大数据时代，医疗行业信息安全面临的机遇与挑战

中国信息安全测评中心 刘孝男 付嵘 李连磊

英国学者维克·托迈尔–舍恩伯格（Viktor Mayer–Schonberger）在其著作《大数据时代》（Big Data：A Revolution That Will Transform How We Live，Work，and Think）中指出，医疗领域的变革存在于生活、工作与思维三点上，大致表现在以下两方面：一是为人类医疗集体经验的快速提升提供帮助，这种颠覆式创新将让每个人都成为控制自己疾病的主人；二是“取之不尽、用之不竭”的医疗数据创新是显性的，带来极具商业价值的产业效应。然而在如火如荼的医疗大数据发展背景下，医疗数据安全、个人隐私保护甚至国家安全的问题日益凸显。因此，如何在大数据时代，为医疗行业信息安全保驾护航，将成为一个国家乃至每一个医疗行业信息安全保卫战士需要坚守的重要任务。

一、医疗大数据在国内外的发展现状

2013 年，英国建立了英国国民医疗服务系统（National Health Service，NHS）。2013 年 5 月，奥巴马政府宣布了“大数据的研究和发展计划”。2013 年 6 月，日本安倍内阁宣布了“创新最尖端 IT 国家宣言”，包括大数据在新医疗技术开发领域的应用。同年，韩国完成了国民健康数据认证（DQC–V）和国民健康数据管理认证（DQC–M）两个系统的建设工作。此外，德国、法国、欧洲多国也开展了医疗大数据的建设。

2017 年 4 月，医疗行业发生两件大事，先是由中国电子信息产业集团有限公司等 4 家公司发起的中国健康医疗大数据产业发展有限公司成立，紧接着

由神州数码等 13 家公司发起的中国健康医疗大数据股份有限公司成立，两大集团都以国有资本为主体，行业领军企业东软集团、万达信息、易联众、荣科科技成为核心成员单位，这都表明我国健康大数据行业迎来正规军。

二、大数据在医疗行业更具价值体现

大数据在医疗行业可服务于居民，首先，为居民提供精准医疗、个性化健康指导，为居民在医院、社区及线上提供心脑血管、癌症、糖尿病等疾病的干预、管理、预警及宣教等持续性服务；其次，医疗行业物联网的建设，可实现移动医疗、临床监控及远程患者监控等功能，以此减少患者住院时间，减少急诊数量，提高家庭护理比例，合理调控医生预约量。可服务于医生，在用药分析、药品不良反应、疾病及并发症、治疗效果等方面提供数据，为医生制定个性化治疗方案时提供快速而准确的临床决策支持。

可服务于科研，根据临床阶段的数据集对疾病进行诊断和预测，通过使用统计工具和算法提高临床试验设计水平，分析临床试验数据和病人记录确定药品适应症和副作用，通过对大型数据集（例如基因组数据、极端表型人群等）的分析发展个性化治疗。可服务于管理机构，针对流行病、急病等预防干预及处理措施进行评价，医疗支付方通过大数据分析对医疗服务进行定价，通过临床收集数据进行临床路径优化，通过药品使用数据进行规范性用药评价。可服务于公众健康，通过全国的患者电子病历数据库针对危机健康的因素进行检测、监测及响应；通过网络平台和社区服务可产生大量有价值的数据，如病人可以分享治疗经验、医生可以分享医疗见解等。

三、医疗行业大数据信息安全面临的挑战

医疗是一个特殊的领域，其特殊性在于它以“人”为研究对象，所有医疗行为及其结果都以获取个人信息为基础。因此，医疗大数据信息安全应被界定为涉及“人”和“数据”两个维度的安全。

医疗大数据信息安全中“人”的安全，涉及的是数据隐私保护问题。这里所指的隐私包括医生隐私和患者隐私。相对于患者隐私，在现实生活中，医生隐私的保护问题常常被忽略，不能说医生“遵守职业规范”就必须出让自己的隐私（包括但不限于：宗教信仰、政治偏好、犯罪记录和性别倾向等数据），其同样需要保护。患者隐私主要包括：体检、诊断、治疗、疾病控制、医学研究过程中涉及的个人集体特征、健康情况、人际接触、遗传基因、病史病历等。患者隐私不等同于个人医疗信息，患者隐私包含患者私人信息、私人领域和私人行为，个人医疗信息中隐私部分与患者隐私信息存在交集，但两者所涵盖的范围是不同的。明确患者隐私和个人医疗信息的异同，有助于明确医疗信息及其隐私保护对象，进而分辨出哪些医疗数据属于隐私且需要重点保护，哪些医疗数据可以共享和利用。

医疗大数据信息安全中“数据”的安全，涉及两个方面：一是含有的敏感数据会吸引潜在的攻击者；二是对现有的存储或安全防范措施提出挑战，大数据时代复杂多样的数据存放在一起，常规的安全扫描手段无法满足安全需求。

蛋壳研究院通过对 2010 年至 2015 年美国医疗信息泄露事件总结分析发现，个人医疗信息主要从医疗保险商、医疗机构和商业合作公司三大机构中泄露。其中，保险公司成为医疗信息泄露的主要来源。典型案例：2015 年 2 月，美国第二大医疗保险公司 Anthem 宣布黑客盗取了其公司超过 8000 万客户的个人信息，包括了用户家庭住址、生日、社保号和个人收入信息，此次泄露成为美国有史以来最严重的医疗信息泄露事件。2015 年 5 月，美国联邦医疗服务商 Blue Cross Blue Shield（BCBS）旗下的 CareFirst 保险公司宣布因为黑客攻击，1100 万用户信息泄露。2015 年 9 月，美国一家名为 Excellus 保险商被黑客入侵，近千万用户信息遭到泄露。

医疗信息泄露的原因主要有以下五大类：黑客入侵、使用者处置不当、非法登陆、丢失和被窃，其中黑客入侵成为主要的直接泄露原因。医疗信息泄露的渠道主要有以下几种形式：台式电脑、笔记本电脑、服务器、电子医疗档案、电子邮件和传统纸质文档，其中服务器是造成信息大量泄露的主要渠道。

“冰冻三尺非一日之寒”，医疗行业信息安全事件频发的原因还得从医疗自身内部说起。首先，医疗机构使用信息化系统的比例不断提高，机构间共享数据随之普遍，医疗信息数据的迅猛增长直接增加了泄露发生的可能。其次，医疗信息系统软件在设计之初，没有完全考虑到互联互通时可能存在的安全问题，使得医疗机构内部和医疗机构之间软件“碎片化”严重，从而留下了很多安全隐患。再者，绝大多数医疗机构信息系统安全运维部门处于人员短缺的状态，没有足够的信息安全专家，医务人员缺乏信息安全的有效培训，这些都增加了信息安全泄露的风险。

相比上述提到的医疗内部因素，现在来自外部的因素正在成为医疗行业信息泄露的主要驱动力。因

为，黑客们已然发现这是一条稳定的“生财之道”。黑客们利用医疗信息安全漏洞获利的方式主要分为以下两类：

一是利用泄露的信息直接“变现”。黑市上，个人医疗信息的价值比信用卡信息要高出 50 倍。由于个人医疗信息包括了患者的个人基本信息、财务信息和健康信息等多种敏感数据，不法分子可以利用这些信息进行诈骗和勒索。2016 年 7 月，我国 30 个省份至少有 275 位艾滋病感染者的个人信息遭泄露，犯罪分子在诈骗电话中能准确地描述出病患的个人信息，包括真实姓名、身份证号、联系方式、户籍信息、确诊时间、随访的医院或区县疾控等等，并谎称能为患者办理补助而需要收取不菲的手续费。

二是利用安全漏洞间接“变现”。黑客们通过网络安全漏洞控制医院网络系统，进而向医院索要赎金。2017 年 5 月 12 日 20 时，全球爆发大规模比特币勒索感染事件。比特币勒索的核心就是“要钱”，黑客们利用某些技术手段阻止受害者正常访问数据或电子设备，通过逼迫、恐吓或威胁受害人的方式，达到骗取赎金的目的。此次勒索事件中，美国圣地亚哥一所医院由于无法使用电子设备，只能通过纸笔重新为病人服务，导致无法准确判断病人的情况，造成多起病情延误，给病人以及家属带来无可挽回的损失。其实，早在 2016 年 2 月份，美国洛杉矶的好莱坞长老会医院就发生了一起比特币勒索事件，2016 年 2 月 5 日，黑客控制医院网络系统，对系统内的文件进行加密，使得全部电子病历数据无法使用，以解锁密钥作为筹码向医院索取赎金，医院在尝试各种方法都无法恢复系统之后，于 2016 年 2 月 15 日向黑客支付了 40 比特币（约 1.7 万美金）才得以恢复正常运行。

对于患者和医疗机构而言，不法之徒利用网络安全漏洞进行“谋财”仅仅是“噩梦”的开始，潜在的最大危害则是黑客们利用网络安全漏洞直接对医疗设备进行控制进而危害医疗安全和患者的生命。2012 年黑客攻击了美敦力公司，远程控制了该公司生产的好几种型号的胰岛素泵，通过让安全警告失效从而操纵注射剂量。2015 年 5 月 7 日，TrapX 安全实验室的研究人员通过入侵医院 HIS 系统，找到 ICU 病房中的 NOVA CRITICAL CARE EXPRESS 设备，针对 Windows 2000 操作系统实施入侵行为并安装后门，导出数据库信息的同时获取了可以摧毁系统的相关权限。2015 年 9 月，南阿拉巴马大学模拟人体课程的主任教师 Mike Jacobs，通过无线虚拟病人远程侵入心脏起搏器和心脏除颤器，早在德国汉堡第 32 界混沌通信大会上，前挪威计算机应急响应小组的成员 Marie Moe 就曾揭示了现代起搏器设备不安全的一面。

四、医疗行业信息安全的对策与建议

首先，完善网络安全组织机构和管理体系，加强行业信息安全人才队伍建设。单位设置专门的网络管理机构和岗位，明确网络安全的关键岗位、职责分配、员工技能和员工数量要求，培养行业安全专家。建立行业网络安全专控队伍，定期或不定期开展行业重要信息系统的安全测评和风险评估工作。

其次，加强医疗行业的统筹力度，降低信息安全短板效应。建立建全行业政策、规范及标准，建立符合医疗行业特色的信息安全体系架构，制定具备行业特性的安全要求，针对网络及信息系统的设计、实施、运维等方面提出信息安全指导性意见，为医疗行业单位间在信息安全方面提供平行沟通交流渠道，通过对比及时发现自身问题。

第三，纵深防御信息系统，强化医疗信息数据隐私保护。针对信息的传输和存储部署行而有效网络隔离措施，对系统不同的接入用户在权限上进行严格的分级分类，改进安全感知、安全处置和安全审计等方面的数据防护能力，加强对第三方安全运维单位的监管。

第四，完善医疗设备、商业化软件以及运维服务商的安全审查机制。建立医疗设备及商业化软件的安全审查和安全检测环节，制定设备远程运维过程监管制度。

（本栏责编：冯雪竹）