操作简便，得到广泛的应用。在此基础上发展出多种一代 DNA 测序技术，其中最重要的是毛细管荧光自动测序技术。

第二代测序技术：高通量测序。高通量测序（**high-throughput sequencing**）是基于 PCR 和基因芯片发展而来的 DNA 测序技术。其基本工作原理是：高通量测序开创性地引入了可逆终止末端，实现了边合成边测序；在 DNA 复制过程中通过捕捉新添加的碱基所携带的特殊标记（一般为荧光分子标记）来确定 DNA 的序列。由于在高通量测序中，单个 DNA 分子必须扩增成由相同 DNA 组成的基因簇，然后进行同步复制，来增强荧光信号强度，从而读出 DNA 序列；而随着读长增长，基因簇复制的协同性降低，导致碱基测序质量下降。高通量测序适合扩增子测序（如 16S、18S、ITS 的可变区），而基因组、宏基因组 DNA 则需要使用鸟枪法打断成小片段，测序完毕后再使用生物信息学方法进行拼接。目前，高通量测序技术在全球范围主要包括以 **Illumina**（因美纳）为代表的桥式 PCR 扩增与边合成边测序结合的技术路线、以 **Thermo Fisher** 为代表的乳液 PCR 扩增与半导体测序结合的技术路线和以华大智造为代表的 DNA 纳米球与联合探针锚定聚合（**combinatorial probe anchorsynthesis, cPAS**）相结合的技术路线三大技术流派。国产测序平台除了华大智造外，华因康、真迈生物、菲鹏生物等公司也在研制自产测序仪并陆续注册获批。在国产测序仪

领域，我国虽然起步较晚，但是已经逐步达到国际先进水平。

第三代测序技术：单分子测序。目前市场上单分子测序技术的主流代表为美国太平洋生物科学公司（**Pacific Bioscience, PacBio**）和英国 **Oxford Nanopore** 公司开发的三代测序技术。**PacBio** 测序技术工作原理为：利用 4 种荧光分别标记 4 种 dNTP，在测序芯片的底部做出许多与入射光波长相应的小孔，特定的孔径保证了入射光在小孔中只走很短的距离。只够照到正好与酶在相互作用的荧光 dNTP 底物，把聚合酶锚定在测序芯片的底部；让 DNA 链与酶结合，进行测序；测序时，荧光 dNTP 与酶+DNA 模板形成复合物，短暂结合；荧光 dNTP 被激光照射，发出荧光，荧光被检测到；酶反应过程，一边使链延伸，一边使 dNTP 上的荧光基团脱落，进行聚合反应的同时测序持续进行。而 **Nanopore** 测序技术核心原理则是：是利用一个纳米孔，孔内共价结合有分子接头，将纳米孔蛋白固定在电阻膜上后，再利用动力蛋白牵引核酸穿过纳米孔；当核酸通过纳米孔时使电荷发生变化，从而引起电阻膜上电流的变化；由于纳米孔的直径非常细小，仅允许单个核酸聚合物通过，而 **ATCG** 单个碱基的带电性质不同，因此不同碱基通过蛋白纳米孔时对电流产生的干扰不同，通过实时监测并解码些电流信号便可确定碱基序列，从而实现测序。在国内测序市场，华大智造也刚刚发布了自己的纳米孔测序技术—**CycloneSEQ™** 测序技术，成为首具备备激发光、自发光和不发光三种不同技术原理的基因测序公司。

表 1 不同基因测序技术对比

测序技术类型	Sanger 测序技术	高通量测序技术			单分子测序技术	
	毛细管电泳法	桥式 PCR 扩增与边合成边测序	乳液 PCR 扩增与半导体测序	DNA 纳米球与联合探针锚定聚合测序	零模波导孔技术	纳米孔测序技术
所属公司	ABI (已被 Thermo Fisher 收购)	Illumina	Thermo Fisher	华大智造	Pacific BioSciences	Oxford Nanopore
读长	几百至 1x1000 bp	1 x 36 bp 至 2 x 300 bp	1 x 200 bp 至 1 x 600 bp	1 x 50 bp 至 1 x 400 bp	几十 Kb	几十 Kb
最大通量/运行	240 kb	6 Tb	24 Gb	72 Tb	120 Gb	7 Tb
准确率	>99.9%	>99%	>99%	>99%	>90%	>90%
优缺点	测序读长长、准确率高但测序通量低、成本高	测序通量高、速度快、成本较低且自动化程度高，但读长较短			超长读长和实时测序但准确率偏低、成本偏高	
主要应用	司法鉴定等	生殖健康、肿瘤基因检测、传感染鉴定，司法鉴定等			科学研究等	

数据来源：《分子诊断技术与应用》

（二）基因测序应用场景广泛，市场拓展潜力巨大

基因测序技术作为生命科学领域的重要分支，可以对生物体内的基因进行全面深入的研究分析，应用领域十分广泛。随着测序技术的快速发展和测序成本的不断降低，基因测序已经逐步在医疗健康、生物医药、农业、环境保护、司法鉴定等领域广泛应用。

随着社会发展、人们健康意识的提高以及相关政策的支持，基因测序技术在医疗健康领域的市场应用场景快速拓展。依据需求的不同，基因测序技术在医疗健康领域的应用可分为研究性测序、诊断性测序和个性化医疗测序。其中，研究性测序主要服务于科研机构、高等院

校以及制药企业等，科研人员利用高精度的基因测序技术，深入解析基因的结构与功能，揭示生命活动的奥秘，为新药研发、遗传病研究及作物改良等提供强有力的数据支持。如，基因测序技术可应用于病因研究、疾病预后评估、疾病自然史研究等，通过对癌症患者进行大规模的全基因组测序，增进研究人员对疾病的理解，有利于提高新药筛选的效率。诊断性测序主要是借助测序技术来帮助医生确定患者是否存在特定的基因突变或变异，诊断疾病或者确认遗传病的存在，进而指导治疗方案的制定。如，在产前筛查中，帮助检测胎儿是否存在染色体异常或遗传性疾病；在肿瘤诊断中，帮助检测肿瘤相关的基因突变，为肿瘤的精准治疗提供依据。个性化医疗测序主要是借助基因测序技术帮助医生了解患者的遗传背景，根据个体的基因组信息制定个性化的治疗方案，选择最适合患者的治疗方式、治疗药物和剂量等。如，在肿瘤治疗中，通过了解肿瘤的基因突变情况，选择针对性的靶向药物或免疫疗法；在遗传病治疗中，通过确定患者的基因型，选择最有效的治疗方案。随着技术的不断进步和成本的降低，基因测序技术在生物医药领域的应用仍不断拓展，如用于药物研发、疾病风险评估等。

此外，在农业领域，基因测序技术可用于农作物的育种，通过解析基因组序列，发现关键基因并进行选育，提高作物产量、抗病性和适应性。在环境保护领域，基因测序技术可用于检测水体、土壤和空气中的微生物和有机污染物，评估污染程度和生态风险，为污染治理提供科学依据。

根据有关数据显示¹，2021 年全球基因测序市场规模约为 157 亿美元，预期 2026 年增长至 377 亿美元。其中，中国基因测序市场规模为 15.9 亿美元，占全球市场的 10.13%，预期 2026 年增长至 42.35 亿美元。未来，在技术进步、政策支持、市场需求等多方因素的影响下，基因测序市场将继续保持逐年增加的局面。

（三） 基因测序链路环节相连，数据类型复杂多样

基因测序产业链路主要包括上、中、下游三个环节，其中，产业链上游主要包括基因测序仪器、耗材以及试剂的供应，为基因测序提供平台和解决方案。当前，国内外主要供应商包括因美纳（Illumina）、赛默飞（Thermo）以及国内的华大智造、华大基因、达安基因、贝瑞基因等。产业链中游主要提供包括样本处理、测序、数据分析等的基因测序服务。国内主要服务商包括迪安诊断、燃石医学、艾德生物等。产业链下游主要为基因测序结果的使用方，可分为科研和临床应用两大领域，主要包括医院、药企、科研机构、患者等。基因测序产业的各个环节紧密相连，相互依赖，基因测序数据也在该链路之间进行传递。

此外，基因测序流程涉及多个环节，数据处理流程复杂。基因测序起点为 DNA 提取与文库构建，从生物体的细胞中提取出 DNA，并对其进行纯化，以获得高质量的 DNA 样本，再将提取后的 DNA 片段插入载体中，进行文库构建，构建测序文库。测序过程为利用 Sanger 测序、高通量测序和单分子测序等技术，对构建好的文库进行

¹ 数据来源：智研咨询—<https://caifuhao.eastmoney.com/news/20240717132431334923290>

DNA 序列信息的获取。基因测序的数据处理则是对获取的 DNA 序列信息进行处理分析，涉及数据质控、预处理、序列对比、变异检测、结果解释与数据分析、结果可视化等关键步骤。

基因测序数据结果类型复杂多样，根据其研究目的和测序技术的特点，可主要分为 DNA 测序数据、RNA 测序数据和表观基因组测序数据等。DNA 测序数据主要包括：适用于个体基因组分析、变异检测（如 SNP、插入-缺失变异）以及复杂疾病研究的全基因组测序（WGS）；适用于遗传性疾病研究、肿瘤相关基因突变检测的全外显子测序（WES）；适用于临床精准医疗、基因组特定区域突变分析的靶向区域测序（Targeted Sequencing）。RNA 测序数据主要包括：适用于基因表达量分析、新的转录本发现和可变剪接研究的转录组测序；适用于免疫细胞亚群分类、肿瘤微环境研究和发育生物学等领域研究的单细胞 RNA 测序。表观基因组测序数据主要包括：适用于癌症甲基化标志物研究和表观遗传调控机制分析的甲基化测序；适用于基因调控网络分析和组蛋白修饰模式研究的染色质可及性测序。此外，还有长读长测序数据，其读长可达 10,000 bp 以上，适合分析复杂结构变异，如重组基因组拼接和复杂重复区域检测。这些数据在科研和临床诊疗中发挥着重要作用，为疾病的诊断、治疗和预防提供了有力支持。

（四） 基因测序数据体量激增，数据安全不容忽视

近年来，基因测序技术飞速发展，广泛应用于生命科学各个前沿领域。它帮助科研人员深入探索生命奥秘，助力医生精准诊断、治疗

疾病，也为遗传学研究开拓了全新视野。但随着应用普及，基因测序数据量呈爆炸式增长，安全存储与管理压力骤增。根据有关数据显示²，基因测序的数据量平均每七个月就会翻一倍，2025 年全球测序能力预计将达到 Zb 级别，其中，仅人类全基因组存储的数据量就将达到每年 2-40Eb。

数据安全重要性日益凸显。国家安全方面：随着医疗器械与人工智能、云计算、网络技术的深度融合，医疗器械数据安全问题愈发显著，尤其是基因数据的保护成为重中之重。基因数据的汇集与分析，能深度揭示民族的遗传特质与疾病易感性等高度敏感信息。一旦这些信息落入敌对势力之手，将对国家安全构成不容忽视的潜在风险。**隐私保护方面：**随着基因测序技术的普及和成本的降低，越来越多的人开始接受并使用基因测序。但基因测序数据包含了大量的个人隐私，如遗传特征、健康状况、疾病风险等，一旦这些数据发生泄露或被滥用，可能会对个人的隐私造成侵害，严重影响个人的生活、工作以及心理健康。**伦理法律方面：**基因信息包含了个体最核心的遗传密码，涉及生物安全问题，一旦泄露或被滥用，后果不堪设想。比如，可能会导致个人隐私毫无保留地暴露，甚至引发基因歧视现象，对个人的就业、保险等权益造成严重损害。如何建立完善的防护机制，确保个体遗传数据的安全，已然成为当下亟待解决的重要课题。**医疗和科研方面：**基因测序数据在疾病诊治、新药研发等方面具有极高的应用价值。借助基因测序数据，医生可以更准确的判断病情，制定个性化的

² 数据来源：NVIDIA 英伟达—<https://m.elecfans.com/article/1994614.html>

治疗方案，科研人员也可以更加深入地了解发病机理，推动医学的科学发展。然而，如果基因测序数据被篡改或破坏，不仅直接影响到患者治疗效果和生命安全，甚至会严重影响科研进展和成果。此外，由于基因测序数据的特殊性，各国政府和相关机构对于基因测序的数据安全也愈加重视，纷纷出台相关法律法规保护其安全性。

二、全球基因测序仪数据安全现状

鉴于当前日益严重的数据安全问题，全球各个国家及监管机构都在不断强化医疗器械数据安全意识，陆续发布相关网络和数据安全的法规、要求、指南等，保证医疗器械数据的安全性，保障公众健康。基因测序仪预期与适配试剂配合使用，用于对样本中 DNA 或 RNA 分析，检测基因碱基数量和序列变化。基因测序仪作为实现基因测序的平台和工具，是一种关乎个人信息安全、国家安全的医疗器械，其网络和数据的安全性尤为重要，受到了国内外特别的关注和严格的管理。

（一）美国持续加强基因测序仪数据安全现状

美国 FDA（Food and Drug Administration，食品药品监督管理局）是由美国国会授权专门从事食品与药品管理的执法机构。FDA 一直是全球网络安全研究的引领者。为保障公众用械安全，FDA 对医疗器械网络安全的要求在不断加强，近年来发布了一系列相关的法规和标准，以使医疗器械满足网络、数据安全的要求。

同时在全球网络安全威胁不断增加、生物技术和信息技术持续融合的背景下，近期美国政府和国会出台了一系列行政令和立法议案，

加强在个人数据和生物学领域的安全。

医疗器械网络安全的上市前和上市后管理：2014 年 10 月 FDA 发布了医疗器械网络安全管理上市前提交内容的相关指南草案。在 2014 年到 2023 年的近十年时间里，网络安全形势快速发展，各国对网络安全威胁的认识也在逐步加深，FDA 也在逐步更新其考量点、管理范围以及管理的方法。为此该指南草案也在不断更新，最终于 2023 年 9 月 FDA 发布了最终版指南文件《Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions》（医疗器械网络安全：质量体系注意事项和上市前提交内容）。该指南重点强调了产品的设计安全，网络安全是产品安全 and 质量体系法规的重要内容，安全风险管理是制造商整个质量体系的一个组成部分，网络安全应贯穿于产品整个生命周期之中。同时该指南还明确地概述了 FDA 对上市前提交内容的建议，以及如何解决网络安全问题（包括设备标签）。FDA 表示：“这些建议旨在促进一致性，促进有效的上市前审查，并帮助确保上市的医疗器械对网络安全威胁具有足够的抵抗能力”。

对于上市后医疗器械网络安全的管理，FDA 在 2016 年发布指南《Postmarket Management of Cybersecurity in Medical Devices - Guidance for Industry and Food and Drug Administration Staff》，旨在告知医疗器械行业以及 FDA 工作人员对已上市销售的医疗器械网络安全漏洞的建议。该指南强调医疗器械生产企业应该监控、识别和解决网络安全漏洞，并将其作为医疗器械上市后管理的一部分。基于风

险思维的理念，该指南建立了一个基于风险的框架，用于评估上市后医疗器械网络安全漏洞，以及何时向监管机构报告。对于生产企业为纠正器械网络安全漏洞和可能对健康构成风险的漏洞而采取的轻微变更，FDA 要求医疗器械生产企业通知监管机构。对于器械对健康构成的风险可能导致患者受到伤害，FDA 建议评估患者伤害风险是否得到充分控制。同时，评估应是基于对攻击可能性的评估，攻击对产品安全性和基本性能的影响，以及攻击对患者伤害的严重程度。

NIST 网络安全框架：FDA 建议医疗器械自愿性地采用 NIST—美国国家标准与技术研究院（National Institute of Standards Technology）网络安全框架，该框架为全球公认的网络安全框架。FDA 指导文件与 NIST 网络安全框架保持高度一致，为制造商提供确定网络安全风险和漏洞的公认风险和影响评估工具。NIST 网络安全框架包含五个核心功能：识别（ID）、保护（PD）、检测（DE）、相应（RS）和恢复（RC）。2018 年 4 月，NIST 发布了网络安全框架 1.1 版本，2023 年 12 月更新发布了 2.0 版。医疗器械制造商通过实施 NIST 网络安全框架，可以提高医疗器械产品的安全性，更好地保护患者数据和隐私。

漏洞管理：FDA 认可标准 ISO/IEC 29147：信息技术-安全技术-漏洞披露和 ISO/IEC 3011：信息技术-安全技术-漏洞处理流程，可帮助企业有效应对内外部的漏洞风险。ISO/IEC 29147 为企业提供了有关披露产品和服务漏洞的要求和建议，用于解决与披露产品和服务中的潜在漏洞相关的问题。ISO/IEC 3011 提供了有关如何处理和修复产品或服务中报告的潜在漏洞的要求和建议，用于指导企业如何调查、

分类和解决产品和服务中潜在的漏洞。实施 ISO/IEC 29147 与 ISO/IEC 30111 可帮助企业减少漏洞的影响和暴露，在漏洞被利用之前得到识别和处理，从而提高产品的安全性，同时还可以帮助组织改善内部沟通、协作以及漏洞处理的协调。

制造商的披露声明：FDA 对于医疗器械网络安全透明度中网络安全风险的标签建议，推荐使用 MDS2 《Manufacturer Disclosure Statement for Medical Device Security-MDS2》（HN 1-2013）。MDS2 是由美国国家电气制造商协会（NEMA）和医疗保健信息和管理系统协会（NEMA）发布的一份关于医疗器械网络安全能力披露文件，供制造商进行参考，协助负责安全风险评估过程的专业人员管理医疗器械的安全问题。作为对产品安全和客户服务承诺的一部分，企业可使用 MDS2 向客户提供有关其产品的安全信息，帮助客户评估、解决与维护传输 ePHI（受保护的电子健康信息）的产品相关的漏洞和风险。

HIPAA 对患者健康信息的要求：《健康保险流通与责任法案》（HIPAA）是美国卫生与公众服务部在 1996 年颁布的一部联邦法律，其规定了如何处理和保护健康信息。HIPAA 要求对电子健康信息采取安全控制措施并规定了隐私保护措施，以确保个人健康信息得到适当保护，同时促进高质量医疗健康信息的流通。FDA 在网络安全控制类型阐释时提到，制造商应确保支持可能导致患者伤害的任何数据的机密性（例如，通过未经授权而使用其他有效凭据，缺乏加密等）。凭据保密性的丧失可能被攻击者用来对患者造成伤害。缺乏加密来保

护静态和传输中的敏感信息和/或数据，可能会使这些信息被滥用，从而导致患者受到伤害。

HIPAA 在 2013 年的修正案最终法案中，将遗传信息纳入 HIPAA 对健康信息的定义中，并禁止健康保险发行人以推销保险为目的使用和揭露基因信息。基因信息与其他健康信息一样，受 HIPAA 隐私条款的保护，HIPAA 隐私法令严格限制未经个人授权的基因信息的使用和公布。

尽管保护 PHI (Patient Health Information, 患者健康信息) 的机密性超出了 FDA 的监管范围，但制造商和其他实体，根据产品实际情况，可能有义务根据适用的美国联邦和州法律，包括 HIPAA，在整个产品生命周期中保护 PHI 的机密性、完整性和可用性。

美国正在逐步加强对基因数据的传输限制：为了保护个人隐私、国家安全和经济利益，近年来美国对其国内数据安全和生物信息安全的关注度逐渐提高，对数据传输出境的政策开始实施严格的限制，对国际间的数据流动逐渐产生深刻的影响。

2024 年 9 月 9 日，美国众议院通过的《生物安全法》(Biosecure Act) 草案，计划禁止美国行政机构与受关注的生物科技公司进行特定交易，旨在防止美国人的基因数据流入受关注国家 (Countries Of Concern)，而中国便是其中受关注的国家之一。

(二) 欧盟对基因测序仪数据安全进行严格监管

近年来，网络与数据安全成为欧盟重点关注的内容。由于网络攻击越来越隐蔽、越来越频繁，医疗器械亦不例外。网络攻击使患者及

整个医疗服务系统都面临着安全考验。为此，欧盟发布的医疗器械及体外诊断器械法规，对网络安全规则进行了严格规定，将网络安全贯穿于产品整个生命周期过程，以确保医疗器械设计、制造、使用、维护等全过程的安全性。同时欧盟亦意识到，个人数据的网络泄露使公民面临着巨大的风险，为此出台了严格的数据保护立法，为解决数据在收集、存储、传输、使用等过程中出现的安全问题提供了强有力的依据。

2017 年 5 月 5 日，欧盟发布了新的《医疗器械法规》（**Medical Devices Regulation, MDR**）（EU）2017/745 和《体外诊断医疗器械法规》（**In Vitro Diagnostic Medical Devices Regulation, IVDR**）（EU）2017/746，替代之前的《医疗器械指令》（**Medical Devices Directive, MDD**）和体外诊断器械指令（**In Vitro Diagnostic Medical Devices Directive, IVDD**）。新的法规在立法层次、监管力度、临床性能、可追溯性、信息透明度和上市后监督等方面进行了重大调整和完善。

为了加强对投放到欧盟市场的医疗器械应对网络安全风险相关新技术挑战的关注，以帮助医疗器械制造商满足 MDR 和 IVDR 中的网络安全要求，医疗器械协调小组（MDCG）于 2019 年 12 月发布了指南文件《**MDCG 2019-16 Rev.1 Guidance on Cybersecurity for medical devices**》。该指南详细描述了医疗器械网络安全的问题，关注的产品包括所有包含电子可编程系统的医疗器械以及本身即是医疗器械的软件，强调了网络安全的重要性。与 FDA 指南类似，其指出

生产企业在设计时就应考虑网络安全的问题，并贯穿于产品整个生命周期之内。该指南详细阐述了上市前和上市后的要求，以帮助医疗器械生产企业在产品收益和风险之间取得适当的平衡。同时，该指南指出，进行网络安全测试是产品安全验证和确认的主要方法，可能的方法包括安全功能测试、模糊测试、漏洞扫描和渗透测试等。

MDCG 指南重点旨在帮助企业满足 MDR 和 IVDR 附件一中列出的关于具有网络安全风险的设备的通用安全和性能要求(General safety and performance requirements, GSPR)。MDR 和 IVDR 中的 GSPR 要求医疗器械生产企业在产品整个生命周期中实施当前技术水平 (state of the art) 实践，同时必须考虑风险管理的原则，包括信息安全和 IT 安全。这种当前技术水平包括适用的标准、指南、现有专有知识以及可公开获取的科学/技术信息。对于网络安全的关键要求记录于 MDR 附件一第 17.2、17.4 节和 IVDR 附件一第 16.2、16.4 节中，同时对说明书的内容也提出了要求。

MDCG 指南指出，在欧盟层面 NIS 指令 (EU 2016/1148) 和《通用数据保护条例》 (EU 2016/679 GDPR) 与医疗器械的网络安全或与处理医疗器械中存储的个人数据的保护或处理的运营商相关，并可能与 MDR/IVDR 法规同时适用。

NIS (Network and Information Systems, 网络和信息系统) 是欧盟成员国范围内重要的网络安全立法，初版为 2016/1148 号指令。NIS2 指令 (2022/2555 号) 于 2023 年 1 月 16 日生效，取代 NIS1。NIS2 扩大了 NIS 中所涵盖的实体和管理要求，从之前的 7 个实体扩

展到了 15 个，增加了医疗保健机构以及从事医疗器械制造的实体。NIS2 创建的网络安全框架，规定了管理层的个人责任，实施了更高的网络恢复力，加强了对供应链安全的要求。将 NIS2 应用于医疗领域，体现了欧盟在平衡技术创新与安全方面的考虑，是数字医疗健康发展的基础。

欧盟于 2016 年通过了《通用数据保护条例》（General Data Protection Regulation, GDPR 679/2016），于 2018 年 5 月 25 日生效执行。该条例是欧盟为解决互联网时代用户数据的收集、使用问题而制定，并适应云计算、互联网、大数据。目前 GDPR 是全球在保护个人数据方面规定最为严格、处罚最为严厉的法规之一。

在医疗健康领域，GDPR 的实施彻底改变了患者数据的管理方式。GDPR 使患者有更多权利控制其个人数据的收集及使用。首先新法规突出了患者对其个人数据的知情权和拥有权。医疗机构需要得到患者的同意才可以收集、存储和加工数据，对于数据的收集应符合预期的规定，对数据的处理也应遵守此预期目的。GDPR 使患者对个人的数据有全面的了解，并将其掌握在自己手中。

由于对基因数据潜在滥用问题的关注日益增多，GDPR 增加了对基因数据的适用性，对基因数据的使用建立了严格的要求。GDPR 中指出，与健康有关的个人数据包括从遗传数据和生物样本中获得的信息，而“遗传数据”是指与自然人遗传或获得的遗传特征有关的个人数据。为唯一识别自然人而处理遗传数据、生物特征数据，在 GDPR 中被定义为特殊类别的个人数据，需要提供更高的保护和更严格

的要求。

GDPR 也对数据跨境传输做出了严格要求，欧盟境内医疗器械制造商或相关医疗机构在将数据传输到非欧盟国家时应确保数据接收方提供的保护水平与欧盟标准一致。

（三）IMDRF 不断发布医疗器械网络安全新指南

IMDRF（International Medical Device Regulators Forum，国际医疗器械监管机构论坛）是一个以世界各国医疗器械监管机构为主导的自愿性的法规协调组织。我国在 2013 年 3 月以正式成员代表身份加入 IMDRF，成为其中的一员。IMDRF 高度重视医疗器械的网络和数据安全，近年来陆续发布了多个与医疗器械网络安全相关的标准。

医疗器械安全原则与实践：IMDRF 于 2020 年 4 月发布了《Principles and Practices for Medical Device Cybersecurity》（医疗器械网络安全原则与实践）官方指南。该指南就医疗设备网络安全的一般原则和最佳实践向所有利益相关者提供具体建议，强调医疗器械全生命周期的安全风险管理，划分了各个参与方的安全责任，包括医疗器械制造商、医疗保健提供商、监管机构和用户等，以最大限度地减少设备的网络安全风险。美国 FDA 上市前网络安全指南及欧盟 MDCG 网络安全指南均参考或与 IMDRF 的网络安全指南相一致。

医疗器械安全软件物料清单原则与实践：软件物料清单 SBOM（Software Bill of Materials），是一份详细记录软件构建过程中使用的所有组件、库和依赖项的清单。SBOM 的关键信息包括组件名称、供应商、版本号、许可证信息等。通过提供所有细节的正式列表，使

其他人能够了解其软件中的内容并据此采取行动，从而降低生产者和用户的风险。2023 年 IMDRF 发布指南文件《Principles and Practices for Software Bill of Materials for Medical Device Cybersecurity》，该指南强调了设备制造商和医疗提供者的作用和责任，并就实施 SBOM 和提高医疗器械软件使用的透明度提出了建议。

遗留医疗器械的安全原则与实践：遗留医疗器械，是指不能合理防护现有网络安全威胁的医疗器械，并非指上市时间较早的医疗器械，因而与其目前使用的年份无关。2022 年 IMDRF 发布了指南文件《Principles and Practices for the Cybersecurity of Legacy Medical Devices》（遗留医疗器械的网络安全原则和实践），该指南旨在就如何将产品全生命周期过程应用于遗留设备提供具体建议，提供了如何鉴别潜在的遗留设备，以及解决网络安全问题不同的方法。该指南是对《医疗器械网络安全原则与实践》的补充。

（四） IEC 积极制定医疗器械数据安全标准

IEC（International Electrotechnical Commission，国际电工技术委员会）也积极对医疗器械的网络安全风险管理进行研究，以应对与医疗器械软件相关网络安全问题日益增长的挑战，建立和发布了一系列具体可执行的网络安全标准。

医疗 IT 网络的发展，使医疗机构的内部网络不断得到加强和完善，对此 IEC 发布了 IEC/TR 80001 系列标准文件：包含医疗器械的 IT 网络的风险管理应用，提出了针对医疗 IT 网络进行风险管理的方法论。如 IEC 80001-1: 2021 描述了联网医疗器械或健康软件在其实

施和使用中的安全性、有效性和网络安全。IEC/TR 80001-2-2 为医疗器械安全需求、风险 and 控制的披露和沟通指南，规范了医疗 IT 网络安全的 19 项能力。IEC 81001-5-1 考虑到健康软件的特殊需求，描述了健康软件产品生命周期中安全性的活动，是对 IEC 62304 中网络安全相关内容的补充。IEC/TR 60601-4-5: 2021 为医疗 IT 网络中使用的医疗设备的安全特性提供了技术规范，涉及的医疗器械包括医疗电气设备、医疗电气系统和医疗器械软件，但是不适用于体外诊断设备（IVD）。

IEC 82304-1:2016 规定了健康软件产品安全的通用要求，适用于健康软件产品的安全和网络安全，主要关注对制造商的要求。目前该标准已被国内转化为 GB/T 42984.1-2023《健康软件 第 1 部分：产品安全的通用要求》。

（五）我国基因测序仪的数据安全管理在不断加强

当前，网络技术、数字化技术深刻影响着医疗领域，显著提升了我国医疗技术水平，满足了公众对于健康生活更高的要求。而医疗数据作为一种特殊而敏感的资源，其安全性一直是全社会关注的焦点。

1. 顶层设计构建数据安全基本要求

“没有网络安全就没有国家安全”，党的十八大以来，习近平总书记多次在不同场合就网络安全发表一系列重要论述。2016 年 11 月 7 日，十二届全国人大常委会第二十四次会议表决通过《中华人民共和国网络安全法》，成为我国第一部关于网络安全的基础性法律。医疗器械网络安全是医疗器械安全性和有效性的重要组成部分，也是国

家网络安全的组成部分之一。基因测序仪的网络安全性不仅在于使网络处于稳定可靠的状态，保证产品的安全有效运行，更是基因测序数据安全性的重要保障。

医疗器械产品的海量数据，成为数字化时代的重要资源，此类数据资源具有重要的医疗价值，并且关系到千千万万患者的隐私和健康安全，对这类数据的安全保障尤为重要。随着基因测序技术的发展，基因测序的需求以及产生的数据也在不断增加，同时数据的共享进一步推动了生物学科学的研究和医学的进步，在此过程中数据安全和隐私保护成为行业发展的重要挑战。基因测序数据涉及个人隐私和国家安全，一旦泄露或被非法利用，将带来严重的后果。因此，基因测序数据安全和隐私保护成为基因测序行业发展的必要条件。

2021 年 6 月，我国通过的首部针对数据安全的专项法案——《中华人民共和国数据安全法》，对行业数据安全、个人数据隐私保护等各个方面提出了明确的要求和规定，成为了我国数据安全治理体系的重要基石。2021 年 8 月 20 日，我国通过了首部针对个人信息安全的专项法案——《中华人民共和国个人信息保护法》，使得医疗数据处理活动得到了规范，医疗数据得到合理的利用，保障了患者个人权益。《个人信息保护法》赋予了患者更多元化的个人信息权益，包括知情权，决定权，查阅、复制权，更正、补充权，可携带权，删除权，解释说明权等。

2.国家药品监督管理局持续强化医疗器械网络、数据安全

2014 年 2 月，当时国家食品药品监督管理总局（CFDA）与国家卫计委联合发布《关于加强临床使用基因测序相关产品和技术管理的通知》，对于基因测序诊断产品，包括基因测序仪及相关诊断试剂和软件，进行监督管理，在产品研发、生产、注册、临床试验、临床使用等环节提出了要求，由此基因测序行业逐渐有了明确的规范约束。

2014 年，当时国家食品药品监督管理总局医疗器械技术审评中心启动制定首版《医疗器械网络安全注册审查指导原则》，依据中华人民共和国网络安全法，结合我国国情，以及医疗器械行业的发展状况，于 2017 年 1 月 20 日首次发布，用于指导我国医疗器械网络安全的注册工作。

2022 年 3 月，国家药监局器审中心发布修订版的《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增加了更多的技术考量和相关的概念解释，重点对网络安全能力、漏洞评估、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、软件维护与升级等进行了修订。新版指导原则对网络安全的描述更加详实，要求更加全面和具体，进一步提升了对医疗器械网络安全的管理。基因测序仪因其数据的特殊性，网络安全级别属于严重级别，受到了国家药监局的严格关注。

3.人类遗传资源管理不断加强

我国是多民族的人口大国，人类遗传资源丰富且独特。为加强对我国人类遗传资源保护，守护民族基因安全，国家先后出台了一系列的规定，以有效保护和合理利用我国人类遗传资源。

1998 年，国务院办公厅颁布了《人类遗传资源管理暂行办法》，首次对我国人类遗传资源的研究、利用、管理等过程进行了规范。2011 年、2013 年科技部又先后发布了《关于加强人类遗传资源保护管理工作的通知》、《关于进一步加强人类遗传资源管理工作的通知》，强调开展人类遗传资源研究的单位应对所涉及人类遗传资源的安全负责，并杜绝人类遗传资源违法违规出境。2015 年，科技部先后发布了《人类遗传资源采集、买卖、出口、出境审批行政许可事项服务指南》、《关于实施人类遗传资源采集、收集、买卖、出口、出境行政许可的通知》，进一步明确了“分级管理、统一审批”的监管体制。

随着人类遗传资源研究和利用的不断深入，人类遗传资源非法外流的事件仍旧时有发生，逐渐凸显出我国人类遗传资源的利用不够规范、制度不够完善。2016 年科技部在总结暂行办法施行经验的基础上开始制定《人类遗传资源管理条例》，并于 2019 年 5 月由国务院通过并正式公布。条例中明确规定在我国境内采集、保藏和对外提供我国人类遗传资源必须由我国科研机构、高等学校、医疗机构和企业开展。境外组织、个人及其设立或者实际控制的机构不得在我国境内采集、保藏我国人类遗传资源，不得向境外提供我国人类遗传资源。将我国人类遗传资源信息向外国组织、个人及其设立或者实际控制的机构提供或者开放使用的，应当向国务院科学技术行政部门备案并提交信息备份。

2020 年 10 月，全国人大常委会通过的《生物安全法》，也对人类遗传资源与生物资源安全做出了规定，境外组织、个人及其设立或

者实际控制的机构在我国境内采集、保藏我国人类遗传资源，或者向境外提供我国人类遗传资源的，由国务院科学技术主管部门责令停止违法行为，没收违法所得和违法采集、保藏的人类遗传资源，并处相应的罚款。

4. 医疗数据出境得到严格控制

新版指导原则指出，医疗数据属于重要数据资源，特别是敏感医疗数据含有个人信息，因此医疗数据出境应符合重要数据、个人信息、人类遗传资源信息出境安全评估相关规定。基因测序仪作为基因数据的产出主体，直接带动了下游的存储、计算、分析、诊断、研究等活动，不仅包含有个人信息，同时包含人类遗传资源信息，不仅关乎个人信息安全，同时涉及国家安全，因此，我国对基因测序相关数据的出境做出了严格的控制。

《网络安全法》、《数据安全法》和《个人信息保护法》都明确规定关键信息基础设施运营者收集的个人信息、数据应存储在境内，确需向境外提供的，须经过网信部门主导的安全评估。

2020 年国家互联网信息办公室发布的《数据出境安全评估办法》指出，数据处理者向境外提供重要数据，应当通过所在地省级网信部门向国家网信部门申报数据出境安全评估。生物医药、健康医疗等相关领域的数据处理者或信息提供者，凡涉及人类遗传资源信息、基因信息等跨境流动，应注意审查其出境活动是否触发评估办法规定的数据安全评估和申报。2024 年 8 月国务院通过的《网络数据安全条例》指出，数据处理者因业务等需要，需向中华人民共和国境外提

供数据的，应当具备相应的条件。数据处理者向境外提供个人信息的，应当向个人告知境外数据接收方的相关信息，并取得个人的单独同意。数据处理者向境外提供在境内收集和产生的数据，一定情形下应当通过国家网信部门组织的数据出境安全评估。

三、安全风险挑战

当前基因测序仪大多具有联网功能，基因测序仪也可能包含容易受到网络安全威胁的软件，同时基因测序仪需要与外部数据服务器进行通信，以实现测序数据的传输，外部的数据服务器可能部署在本地，或者部署在云服务器上，基因测序仪亦可能通过本地运行管理系统进行数据交互或者由远程进行访问。

基于测序仪的设计和运行方式，如果产品本身或数据传输过程中存在网络安全漏洞，可能会导致数据泄露，缺失，或生成不准确甚至被篡改的基因测序数据，从而给基因测序数据带来严重的安全风险和挑战。当前，基因测序面临的主要安全风险如下：

（一）身份验证和访问控制不足造成的风险挑战

确保只有授权人员能够访问基因测序数据至关重要。访问控制和身份验证是医疗器械重要的网络安全能力，确保只有授权用户才能访问基因测序仪中敏感的资源，以保持数据的机密性、完整性、可用性。

访问控制是通过限制对系统、网络和数据资源的访问权限，以防止未经授权的修改或破坏活动，以确保系统的安全性。身份验证是确认某个角色是否具备执行某项操作或查看某些资源的权限，从而降低恶意攻击的风险。通过合理设计和实施的访问控制机制和准确有效的

身份验证方法，是保障信息安全的重要途径，相当于是测序仪的“门卫”，守护者的测序仪安全的第一道防线。

从现实中已经披露的基因测序仪网络安全事件中可以看出，不健全的访问控制和身份验证安全机制，会给测序仪的网络安全性带来致命的危害。薄弱的身份验证机制，如简单的用户名和密码组合，容易被攻击者破解，从而获取未经授权的访问权限。同样的，如果测序仪未配置访问控制功能，攻击者就可以通过各种技术手段访问其他账号下的数据和功能，或者纵向提升到一个更高的用户级别（如系统管理员），攻击者就会具有更高的权限，进而对测序仪在操作系统层面进行不当访问；或者修改测序仪或客户网络上的设置、配置、软件或数据，影响仪器中的基因测序结果，包括导致仪器提供不正确的结果、改变的结果或数据泄露等。

（二） 第三方供应链安全风险挑战

近年来，软件供应链攻击的发生频率呈明显增长趋势，攻击者利用软件供应链的复杂性和互联性，通过恶意软件植入、代码篡改、供应链流程破坏等方式，可以实现对基因测序仪的深度渗透和控制。一旦某个环节产生漏洞，恶意代码就可能如病毒般快速传播，影响所有基因测序仪的下游用户。这种攻击方式具有极大的隐蔽性和破坏性。在开发和测试环节缺乏统一安全发布、未检测工具集，在终端应用环节使用含有漏洞的软件、未受信赖的安装源、未经认证升级包，都有可能导致对数据隐私造成威胁。

（三）数据传输过程的安全风险挑战

基因测序数据因其处理流程复杂，在数据从基因测序仪传输到数据服务器的过程中，可能面临网络攻击、数据拦截和篡改的风险。例如，黑客可能利用网络漏洞入侵传输通道，窃取敏感的基因测序数据。不安全的传输协议或未加密的数据传输可能导致数据泄露，给患者和使用机构带来严重的后果。

基因测序仪数据的传输大体可分为三种情况，一种是测序仪和外部数据服务器之间的数据传输，这类数据主要是原始测序数据以及一些通信校验数据等。另一种数据传输是，如果测序仪配置了像本地运行管理软件之类的远程监控和管理模块，用于对设备运行状态进行远程监控和管理，创建测序运行、监控运行状态、分析测序数据和查看结果，则此类数据属于传输控制命令、仪器工作状态、测序数据结果等。第三种数据传输是测序仪通过消息队列等方式与 LIMS 系统等传递和接收运行数据和指令。这三种数据传输对测序仪来说非常重要。

从现实中已经披露的基因测序仪网络安全事件中可以看出，远程监控和管理模块与测序仪进行数据传输时，如果缺乏机密性的安全措施造成网络安全漏洞，攻击者就可以利用该漏洞，对传输中的敏感数据（包括访问凭证）进行中间人攻击，导致未经授权的用户远程控制测序仪。同时如果测序仪与外部数据服务器未配置节点鉴别、或数据传输过程中未采取机密措施，极有可能造成中间人攻击和数据泄露。测序仪如果具备与外部实验室 LIMS 系统进行消息同步，则此类消息传输机制如果未进行身份验证或通讯加密，同样有可能造成未授权的

访问。

（四）数据存储、计算过程的安全风险挑战

基因测序数据在存储或计算中也可能存在被泄露的风险。由于某些原因，基因测序数据会被存储在公共云服务器上并执行计算任务，此时数据的存储和处理都依赖于云服务器。由于云服务器属于公共网络且多是由第三方来管理，恶意攻击者便可能会利用网络安全漏洞攻击服务器或相应的服务。

云服务器上存储的基因数据同样重要，不仅关乎个人隐私的保护，还关系到组织的声誉甚至国家利益。如果云服务器上的数据使用了不安全的加密算法进行存储，或者对于数据的访问未做管理控制，亦或未对登录用户的身份做严格的认证等，均可能被黑客利用出现数据泄露或被篡改的情况，进而导致严重的后果。

鉴于云服务具有开放性和复杂性的特点，由此带来了网络和数据在使用和存储上的安全挑战。

（五）数据意外丢失或损坏造成的安全挑战

基因测序是一个典型的海量数据驱动的行业。基因测序仪产生的测序数据，直接传输给外部数据服务器或者云服务器上，以供下游进行分析。一个测序实验室每天大约会产生 10TB 到 100TB 的下机数据，有的甚至可以达到 PB 级别。

在基因测序成本逐渐降低，测序需求量快速增加的情况下，基因测序行业对数据存储系统及数据保存方式提出了更高的要求。基因测序过程中产生的海量数据，对业务的分析极其重要，并需要长时间保

留。如果由于人为因素、系统故障或者遭受网络攻击而造成测序数据的意外丢失或损坏，则会给测序数据的安全存储造成重大挑战。

（六）基因组数据共享的隐私安全挑战

基因组数据保存着生物体生命特征的重要信息。作为一种数据资源，基因组数据不仅具预测疾病风险、个人特征识别性等其他数据资源所没有的特性，且一旦泄露，将会对数据主体造成无法预计的伤害。

在基因检测过程中涉及大量基因组数据，这些基因组数据往往被储存在公开的基因组数据库中，以备研究使用。这些数据尽管经过了匿名化处理，但数据的隐私安全仍然很难得到保护。

有研究发现，在基因组数据共享过程中，个体可以被识别出来，从而揭示出个体当前与某些疾病的关联，进而导致个人隐私泄露。虽然这种识别需要大量统计数据，但是基因组数据的共享利用却引发了相关的数据隐私安全问题。因此，如何使基因组数据在实现数据的共享的同时确保其隐私安全，便成了新的挑战。

四、安全技术与管理措施

鉴于基因测序存在的重大安全挑战，以及基因数据对于个人隐私和国家安全的重要影响，因此，在产品的设计之初，对产品采取一系列的安全风险控制措施，以应对网络和数据安全攻击。

同时应该清晰地认识到，数据安全是一个持续性的过程，漏洞对产品以及患者构成的风险，需要在整个产品生命周期内进行维护。积极、持续性地应对数据安全风险，可有效降低产品整体的安全风险。下列各项为基因测序仪网络数据安全防护重要的技术与措施。

（一） 身份识别与权限控制

身份识别是安全体系的第一道大门，是网络安全的基石，是基因测序仪确认操作者身份的过程。权限控制是测序仪将使用权限分配给不同的角色，而不是直接分配给用户，这样不同的角色获得不同的权限，以提升产品安全性。如果在身份识别和权限控制方面出现漏洞，将给基因测序仪造成灾难性的后果。

身份识别和权限控制通常结合使用，在基因测序仪中，通过定义不同的角色，并为每个角色分配合理的权限，确保只有经过适当授权的人员才能操作仪器并访问敏感数据。

此外，在识别和控制措施方面，基因测序仪应该采取高级别的强度。例如对登录口令设置复杂度要求，选择大写字母、小写字母、数字、符号等混合使用，设置为强口令。对登录口令设置变更周期，提示或要求定期进行更换。对用户登录可启用登录失败处理功能，例如：当连续输入密码错误若干次后，暂停一段时间该用户的登录。

（二） 系统安全加固

安全加固是通过采取一系列措施，提高系统安全性，降低产品被攻击的风险。对基因测序仪进行系统加固，可以构筑坚固的防线，抵御各种安全威胁。常见的加固措施有（不限于）：

a) 安装防火墙，以抵御来自网络的攻击，确保防火墙处于启用状态，并根据需求配置好防火墙规则。

b) 关闭不必要的通信端口、服务、功能、共享文件等，以减少攻击面，降低被攻击的风险。

- c) 安装并启用防病毒软件，并定期更新和升级病毒库。
- d) 对于 Linux 系统，尽量不使用 root 账户登录系统，可以使用 `sudo` 等命令授予普通用户必要的管理权限。
- e) 对于不使用无线连接的仪器，禁止无线网络的连接功能。
- f) 若测序仪预期仅在局域网内使用，应提示禁止将其连接至互联网，以防被网络黑客识别，进而遭受恶意的网络攻击。
- g) 如果测序仪配置有远程监控和管理模块，或者其他的 Web 服务，则应在 SQL 注入、XSS 跨站脚本攻击、文件上传等方面加强防御。

(三) 安全日志审计

安全日志审计在网络安全中起着至关重要的作用，它通过对产品产生的日志进行分类、分析，进而对网络安全事件进行溯源，以发现异常行为，评估安全状况，进而采取进一步的措施。

基因测序仪不正确或者非授权的使用，系统或应用程序非预期的运行，均会导致测序仪存在网络安全方面的风险。基因测序仪可通过创建安全审计功能来跟踪系统、应用程序的工作及健康数据的访问、修改或删除等，从而记录和检查测序仪的活动。

审计内容的创建应特别关注系统的启动、关闭、运行的异常和故障，系统及应用程序用户的登录、访问、操作，用户的创建、修改、删除，个人数据和/或健康数据的访问和处理（包括存取、存储、转移）等。

实际中可使用适当的工具进行审计的创建和维护，采取相应的安

全措施以保证日志的安全性，如考虑存储在安全的位置、定期备份、访问控制等，同时确保无法编辑或删除审计数据。

（四）漏洞管理和网络安全补丁升级

漏洞的管理是一个长期的过程，在基因测序仪生命周期的整个过程中应定期识别其运行的环境，评估当前的安全情况，使用自动化工具或邀请第三方机构对产品进行漏洞扫描、渗透测试等，识别产品存在的漏洞，评估漏洞的影响和修复方式，及时进行漏洞的处理及网络安全补丁的更新和升级。同时定期关注产品所使用的操作系统、数据库、第三方应用软件的官方信息，识别相关风险，适时安装官方发布的安全补丁。

（五）密码学的应用

将密码学应用到测序数据的存储、传输、计算等过程，可有效避免隐私信息的泄露。虽然高质量、标准化的加密算法和协议很容易获得，但一些包含加密保护的产品已被证明由于不正确的加密配置或实现而具有可利用的漏洞。密码学不仅被应用在本地的部署中，部分基因测序仪将数据存储和计算的服务移植在云服务器上，因此，密码学在广域网条件下确保数据的传输与存储安全也发挥着重要作用。

数据传输的安全性是测序仪网络安全性的重要组成部分，此时密码学便扮演着重要的角色。SSL/TLS 是常用的数据传输安全协议，其通过加密传输的数据、验证传输双方的身份，以确保数据传输的机密性和完整性，防止攻击者窃取或篡改传输的数据。数字证书则是对通信双方公钥身份的认证，确保对方身份的真实性。使用 SSL/TSL 协

议和数字证书提高了数据传输的安全性，但仍可能存在中间人攻击、重放攻击、抄袭攻击等情况，此时便需要进一步使用安全的加密算法、加强 SSL/TSL 协议的安全配置等工作。

为了确保基因测序数据不被未经授权的访问而泄露，密码学在数据存储方面也发挥着重要作用。产品设计时，综合考虑算法的安全性、效率等，结合应用场景，应选择恰当的加密算法。部分基因测序仪选择将数据存储到云服务器上，此时应优先选择端到端的加密方式，确保数据在整个传输及存储过程的安全性，排除第三方的影响，保障用户数据的机密性和完整性。鉴于基因测序数据的重要性，测序数据多具有备份和恢复的机制，而对备份数据的加密，可进一步提高数据的安全性。

密码学是网络安全的基石，其重要性不言而喻。当前密码学的发展方兴未艾，随着网络技术的发展，测序仪与网络技术的融合将进一步加深，密码学在网络安全中的地位将进一步凸显。

（六） 软件供应链管理

鉴于在产品研发时可大量缩减技术、时间等方面的成本，软件的设计广泛采用了开源组件，基因测序仪亦不例外。在此过程中不等地就会引入安全方面的漏洞。对于软件的安全性，构建面向供应链的安全评估能力，则显得格外重要。

软件成分分析技术是解决软件供应链安全的关键技术，可以使企业在研发过程对软件组成有更深入的了解，增加软件的透明度，同时还可以应对供应链攻击事件。

当前，软件成分分析技术主要包括软件成分分析（SCA）和软件物料清单（SBOM）。使用 SCA 技术可以识别软件中开源组件信息、开源组件中存在的漏洞以及组件的许可证信息等。SBOM 是软件成分清单的一种实现标准，其中包含有软件中使用的所有组件、库和依赖项及其版本、许可证和来源的信息等，描述了软件构建过程中使用的所有组件及其关系。

SCA 技术专注于与开源组件相关的风险，SBOM 更偏于展示软件组成的图景，SCA 分析有助于 SBOM 的生成。通过 SBOM 与 SCA 技术相结合，可以有效地分析和确定软件组件的安全性和可靠性，进而采取措施降低安全风险。

（七）实施数据保护与备份

为防止由于各种意外以及受到网络攻击而造成基因测序数据的丢失或损坏，建立可靠的数据保护和数据备份策略非常必要且重要。实施数据保护与备份工作，不仅可以防患于未然，即使在发生数据丢失或损坏时，可以快速恢复和还原数据，减少对业务的影响，同时也是满足行业相关法律法规的需要，例如我国的数据安全法以及国外的 GDPR、HIPAA 等对于数据恢复和备份的要求。

数据保护主要是通过数据冗余以实现，数据备份则是通过创建数据副本来实现。RAID（独立磁盘冗余阵列）是一种实现数据恢复的关键技术，通过将两个或多个硬盘驱动器（HDD）或固态硬盘（SSD）合并成一个协调的存储单元或阵列，创建数据丢失的故障安全机制，可以在磁盘故障时立即恢复数据。数据备份技术则可以选择本地

备份、远程备份、云备份、镜像备份等方式，鉴于基因测序数据的特殊性，在进行云备份时，应采用专线的方式直接连接基因测序数据输出端与云服务器端。

基因测序实验室或相关机构可以根据测序仪的通量、每天下机的数据量、测序仪的配置以及业务的实际类型、风险管理方针等选择不同的数据保护或备份的策略。

五、案例研究与分析

随着相关政策的不断完善和人们对于全方位全周期健康服务的不断追求，基因测序需求正日益增长，基因测序市场规模呈现快速增长的态势，基因测序数据网络安全重要性日益凸显。本章内容从公开披露的资料入手，分析当前基因测序产业发展所面临的数据安全难题与相关应对政策，为后续基因测序数据安全发展提供建议。

测序仪安全技术有待加强。2022 年，美国食品和药物监督管理局（FDA）及美国国土安全部下属的网络安全和基础设施安全局（CISA）发布的消息显示，某公司的多款测序仪被曝出存在五个网络安全漏洞，其中三个被评定为最高严重等级，具体包括非必要权限执行、路径遍历、危险类型文件的不加限制上传、访问控制不恰当以及敏感数据的明文传输等。这些漏洞可能导致未经授权的用户远程控制仪器，更改仪器或客户网络上的设置、配置、软件或数据，或影响用于临床诊断的仪器中的患者测试结果，包括导致仪器不提供结果或提供不正确的结果、改变的结果，或数据泄露。后续，该公司紧急召回了存在漏洞的涉及 55 个国家和地区的 2200 多台测序仪，并提供了

短期软件补丁以防止漏洞被利用。同时，该公司也在积极开发永久性的软件修复方案。

外部攻击威胁测序数据安全。2023 年，某基因测序巨头公司遭遇黑客攻击。该公司最初声称只有约 0.1%（约 1.4 万名）的客户数据被黑客访问。后经证实，由于该公司的 DNA 查询功能允许用户自动与他人共享部分数据，黑客利用该功能获取了约 550 万人的个人信息。被窃取的信息主要包括个人姓名、出生年份、关系标签、与亲属共享的 DNA 比例、祖先报告和自我报告的位置等。此外，还有约 140 万人选择加入 DNA Relatives 功能的用户的“家庭树档案信息也被访问”，包括显示姓名、关系标签、出生年份、自我报告的地点以及用户是否决定共享其信息等。因此，该公司的数据泄露事件约影响了其 1400 万总数客户中的一半，不仅使得客户隐私遭到严重侵犯，也导致该公司声誉严重受损。后续，该公司在第三方鉴证专家的协助下完成调查，并开始通知所有受影响的用户，同时要求所有用户重置密码，并要求采用双因素身份认证。

上述案例中，基因数据安全问题背后的根源均指向了数据防护的薄弱性。案例中测序仪上存在的非必要权限执行、访问控制不恰当漏洞，可以使用户执行超越其本身权限的行为，造成未经授权的访问和数据泄露，甚至整个系统被控制。路径遍历可以使攻击者浏览整个文件目录结构，访问到隐秘的文件，造成敏感目录和文件的泄露。危险类型文件的不加限制上传，可以使攻击者随意上传可执行的恶意文件到仪器上，进而植入后门，获得仪器的控制权。敏感数据的明文传输，

可以使攻击者通过代理攻击的方式轻松获得传输过程中未加密的基因数据。基因测序公司个人数据的泄露，则是由于客户重复使用密码所造成，同时该公司未对用户登录做加强安全措施，使得黑客利用其他平台数据泄露事件中公开的密码对受害者的账户进行暴力破解，从而获得访问权限。

这两起事件，为基因数据的安全性敲响了警钟，不健全的安全防护会使基因数据一直暴露在安全威胁之中，积极、主动、多重的网络和数据安全防护，对于基因测序乃至整个医疗行业具有重要意义。

六、总结与建议

（一）基因测序数据网络安全至关重要

基因测序数据蕴含着遗传特征、健康状况甚至潜在疾病风险等信息，是个体生命信息的核心载体，其安全不仅关系到个人隐私权的保护，更是国家生物安全、行业健康发展的基石。**从个人层面看**，基因测序技术具有强大的生命信息洞察能力，研究表明，只需给定一些背景信息，个体就有可能在特定的基因组数据中被重新识别，从而揭示个体当前与某些疾病的关联。因此，基因测序数据一旦遭受泄露、篡改或非法利用，可能用于精准诈骗，或是让个人遗传隐私曝光，在保险、就业等领域遭受歧视，将对个人生活造成深远影响。**从国家层面看**，基因测序数据一旦被境外势力获取，可能造成民族基因歧视等恶劣行径，严重危及国家安全和民族尊严。同时，基因测序数据的准确性直接关系到疾病的预防、诊断和治疗，以及科研发现的可信度，在医疗科研领域具有不可替代的价值。因此，在数字化时代，必须强化

网络安全防护，运用加密技术、严格访问权限管理等手段，守护基因测序数据安全，为维护人类生命健康和社会稳定发展筑牢坚实防线。

（二）基因测序数据网络安全发展建议

随着技术的进步和人们认知的提升，基因测序在医疗、生物学等领域的应用日益广泛，未来，基因测序数据网络安全发展需从多方进行保障。技术应用方面，鼓励产业各界共同协作，搭建“产学研用医”联合创新体，加强网络安全人才的培养和引进，持续推动数据加密技术的研发与应用，加强网络安全防护体系的建设与完善，关注云计算、大数据等新技术在基因测序数据安全领域的应用，推进技术创新与融合，提升基因测序数据网络安全防护技术的水平。安全措施方面，强化基因测序全流程的安全防护措施，建立健全的访问控制机制，实施多因素身份认证和基于角色的访问控制，加强隐私保护，保护个人隐私信息，确保数据的合规共享，建立安全审计机制，对异常行为进行监测和报警，并及时采取相应的措施，打造安全可靠的基因测序数据环境。产业生态方面，推动基因测序数据共享与隐私保护的平衡发展，在保障数据安全的前提下，推动基因测序数据的共享与应用，促进产学研用的联动，加强产业链上下游的协作与配合，提高企业自律性和对安全的认知，共同提升基因测序数据网络的安全性，促进基因测序技术的健康发展和广泛应用。政策监管方面，持续更新和完善安全监管策略，建立动态风险评估机制，完善相关法律法规的制定与执行，明确基因测序数据网络安全的责任和义务，规范数据的收集、存储、处理和使用行为，不断优化安全措施和流程，加强国际合作与交流，

共同应对基因测序数据网络安全面临的全球性挑战。

附 录

一、基因测序网络安全相关政策

表 1 MDR 附件一中网络安全的要求

章	节	MDR 要求
附件 1 通用安全与性能要求 第 2 章 有关性能、设计和制造的要求 17.可编程电子系统 ——包含可编程电子系统的器械与本身就是器械的软件	17.2	17.2.针对包含软件的器械或自身为器械的软件，应根据现有技术开发和制造软件，同时考虑开发生命周期原则、风险管理，包括信息安全、验证和确认。
	17.4	17.4 制造商应规定有关硬件、IT 网络特性和 IT 安全措施的最高要求，包括防止非授权访问、按预期运行软件的必要条件。
附件 1 通用安全与性能要求 第 3 章 有关设备提供的信息的要求 23.标签和使用说明书	23.4 使用说明书中的信息	(z)向使用者和/或患者发出关于与器械有关的任何严重事件的通知，应报告给使用者和/或患者所在成员国的制造商和主管机构。 (ab)对于结合可编程电子系统的器械，包括软件或器械本身是软件，有关硬件、IT 网络特性和 IT 安全措施的最高要求（包括防止未经授权的访问）对于运行软件来说所必要的。

表 2 IVDR 附件一中网络安全的要求

章	节	IVDR 要求
附件 1 通用安全与性能要求 第 2 章 有关性能、设计和制造的要求	16.2	16.2 对于包含软件的设备或本身就是设备的软件，软件应按照最新技术进行开发和制造，同时考虑到开发生命周期、风险管理(包括信息安全、验证和确认)的原则。
	16.4	16.4 制造商应列出运行软件所需的硬件、IT 网络特性和 IT 安全措施(包括防止未经授权的访问)方面的最低要求。
附件 1 通用安全与性能要求 第 3 章 有关设备提供的信息的要求	20.4. 使用说明 中的信息	20.4.1. 使用说明书应包括下列所有事项: (ah) 对于包含电子可编程系统(包括软件)或本身就是设备的软件的设备，有关硬件、IT 网络特征和 IT 安全措施的最低要求，包括防止未经授权的访问，这些都是运行软件所必需的。