医疗行业数据安全治理框架研究

王月兵　覃锦端　刘隽良　刘　聪
(杭州美创科技有限公司安全实验室　杭州　310015)
(1005692943@qq.com)

摘　要　随着互联网医疗的深入发展，医疗数据的增长和交换也愈加频繁.由于医疗数据的高度敏感性，如何在互联网医疗的发展过程中保证医疗数据的安全性也越来越受到关注.目前业内针对医疗数据的数据安全治理还没有形成统一的实践，相关国家及行业标准也未能推出.提出了一种针对医疗行业的数据安全治理框架，主要基于数据资产可视化进行数据安全评估，根据数据安全评估结果从管理与技术2个方面介绍了数据安全建设规划，并进行常态化数据安全运营.

关键词　数据安全;数据安全治理;医疗数据安全;数据安全风险评估;数据安全运营

中图法分类号　TP309.2

1　医疗行业数据安全背景

2021年9月1日，《中华人民共和国数据安全法》[1]正式施行.这标志着从法律层面上保障了数据作为生产要素的权利，规范了数据处理活动.而在各种数据中，医疗数据是极特别的一种，基于医疗数据的敏感性，2016年至今，国家也相继出台了不少医疗数据安全政策进行规范，包括《关于促进和规范健康医疗大数据应用发展的指导意见》[2]《互联网诊疗管理办法》《国家健康医疗大数据标准、安全和服务管理办法》等法律法规.由此可见，数据作为一种生产要素，其重要性已不可同日而语.

2　医疗行业数据安全风险

由于医疗数据的敏感性和高价值性，针对医疗数据的犯罪也是层出不穷.目前在数据安全方面主要存在以下安全风险：

1）严峻的网络安全环境.部分医院采用外部接入的方式连接互联网而不是自建互联网医院，网络和数据的主动权不在医院而在互联网服务提供商，缺乏统一的业务和安全规划.此外在医院内部，大量的自助设备、公开的无线网络以及医生办公用的电脑，外部入侵者都能很轻易地接触并进入医院网络.

2）人员数据安全意识缺乏.由于医院患者单体数据的巨大价值，这有意无意地都在挑战人性的弱点.系统使用者的医生或护士、数据库维护人员、第三方开发商都能够很轻易地接触到病人的各类数据.在他们操作数据的过程中，往往缺乏有效的数据管控措施，最终导致数据安全风险.

3）敏感数据流动安全.医院作为一个受到严格管制的行业，需要与众多机构进行数据交换，如医保机构、卫健委、疾控中心等.在数据交换的过程中，涉及到各方主体，缺乏统一的数据安全标准.此外在医院IT系统开发过程中，为了系统的顺利上线，需要使用生产数据进行测试以获得更好的兼容性，在这个过程中，生产数据显然是失控的，极易造成数据泄露.

3　医疗行业数据安全状况研究

3.1　数据安全治理概述

数据安全治理从治理范围来看可以分为国家数据安全治理和组织数据安全治理[3].所谓数据安

收稿日期：2021-12-01

全治理，是数据治理中的一个过程，可以独立进行实施，是数据安全领域中数据、业务、安全、技术、管理的集合.它关注数据的安全保护，以数据业务为出发点，基于数据全生命周期，建立以数据为中心的安全架构体系.

3.2 相关标准研究情况

微软公司于2010年11月提出了治理框架(DGPC).围绕人员、流程和技术3个核心能力维度展开，并与现有的IT管理和控制框架以及数据安全标准等安全标准[4]协同工作，以更好实现数据安全风险控制.

Gartner于2018年4月推出了数据安全治理框架(DSG).框架对各生命周期的数据进行识别、分类和优先级排序，根据CARTA模型选择与数据优先级相匹配的数据安全策略规则和功能，随后部署安全产品、配置策略，并定期或在业务风险发生变化时评估安全策略规则的适用性.

2019年8月30日，GB/T37988—2019《信息安全技术 数据安全能力成熟度模型》(简称DSMM(data security maturity model)[5]正式成为国家标准，并于2020年3月实施.DSMM将数据按照其生命周期分阶段采用不同的能力评估等级.DSMM从组织建设、制度流程、技术工具、人员能力4个安全能力维度进行综合考量，并根据数据安全成熟度划分成1～5个等级，依次为非正式执行级、计划跟踪级、充分定义级、量化控制级、持续优化级，形成一个3维立体模型，全方面对数据安全进行能力建设.

3.3 医疗行业数据安全治理面临的问题

在数据安全治理实践过程中存在大量问题，主要有以下几类：

1) 简单地将数据安全治理等同于网络安全防护[6].在实际数据安全的建设过程中，将网络安全建设措施误认为数据安全措施，进而导致数据安全措施的缺乏.网络安全防护是从系统及网络层面保护承载数据的系统载体不受破坏.数据安全治理是从数据出发，基于数据全生命周期进行的安全防护.这两者是不同的，但也不是孤立的，如在数据传输过程中，同时涉及到网络安全及数据安全，具有一定的交集.

2) 数据安全治理思路不明晰.一方面从组织层面没有具体的数据安全治理小组统筹进行数据安全治理，导致责任不清晰、管理不规范.另一方面组织的数据安全需求不明确，面对数据安全的各项要求，无法分清主次，导致数据安全建设目标和组织要求脱节.

3) 数据繁杂且归属权不清晰，难以保障数据安全.医疗行业涵盖多种业务系统，各种数据分散在不同的业务系统中.在数据安全治理过程中，容易出现眉毛胡子一把抓的情况，没有对数据进行合理的分类分级.其次各类业务系统往往由不同的第三方公司建设，存在系统管理混乱，数据访问管控缺失，出现第三方人员、下属单位、运维人员、外包人员均可以任意访问数据的情况.在医疗数据互联互通的大趋势下，数据的流转更加频繁，由于涉及到的各类流转主体单位不一，其数据安全治理标准往往也不统一.

4) 业务与安全的矛盾性.在实际的数据开发利用过程中，存在用户体验、业务发展、数据安全性这三者难以平衡的情况，结果往往是为了业务发展而丢失数据的安全性.

4 医疗行业数据安全治理框架

4.1 数据安全治理体系

本文提出的数据安全治理体系从数据资产可视化、数据安全评估、数据安全建设、数据安全运营4个维度出发，首先将数据资产可视化，明确了需要保护的数据对象.然后对数据对象进行数据安全评估，全面分析该数据对象可能存在的合规风险和安全风险，同时在安全评估过程中了解当前组织拥有的数据安全能力.在对组织的安全能力和数据安全现状熟悉之后，针对性地从管理和技术2方面进行数据安全建设.并在常态化数据安全运营过程中，不断完善和提升数据安全能力及应急响应能力.

4.2 数据资产可视化

4.2.1 数据资产盘点

数据资产盘点是了解数据资产，明确数据资产构成、特征、范围及流转情况.可通过调研访谈、文件分析、工具探查等多种方式进行，形成数据资产清单、数据权限现状和数据流向图，从而厘清数据资产.

4.2.2 数据分类分级

在数据安全治理过程中，数据分类分级是基础工作，至关重要.只有将数据资产有效分类分级，才能在数据安全防护中实施更合理和精细化的措施，进而在数据全生命周期中实现动态、开放、可视的数据安全治理.数据分类分级主要是数据分类、数据分级 2 个维度.

在《信息安全技术 数据安全分类分级实施指南》中将数据按照重要程度分为重要数据、个人信息数据和其他业务数据 3 大类.具体可基于组织的实际情况，结合医疗行业的分类指南，细化符合组织数据分类方法和标准.

数据分级一般可按照合规性等级、敏感性等级和等级保护等级的要求进行分级，在具体分级过程中需要考虑多种影响因素，如数据影响对象、影响范围、影响程度等，同时结合数据体量、数据实效性进行综合分析，最终完成数据定级.

4.3 数据安全评估

4.3.1 数据基础风险评估

数据基础风险评估主要是针对数据库系统、操作系统、业务系统进行安全基线检查、漏洞扫描、渗透测试，并对发现的脆弱性进行分析，便于后续进行数据基础风险修复，避免信息系统脆弱性被非法利用.

4.3.2 数据安全能力评估

数据安全能力评估是从组织机构整体的数据安全能力成熟度级别的定义以及组织的数据安全管理需求角度出发，评估组织当前的数据安全能力等级.数据安全能力评估首先对组织进行调研，包括系统概况分析、重要数据梳理、过程域解析、过程域评估.在将现状调研清楚后，实施能力测评，实现能力级别的评估.经过数据安全能力评估，组织将清楚自身的数据安全能力级别，为后续数据全生命周期风险评估提供基础，也为数据安全能力级别目标提升提供依据.

4.3.3 数据安全合规风险评估

在数据安全治理过程中，合规是基础和底线.目前合规性评估是基于《中国人民共和国网络安全法》《中国人民共和国数据安全法》《中华人民共和国个人信息保护法》等法律法规，结合医疗行业法规、标准，与组织现状进行对比分析，充分了解其数据安全合规情况，及早规避可能存在的法律风险.

4.3.4 数据全生命周期风险评估

数据全生命周期风险评估基于数据能力成熟度模型 DSMM，针对组织数据收集、存储、传输、使用、交换和销毁等活动，从技术和管理视角出发，按照识别风险、定性分析、定量分析等风险分析的方法，识别组织内数据相关活动或数据资产所存在的安全风险.可首先根据组织的实际情况，确认安全风险评估范围.然后集合过程域、能力维度和风险程度 3 个维度，建立符合组织实际的数据安全风险评估模型.通过数据安全风险评估模型对组织关键控制措施情况进行评估，包括数据机密性、完整性、可用性、可控性、不可否认性、监控力和洞察力等多方面的控制措施情况.

4.4 数据安全建设

4.4.1 数据安全管理建设

数据安全管理建设主要从组织、制度 2 方面，建立起稳定的数据安全运行体系.在数据所有权、使用权、控制权、维护权等权利分属不同主体时，有效地确定各方主体责任与义务，确保数据安全治理措施得到落实.

建立数据安全管理组织架构是数据安全治理工作的基础.组织建设包括部门职责与人员角色确定及动态协同机制.数据安全涉及业务部门、运维部门及安全管理部门，其中业务部门保证业务及数据正常运转，运维部门根据运维体系做好数据运维，安全管理部门进行安全制度制定、安全技术迭代、安全审计、安全检查与事件处理等.根据部门职责后续进一步细化相关人员角色职责.在涉及多部门配合时，以数据流转为基础，对相关人员进行串联，建立有效的动态协同机制，从而充分利用部门资源解决部门运转孤岛问题.

良好的制度建设可以为数据安全管理提供依据和保障.制度建设包括数据安全治理规章制度、管控办法、奖惩机制、技术规范等.由分管领导、数据安全人员、数据管理人员以及相关人员共同制定及执行，形成组织层面的数据安全治理管理制度规范.

4.4.2 数据安全技术建设

数据安全技术建设是基于数据资产可视化、数据安全评估结果，以业务需求为导向，采用层次化、开放式、SOA 耦合架构，利用人工智能[7]、网络技术、云计算、大数据等技术和理念，定制化构建一套符合组织实际的数据安全技术体系.总体上数

据安全技术建设包括数据内控合规、数据全域可管、数据全局可视3方面.

数据内控合规主要为内部管控与合规建设.基于国家法律法规、医疗行业政策、组织安全制度规范以及数据分类分级结果,建设数据安全技术架构.内控合规技术涵盖敏感数据发现、数据动/静态脱敏、数据库日志审计、权限管控和数据资产保护、身份鉴别、高危操作防护、访问控制、特权管理等.

数据全域可管侧重组织数据安全全面感知及管理.基于已有的网络安全和内控安全措施,防御外部和数据流动风险,主要包括入侵防护、漏洞防御、访问控制、误操作恢复、数据加密、计算环境安全、溯源管理、数据加密等,通过数据安全管理平台进行整体的数据全域管理.

数据全局可视是以日志信息、风险操作、告警、数据库运行状态等大数据为基础,从全局视角提升对数据安全威胁的发现识别、理解、分析和响应能力的防护方式.能够将数据资产分布状况、敏感数据访问行为进行动态展示,并通过流量关联分析,预测数据资产可能面临的安全风险,实现统一监控和全局可视.

4.5 数据安全运营

数据安全运营是将数据安全管理体系建设和数据安全技术体系建设以有效运营的方式持续推行并使用下去.通过数据安全策略的持续优化、数据安全规范要求结合业务的持续改进,以及对已发生数据安全事件的处理与后续风险整改措施等,实现从制度指导与策略制定,到事件识别与风险处置,再回归到优化改进制度及策略的闭环持续化运营.

数据安全运营工作机制可从预测、防御、检测、调查取证4个维度,以持续性监控和分析为核心,结合业务特征提炼真实的风险场景及隐私要求,通过技术手段实现对法律法规的遵从性,并建立匹配的治理方案、工具及方法论,形成可收敛的运营体系,使业务运转良性化,实现安全与业务目标一致.

当数据安全事件发生后,启动数据安全应急响应工作机制,该机制建设可参考PDCERF,包括准备阶段、检测阶段、抑制阶段、根除阶段、恢复阶段、总结阶段这6个阶段.PDCERF并不是应急响应的唯一方法,在实际应急过程中不一定严格按照6个阶段的顺序进行,但它是目前适用性较强的应急响应通用方法.

参 考 文 献

[1] 全国人民代表大会常务委员会. 中华人民共和国数据安全法[EB/OL]. (2021-06-10)[2021-12-24]. http://www.gov.cn/xinwen/2021-06/11/content_5616919.htm

[2] 中国人民共和国国务院办公厅. 国务院办公厅关于促进和规范健康医疗大数据应用发展的指导意见[EB/OL]. (2016-06-24)[2021-12-24]. http://www.cac.gov.cn/2016-06/24/c_1119109041.htm

[3] 中国信息通信研究院云计算与大数据研究所. 数据安全治理实践指南(1.0)[R]. 北京:中国信息通信研究院,2021

[4] 高亚楠,刘丰,陈永刚. 信息安全风险管理标准体系研究[J]. 信息安全研究,2018,4(10):928-933

[5] 全国信息安全标准化技术委员会. GB/T 37988 2019 信息安全技术 数据安全能力成熟度模型[M]. 北京:中国标准出版社,2019

[6] 胡国华. 数据安全治理实践探索[J]. 信息安全研究,2021,7(10):915-921

[7] 魏国富,石英村. 人工智能数据安全治理与技术发展概述[J]. 信息安全研究,2021,7(2):110-119

王月兵

高级工程师.主要研究方向为数据安全、零信任、网络安全.

1005692943@qq.com

覃锦端

工程师.主要研究方向为网络安全、数据安全、漏洞挖掘.

tuolajl@163.com

刘隽良

高级工程师.主要研究方向为协议安全分析、隐私增强技术、认证协议设计.

my123feixue@126.com

刘 聪

工程师.主要研究方向为漏洞挖掘、安全工具开发.

liucong@mchz.com.cn