ICS 35.040
L 80

中华人民共和国国家标准

GB/T XXXXX—XXXX

信息安全技术
健康医疗数据安全指南

Information security technology —

Guide for health data security

在提交反馈意见时，请将您知道的相关专利与支持性文件一并附上

（征求意见稿）

（本稿完成日期：2019/4/4）

XXXX－XX－XX 发布　　XXXX－XX－XX 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

目　次

前　言

本标准按照GB/T 1.1—2009《标准化工作导则　第1部分：标准的结构和编写》给出的规则起草。

请注意本文件的其他内容可能涉及专利，本文件的发布机构不承担识别这些专利的责任。

本标准由全国信息安全标准化技术委员会（SAC/TC260）提出并归口。

本标准主要起草单位：清华大学、北京清华长庚医院等。

本标准主要起草人：金涛、刘海一等。

引　言

健康医疗数据包括个人健康医疗数据以及由个人健康医疗数据加工处理之后得到的健康医疗相关数据。随着健康医疗数据应用和“互联网+医疗健康”应用的蓬勃发展，各种新业务、新应用不断出现，健康医疗数据在全生命周期各阶段均面临着越来越多的安全挑战，安全问题频发。由于健康医疗数据安全事关患者生命安全、个人信息安全、社会公共利益和国家安全，为了更好的保护健康医疗数据安全，规范和推动健康医疗数据的融合共享、开放应用，促进健康医疗事业发展，特制定健康医疗数据安全指南标准。

本标准重点围绕个人健康医疗数据安全展开，明确了安全目标、使用目的分类、数据分类分级、角色分类、场景分类、使用披露指南、安全措施要点、安全技术指南包括去标识化指南、安全管理指南。针对常见的健康医疗应用场景，包括医院互联互通、远程医疗、二次利用、临床研究、健康传感数据管理、移动应用、患者查询、商保对接、医疗器械远程维护等，分别提出了针对性的重点安全措施建议。

附录A给出了个人健康医疗数据范围参考，附录B给出了卫生信息数据集分类与标准，附录C给出了医院数据使用管理办法参考，附录D给出了数据申请审批表参考，附录E给出了数据处理（使用）协议参考，附录F给出了检查用表格参考。

涉及人类遗传资源数据（是指含有人体基因组、基因及其产物的器官、组织、细胞、血液、制备物、重组脱氧核糖核酸（DNA）构建体等遗传材料的信息资料），参考相关部门要求。

涉及健康医疗数据的出境安全保护，参考数据出境安全评估相关要求。

涉及国家秘密的健康医疗数据应按照国家保密工作部门有关涉密信息系统分级保护的管理规定和技术标准，结合系统实际情况进行保护。

信息安全技术　健康医疗数据安全指南

1　范围

本标准给出了健康医疗数据控制者在保护健康医疗数据时可采取的措施指南。

本标准适用于指导健康医疗数据控制者对健康医疗数据进行安全保护，也可供健康医疗、网络安全相关主管部门以及第三方评估机构等组织开展健康医疗数据的安全监督管理与评估等工作时参考。

2　规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是标注日期的引用文件，仅标注日期的版本适用于本文件。凡是不标注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 25069—2010　信息安全技术　术语

GB/T 31168—2014　信息安全技术　云计算服务安全能力要求

GB/T 22080—2016　信息技术　安全技术　信息安全管理体系　要求

GB/T 35273—2017　信息安全技术　个人信息安全规范

GB/T 35274—2017　信息安全技术　大数据服务安全能力要求

GB/T 22239—AAAA　信息安全技术　网络安全等级保护基本要求

GB/T BBBBB—BBBB　信息安全技术　个人信息去标识化指南

3　术语和定义

GB/T 25069—2010中界定的以及下列术语和定义适用于本文件。

3.1

个人健康医疗数据　personal health data

能够单独或者与其他信息结合识别特定自然人或者反映特定自然人生理或心理健康的相关数据。

注：涉及个人过去、现在或将来的身体或精神健康状况、接受的医疗保健服务和支付的医疗保健服务费用等，详见附录A。

3.2

健康医疗数据　health data

包括个人健康医疗数据以及由个人健康医疗数据加工处理之后得到的健康医疗相关数据。

注：例如经过对群体健康医疗数据处理后得到的群体总体医疗数据分析结果、趋势预测和疾病防治统计数据等。

3.3

个人健康医疗数据主体　personal health data subject

个人健康医疗数据所标识的个人。

3.4

健康医疗数据控制者 health data controller

能决定健康医疗数据处理目的、方式等的组织或个人。

3.5

健康医疗服务 health service

由健康医疗领域专业人员或专业辅助人员提供的对健康状况有影响的服务。

3.6

健康医疗信息系统 health information system

以计算机可处理的形式采集、存储、处理、传输、访问、销毁健康医疗数据的系统。

3.7

健康医疗专业人员 health service professional

经政府或行业组织授权有资格履行特定健康医疗服务职责的人员。

3.8

受限制数据集 limited data set

经过基本的去标识化处理，但仍可识别相应个人的、需要保护的个人健康医疗数据集。

注1：例如删除与个人及其家属、家庭成员和雇主直接相关的标识。

注2：该数据集可在未经个人授权的情形下用于科学研究、医学/健康教育、公共卫生等目的。

3.9

治疗笔记 notes of treatment

健康医疗专业人员在提供健康医疗服务过程中记录的观察、思考、方案探讨、结论等内容。

注：治疗笔记具有知识产权属性，归健康医疗专业人员及其单位所有。

3.10

披露 disclosure

将个人健康医疗数据向特定个人或组织进行转让、共享，以及向不特定个人、组织或社会公开发布的行为。

3.11

临床研究 clincial research

用于确认针对人的药物、医疗器械、生物制品、体外诊断试剂、临床信息系统、诊断产品和治疗方案等的安全性和有效性的研究。

注：属于医学研究的一个分支。

4 缩略语

下列缩略语适用于本文件。

ACL：访问控制列表（Access Control Lists）

EDC：电子数据采集（Electronic Data Capture）

GCP：临床试验规范标准（Good Clinical Practice）

HIS：医院信息系统（Hospital Information Systems）

HIV：艾滋病病毒（Human Immunodeficiency Virus）

ID：身份标识（Identity）

IP：互联网协议（Internet Protocol）
IPSEC：网际协议安全（Internet Protocol Security）
IT：信息技术（Information Technology）
LDS：受限制数据集（Limited Data Set Files）
PDCA：规划-实施-检查-改进（plan-do-check-action cycle）
PIN：个人识别号码（Personal Identity Number）
PUF：公用数据集（Public Use Files）
RIF：可识别数据集（Research Identifiable Files）
TLS：传输层安全（Transport Layer Security）
USB：通用串行总线（Universal Serial Bus）
VPN：虚拟专用网络（Virtual Private Network）

5 安全目标

健康医疗数据包含个人标识、健康状况以及医疗情况等相关信息，这些数据的合理使用对于健康护理、医学治疗以及科学研究具有积极促进作用。但鉴于健康医疗数据的特殊性，这些数据如被泄漏、篡改或滥用，会影响健康护理、医学治疗以及科学研究效果，在更严重的情况下会导致医疗事故发生。另一方面，健康医疗数据大量涉及个人信息，数据的泄漏、滥用和不正当披露会对个人信息安全造成侵害，甚至可能影响个人正常生活。进一步地，健康医疗数据还和公众利益、国家安全密切相关，例如涉及特殊疾病、基因等健康医疗数据如果被泄漏或滥用，还可能对公众利益和国家安全造成严重后果。

健康医疗数据控制者为保护个人健康医疗数据应采取合理和适当的管理和技术保障措施，以达到以下目标：

a） 保护健康医疗数据的保密性、完整性和可用性；
b） 确保健康医疗数据使用和披露过程的安全性，保护个人信息安全、公众利益和国家安全；
c） 确保健康医疗数据在符合上述安全要求的前提下满足业务需求。

6 分类分级指南

6.1 目的分类

健康医疗数据的使用目的一般可分为医疗卫生服务、监督管理、决策支持、临床研究、健康生活、医学教育和二次利用等，详见表1所示。

表1 使用目的分类

序号	使用目的	描述	涉及的相关方	相关方举例
1	获取医疗卫生服务	主要关注的是如何能获得可及的、优质的医疗卫生服务；获取连续的健康医疗数据、全程的健康管理等方面	居民个人	患者、健康个人
2	提供基本医疗卫生服务	提供基本医疗和基本公共卫生服务与管理，例如门急诊、常见病的住院治疗、妇幼保健、计划生育、免疫接种、慢病管理、老年保健、康复、健康教育等基本医疗、预防保健服务	基层医疗卫生服务机构	社区卫生服务机构 乡镇卫生院 诊所
3	提供专业医疗卫生服务	疾病管理、卫生管理、应急管理、医疗咨询等，对患者进行检查、诊断、治疗和康复等方面的服务以及与这些	专业医疗卫生服务机构	医院 疾病预防控制机构 妇幼保健机构

		服务有关的提供药品、医用材料器具、救护车、病房住宿和饮食的业务		急救中心
				血站
				生殖遗传咨询机构
4	监督管理	以政府为核心的公共部门整合社会的各种力量，强化政府的治理能力，提升政府绩效和公共服务品质，从而实现公共的福利与公共利益。提高区域资源共享水平、强化绩效考核、提高监督管理能力、化解疾病风险等。	卫生行政管理机构	卫健委
				食品药品监督管理机构
				卫生监督机构
5	决策支持	通过大量健康数据进行统计分析,推动医保/新农合业务的开展，完成审核监督、定点医疗机构布点、医保政策制定或更新等辅助管理	其他医疗卫生服务相关机构	医疗保险机构
		从民政系统获取妇女婚姻、残疾人群信息，将划定年龄段的已婚女性作为孕产妇保健预备管理对象，为残疾人群建立残障专项档案、提供残疾康复管理		民政部门
		获取出生人口信息、户口迁入人口信息，触发新增人群（出生、户口迁入）的健康档案建档工作		公安部门
6	提供医疗卫生辅助服务	为居民提供更加丰富更加便捷的健康服务		金融保险机构
		为医疗卫生服务机构提供专业化的信息系统和技术支持		信息系统供应商
		为医疗卫生服务机构提供专业化的医疗设备和技术支持		医疗设备供应商
7	临床研究	以患者为主要研究对象的医学科学研究，主要分析研究疾病的病因、诊断、治疗、预防、自然病程及预后等方面的重要问题		医药企业
				科研机构
8	健康生活	包括通过获取本人的医疗数据来督促人们改变不良的行为习惯，帮助养成积极健康的生活方式等		体检中心、养老院、健康管理机构
9	医学教育	根据社会需求，有目的、有计划、有组织地培养医药卫生人才的教育活动，一般多指大学水平的医学院校教育	医学教育机构	医学教育机构
10	二次利用	政府部门、科研人员、企业公司等第三方对一定批量的医疗数据进行二次分析利用（分析利用目的与数据采集目的不同）	第三方	政府部门、科研人员、企业公司等
			数据汇聚中心	医疗机构、区域卫生信息平台、医联体、学术平台等

6.2 数据分类

健康医疗数据可以分为个人属性数据、健康状况数据、医疗应用数据、医疗支付数据、卫生资源数据以及公共卫生数据等，具体内容如表 2 所示。其中，在数据交换和共享等场景中使用的卫生信息数据集分类和标准可参考附录 B。

a) 个人属性数据指能够单独或者与其他信息结合识别特定自然人的数据。
b) 健康状况数据是指能反映个人健康情况或同个人健康情况有着密切关系的数据。
c) 医疗应用数据是指能反映医疗保健、门诊、住院、出院和其他医疗服务情况的数据。
d) 医疗支付数据是指医院在提供医疗服务过程中所有与费用相关的数据。
e) 卫生资源数据是指那些可以反映卫生服务人员、卫生计划和卫生体系的能力和特点的数据。
f) 公共卫生数据是指关系到国家或地区大众健康的公共事业相关数据。

表2　健康医疗数据分类与范围

数据类型	范围
个人属性数据	1)人口统计信息，包括姓名、年龄、性别、民族、国籍、职业、住址、工作单位、家庭成员信息、联系人信息、收入等； 2)个人身份信息，包括姓名、身份证、工作证、居住证、社保卡、可识别个人的影像图像、健康卡号、住院号、各类检查检验相关单号等； 3)个人通讯信息，包括个人电话号码、邮箱、账号及关联信息等； 4)个人生物识别信息，包括基因、指纹、声纹、掌纹、耳廓、虹膜、面部特征等； 5)个人健康监测传感设备ID等。
健康状况数据	主诉、现病史、既往病史、体格检查（体征）、家族史、症状、健康体检数据、遗传咨询数据、可穿戴设备采集的健康相关信息、生活方式等。
医疗应用数据	门（急）诊病历、门（急）诊处方、住院医嘱、检查检验报告、用药信息、病程记录、手术记录、麻醉记录、输血记录、护理记录、入院记录、出院小结、转诊（院）记录、知情告知信息、基因测序、转录产物测序、蛋白质分析测定、代谢小分子检测、人体微生物检测等。
医疗支付数据	1)医疗交易信息包括医保支付信息、交易金额、交易记录等； 2)保险信息包括保险账号、保险状态、保险金额等。
卫生资源数据	医院基本数据、医院运营数据、医院公卫数据等。
公共卫生数据	环境卫生数据、传染病疫情数据、疾病监测数据、疾病预防数据、出生死亡数据等。

6.3　数据分级

根据数据重要程度和风险级别，分级可划分为以下5级：

a)　第1级：可完全公开使用的数据。例如医院名称、地址、电话和网站等。

b)　第2级：较大范围内可以访问使用的数据。例如不能标识个人身份的数据，各科室医生均可以用于研究分析。

c)　第3级：中等范围内可以访问使用的数据。例如经过部分去标识化处理，但仍可能重标识的数据；或者相关医护人员可以查看的概要级资料。

d)　第4级：较小范围内可以访问使用的数据。例如可以直接标识个人身份的数据，仅限于经治医生访问。

e)　第5级：极小范围内严格限制访问使用的数据。例如绩效评价、药品消耗等数据，或者特殊病种的详细资料。

6.4　角色分类

针对特定数据，在特定的场景，相关组织或个人可划分为以下四类角色。针对特定的组织或个人，围绕特定的数据，在特定的场景，只能归为其中的一个角色。

a)　个人健康医疗数据主体（简称**主体**）：个人健康医疗数据所标识的个人。

b)　健康医疗数据控制者（简称**控制者**）：能决定健康医疗数据处理目的、方式及范围等的组织或个人，包括提供健康医疗服务的组织、医保机构、政府机构、健康医疗科学研究机构、个体诊所等，其以电子形式传输或处理健康医疗数据。判断组织或个人能否决定健康医疗数据的处理目的、方式及范围可以考虑：

1)　该项健康医疗数据处理行为是否属于该组织或个人履行某项法律法规规定所必须；

2)　该项健康医疗数据处理行为是否为该组织或个人行使其公共职能所必须；

3)　该项健康医疗数据处理行为是否由该组织或个人自行决定；

4)　是否由相关个人或者政府授权。

c） 健康医疗数据处理者（简称**处理者**）：代表控制者采集、使用、处理或披露其掌握的个人健康医疗数据，或为控制者提供涉及个人健康医疗数据的使用、处理或者披露服务的相关组织或个人。常见的处理者有：健康医疗信息系统供应商、健康医疗数据分析公司、辅助诊疗解决方案供应商等。

d） 健康医疗数据使用者（简称**使用者**）：针对特定数据的特定场景，不属于主体，也不属于控制者和处理者，但对健康医疗数据进行利用的相关组织或个人。

6.5 场景分类

基于角色以及角色之间的数据流动，数据流通使用场景可分为以下6类，如图1所示。

a） 主体-控制者间数据流通使用；

b） 控制者-主体间数据流通使用；

c） 控制者内部数据流通使用；

d） 控制者-处理者间数据流通使用；

e） 控制者间数据流通使用；

f） 控制者-使用者间数据流通使用。

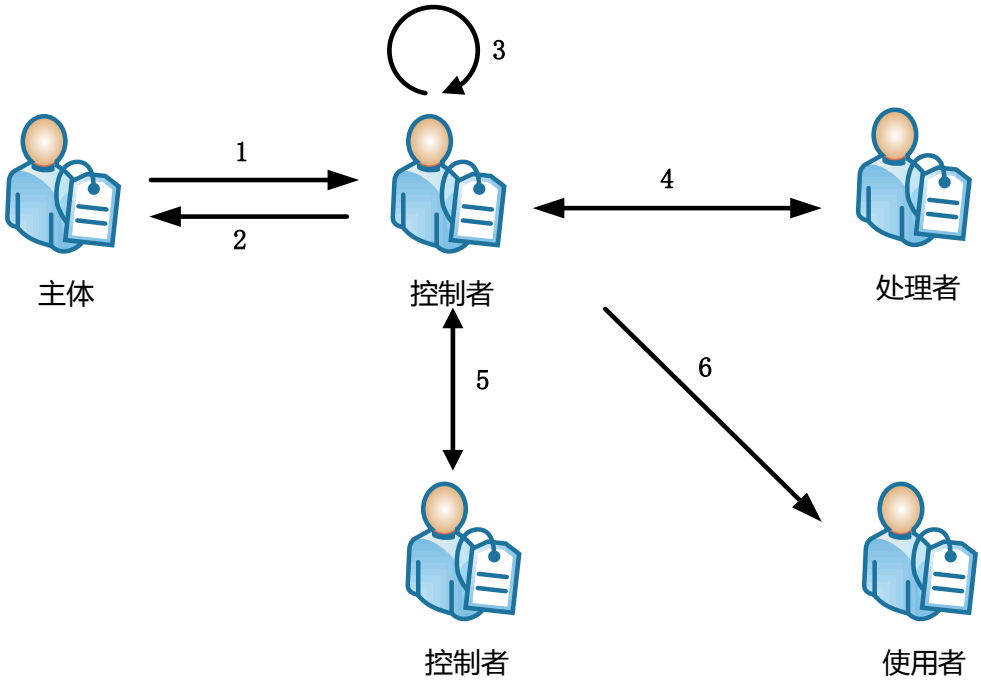


图1 数据流通使用场景分类示意图

7 使用披露指南

控制者在使用或披露个人健康医疗数据的过程中，应遵循以下指南：

a） 控制者在使用或披露相应个人健康医疗数据时，应获得作为主体的个人授权；所有授权应使用通俗易懂的语言，并且包含有关要披露或使用的数据内容、数据的接收方、数据的用途以及使用方式、数据使用期限、数据主体权利以及控制者采取的保护措施等具体信息。使用个人健康

医疗数据不能超出与个人授权的用途具有直接或合理关联的范围。因业务需要，确需超出上述范围使用的，应再次征得主体同意。

b) 控制者在没有获得主体的授权时，在以下情况可以使用或披露相应个人健康医疗数据：
   1) 向主体提供其本人健康医疗数据；
   2) 治疗、支付或保健护理时；
   3) 涉及公共利益或法律法规要求时；
   4) 用于科学研究、医学/健康教育、公共卫生或医疗保健操作目的的受限制数据集；
   在上述情况下，控制者可依靠法律法规要求、职业道德和专业判断来确定哪些个人健康医疗数据允许被使用或披露。

c) 控制者应获得主体授权才能使用或披露个人健康医疗数据进行市场营销活动，但控制者与主体之间进行面对面的营销沟通除外。用于市场营销活动的授权应以合理方式提示主体，并让其充分知悉，明确的作出自主的同意。该授权应是独立的，并且不得作为主体获得任何公共服务、医疗服务或者捆绑于其他的服务条款之中。控制者在取得授权的同时，应书面告知主体其有权随时撤销该授权。

d) 主体（或其授权代表）有权访问其个人健康医疗数据或要求披露其数据，控制者应按其要求披露相应个人健康医疗数据。

e) 主体有权复查并获得其个人健康医疗数据的副本，控制者应提供。

f) 主体发现控制者所持有的该主体的个人健康医疗数据不准确或不完整时，控制者应为其提供请求更正或补充信息的方法。

g) 主体有权对控制者或其处理者使用或披露数据的情况进行历史回溯查询，最短回溯期为六年。

h) 主体有权要求控制者限制使用或披露个人健康医疗数据以进行诊断、治疗、支付或健康服务等，限制向相关人员披露信息，控制者没有义务同意限制请求；但一旦同意，除非法律法规要求以及医疗紧急情况下，控制者应遵守商定的限制。

i) 控制者可以使用治疗笔记用于治疗，在进行必要的去标识化处理后，可以在未经个人授权的情况下使用或披露治疗笔记进行内部培训和学术研讨。

j) 控制者应制定、实施合理的策略和流程，将使用和披露限制在最低限度。

k) 控制者应确认处理者的安全能力满足安全要求，并签署数据处理协议后，才能让处理者为它进行数据处理，处理者不能自行决定数据处理的目的、方式等。

l) 控制者向政府授权的第三方控制者传送数据前，应获得加盖政府公章的相关文件，数据安全责任由第三方控制者承担。

m) 控制者在确认数据使用的合法性、正当性和必要性后，并确认使用者具备相应数据安全能力，使用者签订数据使用协议并承诺保护受限制数据集中的个人健康医疗数据后，可将受限制数据集用于研究、医疗保健业务和公共卫生等目的；使用者只能在协议约定的范围内使用数据并承担数据安全责任，在使用数据完成后，应进行彻底销毁。

n) 控制者针对个人健康医疗数据汇聚分析处理之后得到的不能识别个人的健康医疗相关数据的使用和披露应遵守国家相关法规要求。

o) 控制者因为学术研讨需要，需要向境外提供相应数据的，在进行必要的去标识化处理后，经过数据安全委员会讨论审批同意，数量在250条以内的非涉密非重要数据可以提供，否则应提请相关部门审批同意。

p) 经主体授权同意，不涉及秘密、重要数据的，控制者可向境外目的地传送个人健康医疗数据，数量应控制在250条以内，否则应提请相关部门审批。

q） 不将健康医疗数据在境外的服务器中存储，不托管、租赁在境外的服务器；存储个人生物识别信息时，应采用技术措施处理后再进行存储，例如仅存储个人生物识别信息的摘要；健康医疗数据存储传输实施加密，通过介质传输的，应对介质的使用实施管控。

8 安全措施要点

8.1 分级安全措施要点

可以根据数据保护的需要进行数据分级，对不同级别的数据实施不同的安全保护措施，重点在于授权管理、身份鉴别、访问控制管理。例如，从个人信息安全风险出发划分的数据分级和安全措施要点如表3所示。医生调阅场景下的数据分级及安全措施详见11.1.4.3。临床研究场景下的数据分级详见11.4.4.3。

表3 从个人信息安全风险出发的数据分级与安全措施要点

数据分级	数据特点	适用场合	特征与案例	安全措施要点
第 1 级	**业务要求**：可公开发布 **数据内容**：某些统计值 **数据接收与使用者**：大众	公告	需要公众了解，例如剩余床位信息、剩余可就诊号源信息	是否可公开需要评审
第 2 级	**业务要求**：不需要识别个人 **数据内容**：一般人口信息、各类医疗、卫生服务信息 **数据接收与使用者**：不可识别	管理、研究、教育与统计分析	例如病例分析、各类病种分布统计、流行病研究、疾病队列研究等 **场景举例**：临床研究、医学健康教育、药品/医疗器械研发	应进行去标识化处理，通过协议或领地模式管控，应确保数据的完整性和真实性
第 3 级	**业务要求**：服务对象个人可识别，周边人不易识别 **数据内容**：部分个人可识别信息或代码，与其他信息内容分离，例如张 XX、排队序号等 **数据接收与使用者**：不识别个人，局部小范围人群	服务对象告知	在公开场合通知服务对象，例如门诊叫号、检查叫号、体检服务叫号等	个人信息需部分遮蔽，环境与接收人数量受到限制
第 4 级	**业务要求**：必须准确识别个人 **数据内容**：包含完整准确的个人健康医疗数据 **数据接收与使用者**：可识别的个人、有审计、保护隐私义务	个性化服务与管理	针对个人的医疗服务、卫生健康服务，传染病管控、基因组测序等 **场景举例**：医院互联互通、远程医疗、健康传感数据管理、移动应用、商保对接	由于涉及个人标识信息，环境与接收人应严格管控，应高标准保证数据完整性和可用性
第 5 级	**业务要求**：运营需要 **数据内容**：绩效或药品消耗等 **数据接收与使用者**：可识别的个人、有审计、有保密义务	医院运营管理	医院运营需要，仅限相关责任人知悉。例如绩效评价、药品采购	身份鉴别、访问控制

8.2 场景安全措施要点

基于数据流通使用场景的不同，各角色在健康医疗数据应用过程中所涉及的安全环节与责任不同，安全环节与责任决定了各角色需要满足的安全控制要求。数据使用的应用场景和安全措施要点如表4所示，针对常见场景需要重点关注的安全措施详见第11章。

表4　数据使用安全责任与安全措施要点

场景分类	安全环节	安全责任与安全措施要点	场景与用户举例
主体-控制者间数据流通	采集安全	**控制者**：采集数据知情同意	**场景举例**：医院就诊、健康传感、移动应用 **主体**：个人 **控制者**：医疗机构、科研机构、医保机构、商业保险公司、健康服务企业
	传输安全	**控制者**：加密、存储介质管控	
	存储安全	**控制者**：境内存储、加密、分类分级、去标识化、备份恢复、存储介质管控	
控制者-主体间数据流通	传输安全	**控制者**：加密、存储介质管控	**场景举例**：患者查询 **主体**：个人 **控制者**：医疗机构
	使用安全	**控制者**：身份鉴别、访问控制、敏感数据控制	
控制者内部数据使用	收集安全	**控制者**：收集数据知情同意、审批	**场景举例**：内部数据使用 **控制者**：医疗机构
	处理安全	**处理者**：去标识化、权限管理、质量管理、元数据管理	
	使用安全	**控制者**：审批授权、身份鉴别、访问控制、审计	
	存储安全	**控制者**：境内存储、加密、分类分级、去标识化、备份恢复、存储介质管控	
控制者-处理者间数据流通	传输安全	**控制者**：传输前的审查、评估、授权；加密、审计、流量控制、存储介质管控 **处理者**：数据传输加密、传输方式控制	**场景举例**：医疗器械维护 **控制者**：医疗机构、政府机构 **处理者**：科研机构、健康医疗信息服务企业、医疗器械厂商
	处理安全	**处理者**：去标识化、权限管理、质量管理、元数据管理、审计	
	存储安全	**控制者**：境内存储、加密、分类分级、去标识化、备份恢复、存储介质管控、管理处理者数据存储过程 **处理者**：境内存储、加密、分类分级、去标识化、备份恢复、存储介质管控、销毁机制	
控制者间数据流通	传输安全	**控制者 A**：对接安全、加密、审计、流量控制、存储介质管控 **控制者 B**：对接安全、加密、审计、流量控制、存储介质管控	**场景举例**：互联互通；远程医疗 **控制者**：政府机构、医疗机构、医保机构
	使用安全	**控制者 A**：审批授权、身份鉴别、访问控制、审计 **控制者 B**：审批授权、身份鉴别、访问控制、审计	
	存储安全	**控制者 A**：境内存储、加密、分类分级、去标识化、备份恢复、存储介质管控、销毁机制 **控制者 B**：境内存储、加密、分类分级、去标识化、备份恢复、存储介质管控、销毁机制	
控制者-使用者间数据流通	传输安全	**控制者**：传输前的审查、评估、授权；加密、审计、流量控制、存储介质管控	**场景举例**：商保对接、临床研究、二次利用 **控制者**：医疗机构 **使用者**：商业保险公司、科研机构
	使用安全	**使用者**：审批授权、身份鉴别、访问控制、审计	
	存储安全	**控制者**：境内存储、加密、分类分级、去标识化、备份	

		恢复、存储介质管控、管理使用者数据存储过程 **使用者：**境内存储、加密、分类分级、去标识化、备份恢复、存储介质管控、销毁机制	

注：数据在实际应用场景中存在一个控制者对应多个使用场景的情况，此时需参照多个数据使用场景安全措施要点实施安全措施。

9 安全技术指南

9.1 通用安全技术指南

控制者应参照GB/T 22239—AAAA、GB/T 31168—2014和GB/T 35274—2017等做好数据安全管理工作。

a) 对承载健康医疗数据的信息系统和网络设施以及云平台等进行必要的安全保护。
b) 应针对数据生命周期相关的数据活动，形成数据采集、数据传输、数据存储、数据处理、数据交换、数据销毁等数据安全要求，以降低安全风险，保障数据安全。
c) 应按照规划、开发、部署到运维的系统生命周期各阶段特点，从信息技术角度对数据平台与应用采取必要的安全管控措施，建立安全的数据管理基础设施，降低数据平台与应用运行安全风险，保障业务目标和可持续性。
d) 应对健康医疗数据进行分类分级管理，制定、实施合理的策略和流程，将使用和披露限制在最低限度，安全措施要点参照第8章。
e) 应做好身份鉴别、访问控制、安全审计、入侵防范、恶意代码防范及介质使用管理。
f) 应确保数据质量、完整性，做好备份恢复和剩余信息保护等。
g) 采用密码技术保证数据在传输和存储过程中的保密性。
h) 涉及健康医疗数据的出境安全保护，参考数据出境安全评估相关要求。
i) 密码技术使用需符合国家密码管理相关要求。
j) 应符合重要数据管理、关键信息基础设施安全管理等政策的相关通用要求。

9.2 去标识化指南

控制者应参照GB/T BBBBB—BBBB执行，且只能应用于受控公开共享或领地公开共享（控制者完全控制的环境），应通过数据使用协议约定数据使用目的、方式、期限、安全保障措施等。去标识化策略、流程和结果宜由数据安全委员会审批。数据应用于临床研究和医药/医疗研发时，相关要求如下：

a) 可以唯一识别到个人的信息或披露后会给患者造成重大影响的信息应去除，例如：姓名；身份证/驾照等证件号；电话号码、传真、电子邮件；医疗保险号、病历档案号、账户；生物识别（指纹、视网膜、声音、基因等）；照片；爱好、信仰等。
b) 模糊化后仍有医学意义的数据可以保留模糊后的结果，例如：
   1) 单位、地址、邮政编码等信息，如果单位信息和其他信息组合识别的人群在2万人以上，可以保留单位信息；如果地址信息包括省（直辖市）、市（县）、街道（乡镇）和其他信息组合识别的人群在2万人以上，可以保留，否则应去除街道（乡镇），保证组合识别的人群在2万人以上；如果邮编信息和其他信息组合识别的人群在2万以上，可以保留，否则应将邮编低位设置为‘0’，保证可以识别的人群在2万以上。
   2) 对具体年龄进行泛化处理，例如给出一个年龄范围。例如：38岁可以转换成30-40岁，确保同区域内满足相同年龄条件的人数在2万人以上。
   3) 生日及其他所有日期信息，例如：入院时间、出院时间，只能具体到年，或者进行时间漂移处理。

c） 应删除医护人员姓名以及其他身份标识信息；
d） 数据集中所有属性值相同的人数最低应在5人以上；
e） 对需要追溯到患者的情况，应由控制者内部建立患者代码索引；
f） 去标识化过程中使用的各种参数配置，例如时间漂移范围、患者代码索引、各种个人代码生成规则等应严格保密，仅限于控制者内部专人管理；
g） 在需要进行重标识确定主体时，只能由控制者内部专人处理，处理过程严格保密；
h） 使用者不能参与去标识化相关工作；
i） 应通过签署数据使用协议约束数据的使用目的、期限以及数据保护措施等；
j） 在受控公开共享模式下，使用者需具备数据使用情况审计的能力，并接受控制者审计。

相关示例如表5所示。

表5 去标识化示例

属性	去标识化方法建议	适用数据
姓名（例如：受试者姓名、研究者姓名、医生姓名等）	建议删除或置空	受试者姓名、医生姓名、研究者姓名、家庭成员姓名
联系方式（例如：个人电话号码、邮箱、详细住址等）	建议删除或置空或泛化 例如：住址只具体到市县级，隐藏县级以下地址	个人电话号码、邮箱、账号、住址
日期（例如：入院日期、治疗日期、手术日期等）	建议采用"时间偏移方法”或转换法或泛化 例如： 为不同研究项目定义不同的随机偏移量，通过日期时间+或- 随机偏移量进行数据扰动，以实现数据的去标识化 例如： 入院日期2018-01-01 + 随机偏移量 100 = 入院日期：2018-04-11 出院日期2018-04-01 + 随机偏移量 100 = 出院日期：2018-07-10 入院日期-出院日期= 90天 通过该方法可以保证数据去标识化的同时保证计算逻辑正确。 转换法即用其与其他日期运算得到结果来替换，例如年龄、住院天数。 泛化只保留年月，甚至只保留年。	医疗应用数据中的能通过数据分析关联到个人的时间信息：例如入院日期、出院日期、手术日期等
出生日期	建议删除或置空或者替换为年龄	出生日期
年龄	建议采用“数据泛化”方法 例如 - 年龄≤89 或者 >89 - 年龄区间 <25, 25-29, 30-34,...,85-89 >89 注:>89不能再继续细分	年龄
号码（例如：邮编、身份证号、社保号等）	建议删除或置空 如需要利用到号码的唯一性进行逻辑分析，例如通过身份证号判断多份病历是否属于一个人的场景，可采用基于原数据的随机化产生唯一标识进行替换。	身份证号、社保卡号、工作证号、居住卡号

	如需要利用邮编等隐含地理信息的号码，可采用扰动和泛化方法进行处理 例如：原始邮编记录100080，去标识化后100***	
医疗机构内部所用号码	建议置换或删除 通过这些号码进行逻辑分析而需要保留的，可采用基于原数据的随机化产生唯一标识进行替换。 如不需要这些号码进行逻辑分析，则删除这些号码；	检验结果报告单号、检查报告单号、住院号、门（急）诊号等

10 安全管理指南

10.1 概述

控制者为实现第5章所述安全目标，按照GB/T 22080—2016要求，参照第6章进行数据分类分级、场景分析，分析健康医疗数据安全面临的风险，有针对性的采取安全措施，并对实施措施后的效果进行检查，迭代改进。

首先应建立完善的组织保障体系，组织架构上至少包括健康医疗数据安全委员会和健康医疗数据安全工作办公室，以确保做好健康医疗数据安全管理工作，并形成相应的文档记录，包括但不限于：

a) 建立健康医疗数据安全委员会（简称委员会），对健康医疗数据安全工作全面负责，讨论决定健康医疗数据安全重大事项：
   1) 委员会应包含组织高层管理人员和各业务口负责人等；
   2) 委员会应涵盖信息安全、伦理、法律、统计、审计、保密等相关专业人员；
   3) 委员会负责人应由组织最高负责人担任；
   4) 委员会并不一定要重新建立，可依托伦理委员会、院务会等；
   5) 委员会应协调配置健康医疗数据安全工作必要的人力、物力、资金等资源，例如基于权限分离的原则，配备安全管理员、安全审计员、系统管理员等；
   6) 委员会负责健康医疗数据安全策略、风险评估方案、合规评估方案、风险处置方案和应急处置方案的审核；
   7) 委员会负责数据安全相关规章制度的审核；
   8) 委员会负责数据使用审批流程的确认；
   9) 委员会负责去标识化策略、流程的审核；
   10) 委员会每月至少召开一次工作会议。
b) 建立健康医疗数据安全工作办公室，指定专人（数据安全官）负责健康医疗数据安全日常工作：
   1) 负责落实执行健康医疗数据安全委员会的各项决定，并向委员会报告工作；
   2) 负责制定健康医疗数据安全策略、风险评估方案、合规评估方案、风险处置方案和应急处置方案；
   3) 负责建立数据安全相关规章制度；
   4) 负责制定数据使用审批流程，以及去标识化策略和流程；
   5) 梳理业务流程及涉及的健康医疗信息系统和数据，并进行安全风险分析和合规分析，提出健康医疗数据安全工作建议；
   6) 形成并管理好元数据结构，形成符合业务流程的数据和系统供应链结构；
   7) 负责人员的数据安全教育与培训，确保相关人员具备相应数据安全能力；
   8) 至少每年对健康医疗数据安全工作进行全面自查，并作出整改建议；
   9) 就健康医疗数据使用情况进行审计，并适时调整改进安全措施；
   10) 监测预警健康医疗数据安全状态，并适时调整改进安全措施。

10.2 规划

规划阶段主要工作如下，各项工作应形成相应文档记录。

a) 界定健康医疗数据安全工作范围；
b) 建立健康医疗数据安全策略并通告全组织；
c) 建立数据安全相关规章制度并通告全组织；
d) 建立健康医疗数据安全风险评估方案和合规评估方案；
e) 梳理健康医疗数据相关业务及涉及的系统和数据；
f) 识别健康医疗数据安全风险并评估影响
g) 识别健康医疗数据安全合规风险点并评估影响；
h) 针对风险建立风险处置方案；涉及数据使用披露的，应按照第7章使用披露指南处置；涉及网络和系统安全的，应按照GB/T 22239—AAAA处置；涉及基础安全和数据服务安全的，应按照GB/T 35274—2017处置；涉及云计算安全的，应按照GB/T 31168—2014处置；
i) 评审并通过风险处置方案；
j) 建立数据安全应急处置方案。

10.3 实施

实施阶段主要工作如下，各项工作应形成相应文档记录。

a) 健康医疗数据使用和披露过程中，各个环节需严格执行既定数据安全相关规章制度、安全策略和流程；
b) 实施风险处置方案，包括实施选定的安全措施；
c) 配备适当的资源，包括人力、物力、资金，支撑安全工作开展；
d) 开展必要的信息安全教育和培训；
e) 对开展的信息安全工作和投入信息安全工作的各项资源实施有效的管控；
f) 针对信息安全事件采取有效应对措施。

10.4 检查

检查阶段主要工作如下，各项工作应形成相应文档记录。

a) 监控健康医疗数据相关工作过程，包括实施选定的安全措施的过程；
b) 定期评审风险处置方案实施的有效性，包括评估实施相应措施后剩余风险的可接受程度等；
c) 定期检查健康医疗数据使用披露是否参照第7章使用披露指南进行；
d) 定期检查是否参照第9章进行了安全技术工作和去标识化工作；
e) 检查过程纳入监管；
f) 根据情况实施自查，或是请第三方检查机构进行检查。

10.5 改进

改进阶段主要工作如下，各项工作应形成相应文档记录。

a) 针对监控或检查结果改进安全措施，包括采取预防性措施，或是调整可能影响健康医疗数据安全的业务活动内容；
b) 建立整改计划，并按计划实施。

10.6 应急处置

a) 建立应急预案，包括启动应急预案的条件、应急处理流程、系统恢复流程、事件报告流程、事后教育和培训等内容。应对网络安全应急预案定期进行评估修订，每年至少组织1次应急演练；

b） 应指定专门数据安全应急支撑队伍、专家队伍，保障安全事件得到及时有效处置；
c） 应制定灾难恢复计划，确保健康医疗信息系统能及时从网络安全事件中恢复，并建立安全事件追溯机制；
d） 在数据安全事件发生后，应按应急预案进行处置；事件处置完成后及时按规定向安全保护工作部门书面报告事件情况，内容应至少包括：事件描述、原因和影响分析、处置方式等信息；
e） 应根据检测评估、监测预警中发现的安全问题及处置结果开展综合评估，必要时重新开展风险识别，并更新安全策略。

控制者应建立的数据使用管理办法参见附录C示例，数据申请审批用表格参见附录D示例，控制者和处理者（使用者）签署的数据处理（使用）协议模板参见附录E，控制者自查使用表格参见附录F示例。

11 典型场景数据安全

11.1 互联互通数据安全

11.1.1 概述

通过对各医疗机构组织建设，以电子病历、电子健康档案和区域卫生信息平台为核心的医疗机构信息化项目中应用的医院信息平台实现医院之间数据的互联互通和信息共享，实现跨机构、跨地域健康诊疗信息交互共享和医疗服务协同。

互联互通数据安全综合考虑了《“健康中国2030”规划纲要》提出的：建立专业公共卫生机构、综合和专科医院、基层医疗卫生机构“三位一体”的重大疾病防控机制，建立信息共享、互联互通机制，推进慢性病防、治、管整体融合发展，实现医防结合。建立不同层级、不同类别、不同举办主体医疗卫生机构间目标明确、权责清晰的分工协作机制，不断完善服务网络、运行机制和激励机制，基层普遍具备居民健康守门人的能力。推进基于区域人口健康信息平台的医疗健康大数据开放共享、深度挖掘和广泛应用。消除数据壁垒，建立跨部门跨领域密切配合、统一归口的健康医疗数据共享机制，实现公共卫生、计划生育、医疗服务、医疗保障、药品供应、综合管理等应用信息系统数据采集、集成共享和业务协同。参照中华人民共和国国家卫生和计划生育委员会颁布的WS/T 448—2013《基于居民健康档案的区域卫生信息平台技术规范》、WS/T 447—2014《基于电子病历的医院信息平台技术规范》、WS 537—2017《居民健康卡数据集》、WS 445（所有部分）《电子病历基本数据集》、WS 363（所有部分）《卫生信息数据元目录》、WS 364（所有部分）《卫生信息数据元值域代码等互联互通建设标准》，参考了《电子健康档案向个人开放建设指导方案》、《全国医院信息化建设标准与规范》、《互联互通服务管理规范》等互联网诊疗行为要求。

11.1.2 涉及的相关方

本场景下的相关方包括区域卫生信息平台、居民个人、医联体、卫生行政主管部门等，如表6所示。

表6 互联互通数据相关方

相关方	数据角色	具体用户	涉及的数据	数据使用示例	备注
居民个人	主体	患者、健康个人	个人健康医疗数据、个人电子病历数据	数据调阅、数据授权 调阅临床检验检查结果最终修正报告	获取医疗卫生服务
社区医院	控制者	医生	个人健康医疗数据、个人电子	1、社区医院对患者进行慢性病管理服务，定期监测血糖指标	申请转出患者，查阅综合医院检验结果以及患者既往病史，就医诊断治疗等

			病历数据、初步诊断医嘱信息	等，并将健康数据上传区域卫生医疗平台 2、患者突发痰血、胸闷等症状到社区医院就诊 3、社区医生开具痰样或血细胞计数样品检验查单，并采集痰样或血细胞样品，通过区域协同物流体系将单据和样本送到综合医院做痰样或血细胞计数样品化验检查 4、社区医生接收综合医院出具的痰样或血细胞计数样品临床检验结果最终修正报告或通过区域卫生医疗平台调阅共享临床检验结果最终修正报告，初步诊断患病结果信息 5、将既往诊断治疗数据和健康数据上传区域卫生医疗平台 6、办理转诊申请、重新接收回转康复患者，健康跟踪随访，对综合医院电子病历数据调阅	社区医生进行病情诊断需要综合医院专业化临床检验数据支撑
综合医院	控制者	主治医生	个人健康医疗数据、个人电子病历数据、诊断医嘱信息、临床检验结果认证报告	1、转诊接收 2、经患者授权，调阅共享个人健康医疗数据、个人电子病历数据、初步诊断患病结果信息、调阅痰样或血细胞计数样品临床检验结果最终修正报告等信息 3、统计患者近几个月的血糖监测指标检验结果数据，为患者调整治疗方案或在院内开具新的尿样化验检查 4、调阅尿样初步检验结果报告，形成诊断医嘱信息 5、调阅尿样临床检验结果最终修正报告 6、形成最终诊断医嘱信息 7、回转社区医院继续康复	接收转入患者，查阅社区医院检验结果以及患者既往病史，就医诊断治疗等
		住院医师	个人健康医疗数据、个人电子病历数据	仅可调阅普通病种资料及概要级特殊病种资料	
		主任医师	个人健康医疗数据、个人电子病历数据、诊断	可调阅普通病种资料及详细级特殊病种资料	

			医嘱信息、临床检验结果认证报告		
		临床检验结果报告作者	临床检验结果初步报告	初步检验报告结果	临床检验结果报告的作者。作者可以是自然人（例如实验室医生）或仪器（例如检验信息系统或自动报告设备）。一份检验结果报告可以有多个作者
		临床检验医生的认证	临床检验结果认证报告	认证检验报告结果	临床检验结果初步报告需要临床检验医生的认证，完成对报告数值的确认结果
		临床检验结果报告审核者	临床检验结果认证报告	检验认证报告审核	临床检验结果报告的审核者审核报告内容，但不具有对其审核结果的法定效力
		临床检验结果报告法定审核者	临床检验结果最终修正报告	1、临床检验结果最终修正报告发送通知给主治医生 2、临床检验结果最终修正报告上传到区域卫生医疗平台	临床检验结果报告的法定审核者审核报告内容，并具有对其审核结果的法定效力，例如实验室负责人
卫生行政管理机构	使用者		个人健康医疗数据、个人电子病历数据		质量控制和质量保证目的

11.1.3 涉及的数据

a) 医疗应用数据中的电子病历数据，包括“病历概要、门（急）诊病历、门(急)诊处方、检查检验记录、一般治疗处置记录基本数据集、治疗处置-助产记录、护理-护理操作记录、护理-护理评估与计划、知情告知信息、住院病案首页、入院记录、住院医嘱基本数据集、转诊(院)记录基本数据集、医疗机构基本信息数据集、出院小结基本数据集”等；

b) 健康状况数据中的电子健康档案数据，包括城乡居民健康档案基本数据集(个人基本信息、健康体检信息、妇女保健、疾病管理、医疗服务)、儿童保健基本数据集、疾病控制（接种、传染病、职业病、食源性疾病）基本数据集等。

c) 临床检验结果最终报告,包括血库检查、细胞标志物检查、化学检查、血液凝固检查、治疗性药物监测检查、生育能力检查、血液学检查、人类白细胞抗原检查、微生物学检查、血清学检查、毒理学检查、尿液分析检查、血气检查、细胞计数＋分类检查、微生物敏感性试验、分子病理学检查、实验室检查、刺激耐受型化学检查数据集等。

d) 组学研究中的公开数据或访问控制数据，包括组学相关数据库中的样本信息、DNA/RNA/蛋白质序列信息、注释信息、功能分析测定数据、特异位点分析、质谱分析结果、家族谱系遗传分析报告等。

11.1.4 重点安全措施

11.1.4.1 传输安全

a) 医院的医护人员、卫生机构管理人员、医院间联合体、医疗第三方服务机构人员等对特殊数据访问提供警示功能，并能对患者去标识化处理，采用替换、重排、加密、截断或掩码等去标识化技术对患者信息进行去标识化处理，确保在信息平台中及提供正常医疗服务以外的（例如医疗保险等）传递中使用的资料不向非授权用户透露患者的身份信息及其他敏感信息。
b) 医院的医护人员、卫生机构管理人员、医院间联合体内部信息共享交换系统应提供数据传输加密处理和隐私保护功能，通过加密等方式实施个人健康医疗数据在传输过程中的保密性控制。例如：医嘱改变日志、医嘱执行单打印记录、护士执行记录、门诊医生排班信息修录、电子病历新建、保存、打印、修改患者基本信息等。
c) 确保数据的完整性、有效性和正确性。信息共享交换后确定数据被正确、完整地导入到数据库中，检查缺失数据，确保数据在传输过程中完整性不受到破坏。

11.1.4.2 存储安全

a) 医院的医护人员、卫生机构管理人员、医院间联合体调阅数据库和应用系统文件时，存储的患者医疗敏感信息（例如身份信息、银行卡号等）应加密存储。医院间独立运行，实现各个医院数据互联互通，通过数据交换并统一实时存储到数据中心，包括敏感信息、加解密文件和其他数据块。
b) 有数据库和应用系统各层级的审计功能；
c) 有数据备份和恢复功能。

11.1.4.3 使用安全

11.1.4.3.1 隐私保护

实现患者健康诊疗档案调阅是互联互通最重要的目的，在诊疗场景下，医生调阅应注意保护医疗信息隐私安全。

11.1.4.3.2 数据分级

医生调阅场景下，可分为默认级、告知级、授权级，分别对应6.3中的第2级、第3级、第4级。默认级资料，例如检验检查名称、就诊医院、就诊科室等。告知级资料，例如检验检查报告、手术记录、出院小结等小结报告类资料。授权级资料，例如住院详细病历等。此外，涉及特殊病种、特殊身份的资料均需授权或告知。

11.1.4.3.3 角色定义

医生按职能分为诊疗医生、本科室非诊疗组医生、其他科室医生等，按职称分为住院医师、主治医师、主任医师等，不同角色的调阅权限不同，角色定义明晰，方可进行下一步的权限分配。

原则上，应按所在科室、职称、诊疗组来定义角色类型。

a） 科室即不同诊疗科室，按照医院科室划分，例如消化科、心脏外科。
b） 职称表征医生的专业性及上下级关系，例如住院医师、主治医师、主任医师。
c） 诊疗组即科室内部的诊疗组划分，视医院科室的具体划分而定，不同诊疗组之间的患者管辖相对独立，例如普外科内部分为胃肠诊疗组、肝胆胰诊疗组等，若科室内部未划分则无需定义。

医院需向汇聚中心上传科室组织架构情况（上下级关系及诊疗组），形成权限组。权限组的调整可下放到科室主任，上级医生可动态调配下级医生的诊疗组归属（考虑到诊疗组可能变动频繁，不增加医生工作负担），医院医务科负责日常审计。当人事状态或诊疗状态发生变更时，角色应随之更新。

11.1.4.3.4 权限分配

将数据按分级、颗粒度标注。

a） 标注数据的分级，即定义标识符、特殊病种、特殊就诊身份，以供后期与相应角色的权限匹配。
   1） 标识符：例如：姓名；身份证/驾照等证件号；电话号码、传真、电子邮件；医疗保险号、病历档案号、账户；生物识别（指纹、视网膜、声音、基因等）；照片；爱好、信仰等。
   2） 特殊病种：性生殖相关疾病、传染性疾病、心理疾病、恶性肿瘤、遗传性疾病、肛门疾病、罕见病、其他不治之症等8类疾病。
   3） 特殊身份：婴幼儿、孕产妇、恶性肿瘤患者等。
b） 标注特殊病种相关数据的颗粒度，不同详细程度资料的隐私级别不同，颗粒度分为以下三类。
   1） 概要级资料：例如检验检查名称、就诊医院、就诊科室等。
   2） 摘要级资料：例如检验检查报告、手术小结、住院小结、用药情况等小结报告类资料。
   3） 详细级资料：例如住院详细病历等。
c） 将医生的科室、职称、诊疗组与数据分级、颗粒度匹配。
   1） 对于普通病种的资料，权限范围内医生均可调阅。
   2） 对于特殊病种的资料，不同职称医生的权限不同。
   3） 对于传染性疾病，考虑保护医务人员的原则，默认向接诊医护人员开放。
   4） 每个医生仅可调阅自身管辖范围内患者的数据，上级医师可查看下级医师管辖范围内的患者数据。

权限分配示例如表7所示，同一医生满足多种角色时，其权限取并集。

表7 角色权限示例表

角色	权限
科室医生	仅可调阅本科室患者数据
住院医师	仅可调阅普通病种资料及概要级特殊病种资料
主治医师	仅可调阅普通病种资料及摘要级特殊病种资料
主任医师	可调阅普通病种资料及详细级特殊病种资料
诊疗组	仅可调阅本诊疗组管辖范围内患者资料，不可调阅本科室其他诊疗组内患者资料

11.1.4.3.5 用户登录

调阅时需进行身份鉴别，方式包括账号口令、基于数字证书的身份认证、生物特征（例如人脸、指纹等）识别认证等多因素结合的认证方式。需限制访问时间、地点，非院内IP调阅、非工作时间调阅为异常调阅。调阅后无动作一定时间（例如10分钟）后帐号自动登出，屏幕自动睡眠。

11.1.4.3.6 数据调阅

数据调阅时，应考虑患者知情同意。调阅系统需具备异常行为感知能力，建立监控系统，达到能够追踪异常源头的效果，用来追踪完整访问轨迹。报警方式包括提供现场报警、手机短信、邮件等方式，异常行为达到一定级别后能够触发权限锁定功能。报警内容包括异常调阅用户的IP、时间、账号、访问内容，并能够进行自动阻断。同时制定应急预案等。重点关注处理结果和处理率。调阅日志保存时间应不少于6个月，定期审核调阅日志，并对敏感数据及特殊身份患者的调阅记录进行审计。

11.2 远程医疗数据安全

11.2.1 概述

远程医疗是一方医疗机构（邀请方）邀请其他医疗机构（受邀方），以提升医疗服务为目的，运用通讯、计算机及网络技术为医疗机构诊疗患者提供技术支持的医疗活动。远程医疗服务一般由卫健委搭

建远程医疗信息资源中心，为受邀方和邀请方提高统一业务平台支撑具体远程医疗应用，同时邀请方和受邀方通过专线、MPLS VPN、Internet、3G/4G、卫星等多种手段接入远程医疗信息资源中心。

远程医疗数据安全综合考虑《“健康中国2030”规划纲要》提出的“远程医疗覆盖省市县乡四级医疗远程医疗卫生机构，全面实现人口健康信息规范管理和使用，满足个性化和精准化医疗的需求”的建设目标，参照国家卫生健康委员会颁布的WS/T 545—2017《远程医疗信息系统技术规范》、WS/T 546—2017《远程医疗信息系统与统一通信平台交互规范》、《远程医疗信息系统建设技术指南》等远程医疗建设标准，参考了《互联网诊疗管理办法》、《互联网诊疗管理办法》、《远程医疗服务管理规范》等互联网诊疗行为要求。

11.2.2 涉及的相关方

远程医疗涉及的相关方包括：

a) 主体：参与远程医疗服务的患者本人；

b) 控制者：受邀方医院、邀请方医院、提供远程医疗服务医院的直属卫健委（简称卫健委）；

c) 处理者：包括但不限于远程医疗信息资源中心运营方、网络运营商。

11.2.3 涉及的数据

远程医疗中涉及的控制者所涉及的数据内容如下所示：

a) 邀请方涉及的数据如表8所示；

表8 远程医疗邀请方涉及的数据

数据类型	数据内容
个人属性数据	1)个人身份信息，包括姓名、身份证、工作证、居住证、社保卡、可识别个人的影像图像等； 2)个人通讯信息，包括个人电话号码、邮箱、账号及关联信息等； 3)个人生物识别信息，包括基因、指纹、声纹、掌纹、耳廓、虹膜、面部特征等。
健康状况数据	主述、现病史、既往病史、体格检查（体征）、社会史、家族史、症状、健康体检数据、可穿戴设备采集的健康相关信息、生活方式等。
医疗应用数据	医嘱单、检验报告、诊断结果、用药信息、病程记录、诊治记录、用药记录、手术记录、护理记录、住院记录、疾病转归、医疗效果、医患沟通文书、诊疗项目知情同意书等。
医疗支付数据	1)医疗交易信息包括支付信息、消费金额、交易记录等； 2)保险信息包括保险账号、保险状态、保险金额等。

b) 受邀方涉及的数据如表9所示；

表9 远程医疗受邀方涉及的数据

数据类型	数据内容
个人属性数据	个人身份信息，包括姓名、身份证、工作证、居住证、社保卡、可识别个人的影像图像等；
健康状况数据	主述、现病史、既往病史、体格检查（体征）、社会史、家族史、症状、健康体检数据、可穿戴设备采集的健康相关信息、生活方式等。
医疗应用数据	医嘱单、检验报告、诊断结果、用药信息、病程记录、诊治记录、用药记录、手术记录、护理记录、住院记录、疾病转归、医疗效果、医患沟通文书、诊疗项目知情同意书等。

c) 卫健委涉及的数据如表10所示。

表10 远程医疗中卫健委涉及的数据

数据类型	数据内容
个人属性数据	1)人口统计信息，包括姓名、年龄、性别、民族、国籍、职业、住址、工作单位、家庭成员信息、联系人信息、收入等； 2)个人身份信息，包括姓名、身份证、工作证、居住证、社保卡、可识别个人的影像图像等；

	3)个人通讯信息，包括个人电话号码、邮箱、账号及关联信息等； 4)个人生物识别信息，包括基因、指纹、声纹、掌纹、耳廓、虹膜、面部特征等。
健康状况数据	主述、现病史、既往病史、体格检查（体征）、、社会史、家族史、症状、健康体检数据、可穿戴设备采集的健康相关信息、生活方式等。
医疗应用数据	医嘱单、检验报告、诊断结果、用药信息、病程记录、诊治记录、用药记录、手术记录、护理记录、住院记录、疾病转归、医疗效果、医患沟通文书、诊疗项目知情同意书等。
医疗支付数据	1)医疗交易信息包括支付信息、消费金额、交易记录等；
卫生资源数据	邀请方（远程医疗会诊申请量、转诊量、预约量、远程诊断申请量、申请科室申请量及所占比重、申请医生人数及申请量等）、受邀方（远程医疗服务量数据、专家资源数据、转诊量、医院诊疗数据分析）
公共卫生数据	远程医疗医院需求趋势信息、远程医疗消费者需求趋势信息、远程医疗消费者需求区域信息、需求区域人口信息、需求经济性信息

11.2.4 重点安全措施

11.2.4.1 隐私保护

a) 医疗机构应当根据患者的病情和意愿组织远程医疗服务，并向患者说明远程医疗服务内容、费用等情况，且征得患者书面同意，签署远程医疗服务知情同意书。在一些特殊情况下，例如患者年幼、精神病患者、丧失意识等，是无民事行为能力人或限制民事行为能力人，此时需要其监护人或者近亲属的书面同意。
b) 邀请方的医生有权利在遵循伤害最小化原则的前提下，可自主决定应采集哪些个人健康医疗数据并与受邀方讨论内容。
c) 邀请方的医生对患者病情已有初步判断，仅就患者的某些症状、体征等无标识数据与受邀方进行讨论，并没有泄露患者的个人信息及隐私，在这种情况下受邀方是作为一种被咨询的对象，也没有对患者产生影响，近端医院可以不对患者进行告知。
d) 在沟通过程中，邀请方向受邀方出示了患者全部的个人信息、数据检查指标、病历及隐私部位检查的图片视频资料，此种情况应向患者予以说明，并征得患者同意。
e) 远程医疗服务，例如远程会诊、远程教育等活动，内容的公开程度须严格按照会诊医师、主讲人员、患者等主体的要求确定使用范围。患者信息的公开应在法律允许的范围内，或征得个人同意。
f) 远程医疗设备、平台是顺利开展远程医疗的保障，没有这些保障，医生的专业知识就不能通过网络传输，“远程”的手段也不复存在，所以处理者应具备所需信息的采集和传输的权利。院方可提出合同要求，明确处理者采集个人健康医疗数据的范围和义务。

11.2.4.2 接入安全

a) 邀请方：
   1) 应指定用于远程医疗的终端设备，将此类设备标记为高风险设备，并对这些设备进行重点监控。
   2) 应对远程医疗信息系统的计算节点、存储节点、管理节点以及应用组件（例如虚拟桌面应用组件）等，在安装部署时进行安全加固操作
   3) 建立访问白名单，只允许远程诊疗过程中涉及的主机接入远程医疗网络；
   4) 定期对远程诊疗涉及的所有服务器和终端进行病毒扫描和系统漏洞扫描，及时清除病毒，定期更新漏洞，针对已开放的端口存在漏洞的设备需及时修复漏洞；

5) 对远程医疗服务中传输的数据进行监控与审计
6) 专家主动召集多方远程会诊，应提供经过系统验证的账号和密码才能完成，确保合法用户才能开展业务。
7) 设立主持人/主席控制机制，有会诊主导方控制整个会诊过程的秩序，提供身份验证机制，如果其他会诊参与方存在身份验证不通过的情况，不能对会议过程进行控制。

b) 受邀方：
1) 应指定用于远程医疗的终端设备，将此类设备标记为高风险设备，并对这些设备进行重点监控。
2) 应对远程医疗信息系统的计算节点、存储节点、管理节点以及应用组件（例如虚拟桌面应用组件）等，在安装部署时进行安全加固操作
3) 建立访问白名单，只允许远程诊疗过程中涉及的主机接入远程医疗网络；
4) 定期对远程诊疗涉及的所有服务器和终端进行病毒扫描和系统漏洞扫描，及时清除病毒，定期更新漏洞，针对已开放的端口存在漏洞的设备需及时修复漏洞；
5) 对远程医疗服务中接收的数据进行数据安全性校验。

c) 卫健委：
1) 在接收前对邀请方与受邀方在远程诊疗网络中传输的流量进行病毒扫描和过滤；
2) 对接入的医疗机构进行身份认证，确保各方的身份真实、可靠；
3) 远程医疗信息系统数据中心的出口采取防DDoS攻击措施，对流量采用实时检测和清洗的方式，能够有效防御针对web、视频等远程医疗业务系统的应用DDoS攻击。

11.2.4.3 传输安全

a) 邀请方：
1) 在受邀方医院与卫健委进行个人健康医疗数据数据传输过程中应采用校验技术或密码技术保证数据的保密性、完整性，加密算法的选择应考虑应用场景、传输方式、数据规模、效率要求等，同时实现多种移动终端设备安全、便捷的远程数据传输。
2) 通过Internet接入远程医疗网络，应保证关键数据在传输过程中不被监听或者篡改。数据传输应采用IPSec VPN/SSL VPN等加密技术传输。

b) 卫健委：
1) 数据传输过程中应采用校验技术或密码技术保证数据的保密性、完整性，加密算法的选择应考虑应用场景、传输方式、数据规模、效率要求等，同时实现多种移动终端设备安全、便捷的远程数据传输。
2) 通过Internet接入远程医疗网络，应保证关键数据在传输过程中不被监听或者篡改。数据传输应采用IPSec VPN/SSL VPN等加密技术传输。
3) 应能够检测到虚拟机镜像文件、系统管理数据、鉴别信息和重要业务数据在传输过程中完整性受到破坏，并在检测到完整性错误时采取必要的恢复措施。

11.2.4.4 存储安全

卫健委：

a) 应采用碎片化分布式离散存储技术保存医疗信息资源，本地应有大于2份的数据副本，数据应强制分片后存储于不同机架上
b) 参照6.2章节内容将数据进行分类，参照6.3章节内容对数据进行定级，不同级别的数据建立不同的存储区域并创建数据存储区域隔离，对不同的存储区域采用不同的防护措施。
c) 对存储远程诊疗数据的数据库进行风险扫描和状态监控；

d) 数据的大批量处理，例如数据查询、数据分析，应提供匿名化处理功能，模糊化或隐藏敏感信息来保护隐私。

11.2.4.5 应用安全

卫健委：

a) 对登录用户进行身份鉴别，并对登录用户的操作行为进行审计，防止通过网页爬虫、非法登录等恶意行为盗取远程诊疗过程中的患者数据；
b) 应采取防护手段保证向会诊中心上传或下载会诊中大量的患者影像文件所使用的服务安全。
c) 防止授权用户在登录系统后对患者医疗健康数据进行非法下载、转卖；
d) 对应用进行渗透测试，防止web攻击造成的数据泄露等问题。

11.2.4.6 运维安全

卫健委：

a) 建立系统操作管理规范，包括但不限于操作数据库目的、操作人员、操作数据库时间、操作数据库设备、操作全程记录；
b) 建立系统维护管理规范，包括但不限于操作系统加固、数据库加固、安全补丁更新的时间，修复的内容、操作人员等。

11.2.4.7 使用安全

卫健委：

a) 对敏感数据进行去标识化处理。

11.3 二次利用数据安全

11.3.1 概述

适用于第三方（政府部门、科研人员、企业公司等）出于数据二次利用的非营利性目的申请健康医疗数据，涉及数据量大，无法联系主体或联系主体成本过高的情况。用于医疗、医疗费用支付等为患者本人服务或其他法律法规规定的数据使用情况不在此范围。

二次利用数据安全综合考虑国务院印发的《关于促进和规范健康医疗大数据应用发展的指导意见》中提出的“鼓励基于区域健康信息平台的健康医疗大数据开放共享，将健康医疗大数据应用共享发展纳入国家大数据战略布局”方针路线，参照2018年国务院印发的《科学数据管理办法》、中国科学院印发《中国科学院科学数据管理与开放共享办法（试行）》、贵阳市人大常务委员会通过《贵阳市政府数据共享开放条例》等数据开放共享条例。

11.3.2 涉及的相关方

数据汇聚中心（医疗机构、区域卫生信息平台、医联体、学术平台等）为控制者，第三方相关人员为使用者。

11.3.3 涉及的数据

汇聚中心数据平台所集中的数据，包括基本人口学数据、病历数据、健康档案数据、基因组等生物组学数据、医保支付数据以及费用数据等。

11.3.4 重点安全措施

11.3.4.1 数据准备

控制者应明确数据资源目录，面向申请者提供数据描述。在一定范围内展示可供二次利用的数据资源及申请信息，包括数据信息（变量、样本量、年份）、申请条件与范围、数据清洗处理成本、数据使用要求与责任，并提供少量样本数据或修饰后数据下载。对于生物组学数据，根据组学类型的不同，制作不同的数据包。

控制者应进行数据分类分级，并标签化。可以按隐私级别分为三大类，包括无标识数据集、受限制数据集以及可标识数据集，分别对应6.3的第2级、第3级、第4级。无标识数据集主要是汇总概要级的信息，例如年度某疾病的统计数等群体数据；受限制数据集涉及患者级别的受保护信息，但身份标识符被删除、加密或泛化；可标识数据集则包含患者的身份识别信息，例如部分研究需要使用患者的地址、户籍类型、基因组学数据提供的基因型信息等。对于隐私级别越高的数据集，相应的申请者资质要求、申请流程、审批程序也应更严格。

11.3.4.2 数据申请

控制者应对数据申请者的身份进行限制。如科研目的的使用，限定申请者为研究人员（有一定级别的课题支撑）、在其研究领域有丰富经验和专业知识（有相应职称及高水平论著支撑）、社会信用达到A级等。

对申请渠道进行限制。建议以单位的名义申请，单位应提前做好审核工作，申请者需提供单位审核意见，需单位负责人签字盖章等。

控制者应规范数据使用的目的，仅可用于非营利性目的，包括科学研究、数据创新大赛、人工智能样本训练等。如对于科学研究目的，申请者应当有一定级别的课题立项，且课题符合伦理，申请提取的数据内容应与研究主题紧密相关，满足最少必要原则。控制者有必要对申请人的历史申请记录进行核查，防止数据分批分期泄露。

11.3.4.3 数据审批

控制者应成立数据委员会（或第三方独立审批），审批人员应专业，构成科学。如果组建数据审批委员会，委员会应由医学专家、信息专家、伦理专家、卫生管理专家、公共卫生专家、药学专家、卫生经济学专家、法律专家等构成。建议建立审批专家库，专家按专业随机抽取。制定数据审批委员会章程、数据审批流程，每次审批数据有审核记录，并对敏感数据的审批情况进行审计，定期开会总结审批科学性。

应制定科学、定性或定量的数据申请审批判别指标。例如可从合法正当性、科学研究价值、数据泄漏风险、提供数据成本四方面进行考量，且满足最少必要原则，制定数据审批评分表。合法正当性考量：是否满足相关法规要求；科学研究价值考量：数据本身价值（字段数、记录数、数据量、数据内容、涉及病种等）、数据应用价值（社会效益等）；数据泄漏风险考量：申请者数据保护能力，数据影响人数、涉及病种、患者损失等；提供数据成本考量：提取、清洗、脱敏、传递所耗费的人力物力等。示例如表11所示。

表11 数据审批判别指标示例

维度	**判别指标举例**
合法性、正当性	是否符合相关法规要求
数据申请与数据需求一致性	数据使用中是否会应用所申请的数据，控制超范围申请，保障最少必要的数据需要
数据使用价值	数据本身价值（数据量、涉及病种等）、数据应用价值（社会效益等）
数据泄漏风险	影响人数、涉及病种、患者损失等
提供数据成本	提取、清洗、脱敏、传递所耗费的人力物力等

11.3.4.4 数据脱敏

结合数据申请者需求，对数据进行相应的去标识化工作，完成后进行重标识检测。需要注意实际开展去标识化等具体工作团队的资质和审查。制定保护患者隐私的去标识化规则，例如定义姓名等标识符。需满足最小计数原则，例如去标识化后满足相同描述的人数不少于11，如果A医院本年度诊断为宫颈癌的患者仅10名，计数<11，则“宫颈癌”需泛化。

11.3.4.5 数据传输

不同密级数据的传递方式不同，无标识数据集可采取加密邮件、加密USB或其他可移动设备（仅特定电脑可使用）等方式。受限制数据集和可标识数据集由于涉及患者部分个人信息，可采取数据本地操作、虚拟桌面远程访问（在该系统进行分析，仅审批下载统计分析结果）、数据沙箱等方式。

控制者与申请者需签署数据使用协议及保密协议，约定双方权责、申请者对数据的保护措施或策略、不慎泄露的应急方案、数据使用期限等。

11.3.4.6 数据销毁

申请者在数据使用结束后书面通知控制者，在约定的使用期限后30天内销毁，并提供销毁的书面证明，数据使用衍生结果公开发表需注明数据来源于控制者。控制者对数据销毁情况作核查。

11.4 临床研究数据安全

11.4.1 概述

本指南涉及的临床研究指以患者及相应群体为研究对象，由医疗机构、学术研究机构和/或医疗健康相关企业发起的针对人类以确认药物、医疗器械、生物制品、体外诊断试剂、临床信息系统、诊断和治疗的安全性和有效性为目的的研究。临床研究可以是医疗机构临床医生发起的科研项目，政府资助的科研项目，科研机构发起的以社会公共利益为目的的医学科学研究，或者涉及公共卫生安全的临床科学研究，也可以是医疗健康相关企业发起的以科学或商业为目的的临床研究。临床研究一般是在学术性的医学中心、附属的研究机构或者医疗科研机构进行，其过程主要包括临床试验的方案设计、组织实施、监查、核查、检查，以及数据的采集、记录、统计、分析总结和报告等。

临床研究主要包括以下类型：

a） 按临床数据获取方法区分：回顾性临床研究和前瞻性临床研究；

b） 按研究目的区分：临床基础研究、临床应用研究和临床路径研究；

c） 按产品获准上市与否区分：产品上市前研究和产品上市后研究。

以产品上市获批为目的的临床试验的数据安全，请参照相关主管部门规定，不属于本指南范畴。

在回顾性临床研究中，学术研究机构或健康医疗相关企业以新产品开发和验证为目的，或验证现有产品的临床反应，或以优化现有产品为目的，从医疗机构获取既往数据进行临床研究。

在前瞻性临床研究中，以新产品、新诊疗方案开发为目的，根据主管部门要求对新产品、新诊疗方案的安全性和有效性进行验证，健康医疗相关企业与医疗机构合作采集数据进行临床研究。

临床试验是用于确认产品安全性和有效性的试验。

临床路径研究是通过对医疗机构临床路径的调研、分析和优化，以达到提高医疗服务水平、控制医疗成本、规范医疗行为、提高医患满意度的目的。

产品上市后研究是科研机构或健康医疗相关企业，根据主管部门要求对产品的安全性和有效性进行验证，获取医疗机构使用产品产生的数据，对产品实际质量和有效性进行研究。

临床研究数据安全综合考虑了临床研究主要的应用场景，参照国家卫生健康委员会颁布的《涉及人的生物医学研究伦理审查办法》、ISO 14155《针对人的医疗器械临床研究-最佳临床实践》，国家药品监督管理局《医疗器械临床涉及指导原则》、《医疗器械临床试验质量管理规范》、 《临床试验的数据采集技术指导规则》，同时参考了国家标准GB/T 35273—2017《信息安全技术　个人信息安全规范》。

11.4.2 涉及的相关方

临床研究主要涉及的相关方有：

a) 申办者：指负责临床研究的发起、管理和提供临床研究财务支持的个人、组织或者机构。

b) 临床研究机构：指具有资质的临床试验医疗机构。

c) 研究者：是指在临床研究机构中负责实施临床试验的人。如果临床研究机构是由一组人员实施试验的，则研究者是指该组的负责人，也称主要研究者，在多中心临床研究中负责协调参加各中心研究者工作的一名研究者。

d) 受试者：指参加临床研究，并作为研究用药品或临床研究的接受者，包括患者、健康受试者。

e) 伦理委员会：由医学专业人员、法律专家及非医务人员组成的独立组织，其职责为核查临床试验方案及附件是否合乎道德，并为之提供公众保证，确保受试者的安全、健康和权益受到保护。该委员会的组成和一切活动不应受临床试验组织和实施者的干扰或影响。

f) 监查员：由申办者任命并对申办者负责的具备相关知识的人员，其任务是监查和报告试验的进行情况和核实数据。

g) 核查员：是指受申办者委托对临床试验项目进行核查的人员。

其中，受试者、医护人员可能扮演主体的角色，临床研究机构、申办者（健康医疗相关企业、学术研究机构）可能扮演控制者的角色。

对回顾性临床研究而言，申办者（例如：医疗机构、学术研究机构或健康医疗相关企业）根据需要，从临床研究机构（医疗机构）获得既往数据从事医药/医疗产品和诊疗方案研究。在这个过程中，临床研究机构、申办者共同承担控制者的角色，受试者是主体。

在前瞻性临床研究过程中，申办者（例如：医疗机构、学术研究机构或健康医疗相关企业）和临床试验机构（例如：医疗机构）合作，根据具体研究目的，确认需要采集的数据类型，对采集的受试者（患者）医疗数据进行研究。在这个过程中申办者和医疗机构共同承担控制者的角色，患者是主体。

在临床路径研究中，学术研究机构或健康医疗相关企业和医疗机构及相关医护人员合作，收集了解医疗机构的临床路径及医护人员对临床路径的认识。在这个过程中，学术研究机构或健康医疗相关企业扮演控制者的角色，相关医护人员是主体。如果在该研究中，医疗机构是发起者，医疗机构也承担控制者的角色。

在产品上市后研究中，申办者（学术研究机构或健康医疗相关企业）与临床研究机构（医疗机构）合作，根据研究目的确认需要采集的数据类型，收集相关数据研究产品的质量和治疗/诊断效果。在这个过程中，申办者和医疗机构共同承担控制者的角色，患者是主体。

11.4.3 涉及的数据

临床研究涉及的数据包括但不限于以下临床信息：

a) 基本人口学资料：姓名、性别、血型、生日、单位、住址；个人史 、婚育史、家族史、月经生育史等等基本信息。

b) 检查信息：可分为体检、专科检查(专科疾病的特殊情况，例如外科情况、眼科情况 、妇科情况等)、辅助检查(入院前所做的与本次疾病相关的主要检查及其结果)；具体分为：检查申请号、检查类型名称、检查类型编码、检查项目中文名、检查项目编码、执行科室、检查时间、检查状态、检查设备、检查所见、检查结论等检查信息。

c) 检验信息：检验标本类型、采样部位、检验类型名称、检验项目中文名、检验项目编号、检验结论、检验子项中文名、检验子项编号、检验子项目值、检验子项目单位、检验方法、参考低值、参考高值、参考范围、警戒低值、警戒高值、定性/定量结果、药敏药物中文名、药敏药物英文名、药敏药物敏感度、药敏最低抑菌值、抑菌圈直径等信息。

d) 药品医嘱：长临嘱标识、开单时间、医嘱开始时间、医嘱结束时间、开单科室、开单人、医嘱状态、药品名称、频次、用量、用量单位、天数、用法、剂型、规格、同组标识等。
e) 非药品医嘱：医嘱类别、长临嘱标识、开单时间、开始时间、结束时间、开单科室、开单人、医嘱状态、医嘱中文名、频次、数量、数量单位等。
f) 手术信息：手术名称、手术开始时间、手术结束时间、术前诊断、术中诊断、术后诊断、手术医师、手术助手、麻醉医师、手术切口、麻醉方式、手术经过、术中失血量、术中输血量等。
g) 病理信息：检测方法、取材部位、病理中文名、病理检查日期、检测方法、检测设备、病理标本类型、标本数量、标本部位、标本采集方式、标本状态、病理取材所见、检查所见、病理检查结论、免疫组化结果等。
h) 骨髓穿刺：申请医师、申请号、申请科室、取材部位、形态描述、诊断意见、检验子项目中文名、检验子项目值、检验子项目值单位、参考范围、定性/定量结果、标本类型、采样部位、标本要求、采样时间等。
i) 生命体征：体温、脉搏、呼吸、心率、舒张压、收缩压、血氧饱和度、身高、体重等。
j) 诊断信息：门(急)诊诊断、入院诊断、出院诊断、转科诊断、术前诊断、术中诊断、术后诊断、病理诊断、死亡诊断等。
k) 处方信息：处方编号、处方类别、处方同组标识、医嘱项目类型名称、医嘱频次、医嘱数量、开单人、开单时间、开单科室、医嘱名称、药品商品名、药品通用名、药物类别、次用量、用量单位、总用量、总用量单位、用药途径、药频规格、剂型等。
l) 病历数据：入院记录、出院记录、24小时内入出院记录、24小时内入院死亡记录、首次病程记录、术后首次病程记录、术前讨论、术前小结、手术记录、转科记录、上级医师查房记录、日常病程记录、抢救记录、会诊记录、死亡记录等。
m) 患者报告结局(Outcome)：通过门诊随访、电话随访、互联网随访等手段获取患者症状改善、功能恢复及健康相关的生活质量等情况。
n) 费用信息：治疗费、检查费、CT费、会诊费、病理费、材料费、床位费、磁共振费、放疗费、放射费、核医学费、护理费、化验费、监护费、介入费、冷暖费、麻醉费、配血检费、手术费、手术材料、手术处置、手术设备、西药费、诊查费、中药费、输血费、挂号费、放射材料费、麻醉材料费、血材料费、预约费、测查费、膳食费、造影费、出诊费、输氧费等。

相关主管部门对基因数据的安全有专门规定，所以本指南不涉及基因数据安全。

11.4.4 重点安全措施

11.4.4.1 概述

根据卫健委《涉及人的生物医学研究伦理审查办法》，任何涉及人的医学研究都须得到相应伦理委员会的批准。对于符合免除知情同意的情况，可经过伦理委员会批准后免除知情同意。同时鉴于以新产品、新诊疗方案开发和产品实际质量和有效性验证的目的，在不影响科研目的的前提下，对数据实施去标识化处理。

对于需要追溯到个人的情况，参考相关法律法规和标准，例如卫健委《临床试验数据管理工作技术指南》和GB/T 35273—2017《信息安全技术　个人信息安全规范》等，建立数据保密及患者个人隐私保护制度。

通过合同/协议等形式约定数据使用范围，明确数据保密及隐私保护合同/协议双方的责任和义务。

临床研究数据安全隐私管理包括数据权限控制、个人信息去标识化、数据加密等。面向临床研究和患者服务方面均遵循医疗行业的伦理规范和信息安全等级保护规范，仅提供业务所需最小数据集，同时进行访问审计。

a) 能够对不同权限用户进行权限配置，不同角色不同科室的用户可以查看不同范围的内容，提供业务所需最小数据集。各数据权限拥有不同的数据浏览与检索权限，包括全院层级数据、科室层级数据、所在医疗组层级数据的浏览与检索。
b) 对于病历进行匿名化处理，保护患者隐私与信息安全。开启病历匿名化后，可选择对患者的姓名、年龄、性别、手机号、身份证、电话号码、住址 、家庭成员、职业等隐私信息进行隐藏。
c) 对于数据导出有完整的审批流程并存档。
d) 遵循医疗行业的伦理规范和信息安全等级保护规范，提供业务所需最小数据集，同时进行访问审计。

11.4.4.2 伦理审查和知情同意

在正式研究开始之前，申办者应准备研究计划，叙述研究目的合法性依据，包括：研究内容、目的、涉及的数据类型、数据数量和预期结果，将研究计划报相关医疗机构的伦理委员会审批。涉及人类遗传资源收集的，同时应向有关部门申报批准。

临床研究原则上都需要受试者知情同意。对于研究型医疗机构在患者就诊时可以采用广泛知情同意（Broad Consent）方式，使患者授权其个人健康数据在去标识化前期下用于未来的临床研究中。

对于临床路径研究，由于健康医疗相关企业并不采集涉及人的医学信息，所以不需要获得主体知情同意，也不需要得到伦理委员会批准。

a) 临床研究征得知情同意的例外：
   1) 对于产品上市后研究，以验证产品安全性和有效性为目的，在数据去标识化的前提下，相关申办者不需要获得受试者知情同意；
   2) 申办者出于公共利益开展统计或学术研究所必要，且其对外提供学术研究或描述的结果时，对结果中所包含的个人信息进行去标识化处理的，不需要获得受试者知情同意。
b) 以下情况可以向伦理委员会申请知情同意豁免：
   1) 对于回顾性研究，已无法追溯到患者，或获取受试者知情同意代价太高，在数据去标识化的前提下，可以申请知情同意豁免；
   2) 对于回顾性研究，主体已签署知情同意书，范围包含现有范围，在数据去标识化的前提下，可以申请知情同意豁免。

11.4.4.3 数据分级

科研使用场景下，可分为公用数据集（public use files, PUF）、有限数据集（Limited Data Set Files, LDS）、可识别数据集（Research Identifiable Files,RIF），分别对应6.2中的第1级、第3级、第4级。PUF主要是汇总概要级的数据；LDS涉及患者级别的受保护数据，但身份识别数据被加密或泛化；RIF则包含患者的身份识别数据。隐私级别越高，应对申请者要求越严格，需提交的材料越多，审核部门也越多。

11.4.4.4 数据采集

临床研究数据采集实施的原则：

a) 研究者或其指定的代表在数据收集之前要先确定元数据的格式和内容，并对元数据有必要的描述信息；研究者或其指定的代表需要将所收集的数据内容、用途、共享计划或数据不共享说明提交给监查员；监查员需要确定所收集的健康医疗数据的所有权和责任人，并对其进行收编归档，如碰到人员调动等情况，需要对科研数据的所有权和责任人及时变更。

b） 研究者或其指定的代表需与受试者签署相关协议并说明有关临床试验的详细情况：使受试者了解，参加试验及在试验中的个人资料均属保密；伦理委员会、药品监督管理部门或申办者在工作需要时，按规定可以查阅参加试验的受试者资料等。

c） 数据可以通过多种方式进行接收，例如传真、邮寄、可追踪有保密措施的快递、监查员亲手传递、网络录入或其他电子方式。数据接收过程应有相应文件记录，以确认数据来源和是否已被接收。提交到健康医疗信息系统时应保护受试者识别信息的安全性。数据录入流程应明确该试验的数据录入要求。一般使用的数据录入方式包括：双人双份录入、带手工复查的单人录入或直接采用电子数据采集（EDC）方式。采用EDC方式采集应保证EDC软件设计符合研究要求的安全规范，包含但不限于个人信息去标识化、数据加密等功能。

d） 临床试验受试者的个人隐私应得到充分的保护，对基本人口学资料进行去标识化处理。个人隐私的保护措施在设计数据库时就应在技术层面考虑，在不影响数据的完整性和不违反临床实验质量管理规范（GCP）的条件下尽可能不包括此类受保护医疗信息，例如数据库不应包括受试者的全名，而应以特定代码指代。

11.4.4.5 数据传输

主要涉及临床研究机构和申办者之间的数据传输，应采取以下安全措施保护数据：

a） 确定个人健康医疗数据数据的传输方法，包括但不限于：专线、互联网线路、VPN等链路上，采用TLS、IPSEC等安全传输方式；若采用离线传输方式，例如：光盘、优盘等，数据应加密，加密数据和密钥分开存储，应有数据导入导出和介质交接记录。

b） 确保数据传输的保密性，应采用密码技术保证通信过程中敏感信息或整个数据集不被窃取。

c） 确保数据的完整性、有效性和正确性。在进行数据核查之前，应列出详细的数据核查计划，数据核查包括但不限于以下内容:确定原始数据被正确、完整地导入到数据库中,检查缺失数据，查找并删除重复导入的数据，核对某些特定值的唯一性（例如受试者 ID）。

d） 实施访问控制，按照临床研究电子系统的用户身份及其归属的用户组的身份来允许、限制或禁止其对系统的登录或使用，或对系统中某项信息资源项的访问、输入、修改、浏览能力的技术控制。

11.4.4.6 数据存储

原则上，患者知情同意书和患者代码索引由医疗机构保存，健康医疗相关企业只能获得去标识化后的数据。

a） 建议临床研究申办者在数据存储阶段采取以下安全措施保护数据安全：

1） 如果患者知情同意书和患者代码索引以纸质形式记录,应在物理保存上加锁,由专人负责；如果患者知情同意书和患者代码索引以数字形式记录，数据应加密并建立基于角色的访问控制机制，加密数据和密钥应分别存储；

2） 其他数据应建立基于角色的访问控制机制，推荐使用加密机制，加密数据和密钥应分开存储；

3） 应对数据进行完整性验证，保证数据的完整性及不被篡改；

4） 在研究结束后，应对数据每5年做一次安全和使用审查，如果没有必要继续保存，需对数据进行匿名化或删除，如果匿名化后的数据属于重要数据范畴，按国家相关规定处理。

b） 建议医疗机构在数据存储阶段采取以下安全措施保护数据安全：

1） 通过数字签名等方式实施完整性控制，确保健康医疗数据是准确的、完整的，并为其提供针对非法修改的保护机制；

2) 临床试验所有过程应产生准确和完整的记录，且清晰可读，便于回顾，不仅最后结果需要保存，生成过程的数据（元数据）也需归档，在回顾数据时，能够从最后的结果追溯到原始数据；
3) 中间过程的数据应以合适的方式例如版本升级等形式加以保存，不得覆盖原有过程记录；
4) 应制定数据备份及恢复策略，定期进行数据备份，建立介质存取、验证和转储管理制度，并按介质特性对备份数据进行每年不少于1次的定期恢复的有效性验证；
5) 对于公有云上的临床研究信息共享系统，应采取必要的验证和加密处理，要对临床研究信息共享系统进行访问授权控制，确保数据访问的安全性。应对传输到临床研究信息共享系统的数据进行加密存储，同时应确保临床研究信息共享系统数据的灾备。对于院内私有云存储的数据，要通过网闸、网络隔离等方式，保证院内网络环境与公网环境的隔离，并限制移动存储设备（例如光盘、U盘）的使用，保证院内网络环境与公网环境的隔离。

11.4.4.7 数据使用

a) 利用数据库管理数据的情况，应确保数据管理过程可追溯。数据库锁定是为防止对数据库文档进行无意或未授权的更改，而取消的数据库编辑权限。数据库锁定过程和时间应有明确的文档记录，对于盲法临床试验，数据库锁定后才可以揭盲。如果对数据库锁定和开锁过程进行记录和控制，数据库开锁的流程应至少包括：通知项目团队；定义将更改内容、更改原因以及更改日期；并由主要研究者、数据管理人员和统计分析师等人员共同签署。
b) 第一次的数据录入以及每一次的更改、删除或增加，其稽查轨迹都应保留在临床研究数据库系统中。稽查轨迹应包括更改的日期、时间、更改人、更改原因、更改前数据值、更改后数据值。此稽查轨迹为系统保护，不允许任何人为的修改和编辑。稽查轨迹记录应存档并可查询。
c) 数据应在脱敏的情况下进行使用，应支持患者隐私信息匿名化设置，如患者姓名、家庭地址、身份证号、手机号码、联系人姓名、联系人电话等。
d) 建立数据权限管理机制，包括授权查看、授权使用、可查看的数据、可使用的数据。
e) 临床试验中所有观察结果和发现都应加以核实，以保证数据的可靠性，确保临床试验中各项结论来源于原始数据。在数据处理的每一阶段应采取质量控制，以保证所有数据可靠，处理正确。
f) 多中心试验场景下数据应实施集中管理与分析，并应满足数据传输安全各项条件。
g) 建立基于角色的数据访问控制机制，只有被授权的角色可以访问被授权的数据对象。
h) 数据传输应使用加密技术、身份验证技术和数据完整性校验技术保证数据以安全的方式传输给指定的对象。
i) 应为主要研究者、数据管理员、统计分析师等不同角色的不同人员设置不同的账号且赋予不同的权限。

11.4.4.8 数据发布和共享

研究者在对数据进行发布和共享的时候，应：

a) 对健康医疗数据形成共享说明，包括：数据限制性访问说明、隐私及保密协议说明、科研数据用途说明等；
b) 搭建科研数据共享平台，对不同级别的数据进行评估，确定不同的共享规范和访问控制权限；
c) 对共享和发布的健康医疗数据建立可溯源体系，做到可以分析审计跟踪溯源数据；
d) 对数据的利用、存储、传输、访问控制等要遵守共享说明或相关合同的规定，遵守我国的知识产权法、科研数据共享法等法律法规；
e) 在满足数据安全规范的前提下，研究者要以最大化的共享科研数据为原则。

11.4.4.9 审计管理

a) 审计内容应包括人员审计、管理审计、技术审计（系统、网络、操作、日志审查等）；
b) 任何操作，包括登录、创建、修改和删除记录的行为，都应自动生成带有时间标记的审计记录，包括但不限于修改时间、修改原因、修改内容、修改人及签名等信息，并可供审计；
c) 应制定和部署健康医疗信息系统活动审计政策，重点对于健康医疗数据的访问及操作的合规性进行审计，确定必要的审计控制范围和需要审计的数据及其深度和维度；
d) 应制定适当的标准操作流程，确定异常报告所需的审计跟踪数据和监视程序的类型；
e) 审计记录应安全存储和访问控制，应只允许授权人员能够查看相关记录，保存的内容需反映临床医学研究整个过程。

11.5 健康传感数据安全

11.5.1 概述

健康传感数据是指通过健康传感器采集的，在软件支持下感知、记录、分析，与被采集者健康状况相关的，应用于医疗服务和健康生活的一切数据。

健康传输数据安全综合参考《国务院办公厅关于印发全国医疗卫生服务体系规划纲要（2015-2020年）的通知》工作目标“开展健康中国云服务计划，积极应用移动互联网、物联网、云计算、可穿戴设备等新技术，推动惠及全民的健康信息服务和智慧医疗服务，推动健康大数据的应用，逐步转变服务模式，提高服务能力和管理水平”，参考《信息安全技术 网络安全等级保护要求 物联网安全扩展要求》相关要求。

11.5.2 涉及的相关方

涉及的相关方包括个人、医疗机构、医保机构、商业保险公司、健康服务企业、信息系统服务商等。

a) 主体：佩戴健康传感设备的人员。
b) 控制者：使用健康传感设备采集健康医疗数据的机构包括但不限于医疗机构、医保机构、健康服务企业。
c) 处理者：为控制者提供服务的机构，包括但不限于信息系统服务商。

11.5.3 涉及的数据

健康传感数据管理中涉及的数据如表12所示。

表12 健康传感涉及的数据

数据类型	数据内容
个人属性数据	1)个人身份信息，包括姓名、可识别个人的影像图像等； 2)个人通讯信息，包括个人电话号码、邮箱、账号及关联信息等； 3)个人生物识别信息，包括身高、年龄、体重、性别等。
健康状况数据	监测诊疗数据（血氧饱和度、血压、血糖心率、睡眠）；行为情绪数据（跑步距离、行走轨迹、步数、消耗能量、锻炼时长）；环境数据（紫外线指数、污染指数、温度、湿度、噪声）

11.5.4 重点安全措施

11.5.4.1 隐私保护

a) 使用和披露健康传感数据应征得用户同意；
b) 健康传感数据集成之后应向用户说明应用目的和共享对象。

11.5.4.2 采集安全

a) 健康传感设备应支持用户认证，确保合法的控制和使用健康传感设备，用户认证手段包括但不限于虹膜识别、指纹识别、密码技术。
b) 采集控制措施，用户可选择开启或关闭数据采集和上传的内容。
c) 健康传感设备应支持个人健康数据的存储加密功能。
d) 如果健康传感设备通过网络向终端管理应用传输采集的健康数据，应支持节点认证机制。

11.5.4.3 传输安全

应采用校验技术或密码技术保证个人健康医疗数据在传输过程中的保密性、完整性，加密方法的选择应考虑应用场景、传输方式、数据规模、效率要求等。设备应默认开启数据加密功能。

11.5.4.4 存储安全

a) 采用电子签名及时间戳等技术来保证数据的完整性和可追溯性。
b) 确保数据可用性。制定数据备份及恢复策略，定期进行数据备份，建立介质存取、验证和转储管理制度。通过高性能、可扩展的数据库服务确保各类业务对数据获取服务的性能要求。
c) 建立远程控制措施，一旦设备被窃或丢失，可自行选择删除设备中存储的数据。

11.5.4.5 使用安全

a) 建立数据访问认证和授权机制。建立完善的身份认证以及基于角色的权限控制，严格区分不同用户角色对数据访问的权限。合理、精细的定义角色权限，避免不必要的、超过角色合法职责之外的授权。
b) 对健康传感数据的使用活动进行审计，重点对健康医疗数据的访问及操作的合规性进行审计，确定必要的审计控制范围和需要审计的数据及其深度和维度。应用相应技术手段，保证审计日志的完整性。

11.6 移动应用数据安全

11.6.1 概述

移动应用是指通过网络技术为个人提供的在线健康医疗服务（例如在线问诊、在线处方）或健康医疗数据服务的应用（例如个人电子健康档案）。符合医疗器械定义的应用，由医疗机构使用的用于现场健康医疗服务的应用（例如协助医生采集、使用患者在院内（门、急诊，住院）诊疗信息应用），不在本节范畴之内。

使用目的可能涉及6.1中描述的所有类型，即医疗服务、临床研究、公共管理、决策支持、健康生活、医学教育等。

移动应用数据安全参考GB/T 35273—2017《信息安全技术　个人信息安全规范》。

11.6.2 涉及的相关方

本节所涉及的相关方主要是应用发布者。应用发布者是指与个人签订应用软件使用许可协议的主体，可以是政府机构、医疗机构、医保机构、商业保险公司、科研机构、医药企业、医疗器械厂商、健康服务企业、数据服务企业或其他独立民事主体。

在移动应用的前端主要涉及主体和控制者，在移动应用的后端，主要可能涉及控制者、处理者和使用者。

11.6.3 涉及的数据

涉及的数据从分类角度，包括个人属性数据、健康状况数据、医疗应用数据、医疗支付数据、卫生资源数据以及公共卫生信息。

11.6.4 重点安全措施

11.6.4.1 数据采集

a) 应用发布者应制定隐私政策，参照GB/T 35273—2017《信息安全技术 个人信息安全规范》；
b) 在具体采集个人信息包括个人健康医疗数据时明示所要采集的信息并征得用户同意。

11.6.4.2 访问控制

a) 提供一种在会话级别安全地验证用户的方法（例如，口令，口令短语，PIN，质询短语、基于数字证书的身份认证方法），并且在系统最初建立身份时或者有迹象表明身份可能已被泄露时（例如，多个口令失败）还可利用其他方法或技术进一步验证用户的身份；
b) 访问用户信息仅限于那些需要了解信息以便操作、维护、开发或改进应用程序的授权员工或承包商；
c) 应使用唯一的用户ID来访问应用程序中的所有角色；
d) 使用合适的身份验证方法来验证用户身份；
e) 找回或重置口令时应验证目标用户的身份；
f) 应用程序内的访问应限于该个人特定角色所需的内容；
g) 应对及时提供和取消访问的措施进行记录存档；
h) 远程访问或特权访问应要求双因素身份验证以降低未经授权访问的风险。

11.6.4.3 传输安全

采用校验技术或密码技术保证个人健康医疗数据在传输过程中的保密性、完整性，加密方式的选择应考虑应用场景、传输方式、数据规模、效率要求等。

11.6.4.4 存储安全

a) 提供并使用管理、物理和技术保护措施来保护用户信息免遭未经授权的泄露或访问；
b) 定期备份应用程序数据；
c) 如果使用可移动介质存储健康医疗数据和个人身份可识别信息，则应对存储在介质上的数据进行加密，以防止数据受到未经授权的访问；
d) 存储个人生物识别信息时，应采用技术措施处理后再进行存储，例如仅存储个人生物识别信息的摘要。

11.6.4.5 应用安全

a) 涉及通过界面展示个人属性数据、健康状况数据、医疗应用数据、医疗支付数据等敏感的个人健康医疗数据时，应用发布者应对需展示的数据采取去标识化处理等措施，以降低在展示环节泄露的风险；
b) 与应用程序相关的信息系统应具有防病毒软件和机制，应用程序环境与安全补丁保持同步；
c) 如果任何第三方供应商服务被用作应用程序的一部分，则应对相应的第三方进行信息安全风险评估；
d) 涉及移动支付的，遵守相关数据安全要求。

11.7 患者查询数据安全

11.7.1 概述

患者通过汇聚中心的门户网站，输入相关身份信息，可以查询到自己相关的个人健康医疗数据。平台应做好防止他人冒名查询或批量截取的管控措施。

患者查询数据安全从《基于健康档案的区域卫生信息平台建设指南》提出的“平台建立居民贯穿整个生命周期健康档案，群众可以查询自己的健康资料，从而进行自我医疗管理、制定自我疾病防范及维护自己的健康档案信息”建设目标出发，参考了《网络安全法》、GB/T 35273—2017《信息安全技术　个人信息安全规范》等法规标准要求。

11.7.2 涉及的相关方

数据汇聚中心（医疗机构、区域卫生信息平台、医联体、学术平台等）为控制者，患者个人为主体。

11.7.3 涉及的数据

汇聚中心数据平台所集中的数据，包括基本人口学数据、病历数据、健康档案数据。

11.7.4 重点安全措施

11.7.4.1 身份识别

个人首次注册需关联实名制手机。后通过实名制手机登录，发送手机号验证码。考虑子女代替年老父母等查询信息需要,帐号可绑定子女手机(上传身份证或户口本扫描件即可或由汇聚中心后台认证)。

完成注册后,个人需设置帐号与密码,汇聚中心应对密码复杂度有一定要求,包括定期更改密码等。

11.7.4.2 信息查询

为防止账户假落他人之手，造成个人信息大量泄漏，汇聚中心应对可查询信息进行适当限制。例如HIV、肝炎等敏感检查结果不予显示。默认仅可查询三个月内相关检查检验报告、用药情况等信息。

11.7.4.3 操作权限

汇聚中心应对个人的操作权限有所考量，权限包括另存、复制、打印、下载等。个人进行相应操作时，页面应显示用户需知，例如告知患者下载后数据的信息安全义务在于本人等，提示个人注重信息保护，同时重点语句突出显示（例如标红）。

11.8 商保对接数据安全

11.8.1 概述

购买商业保险的主体，在定点医疗机构就医时，除医保费用报销范围外，涉及其他的医疗费用，且在商业险责任范围内的，经其授权同意，商业保险公司通过与医疗机构建立连接的医疗信息系统，及时掌握主体的就诊治疗情况及发生的费用相关信息，从而根据商业保险公司的核赔规则自动进行支付结算等理赔业务。在医疗机构与商业保险公司建立连接时，应在医疗信息系统对接前、对接中与对接后的三个阶段实施有效的安全措施确保健康医疗数据的安全。

商保对接数据安全综合考虑被保险人发生保单所约定的保险事故，商业保险公司从医疗机构调取健康医疗数据数据，进行核赔这一管理流程；参考了《国家健康医疗大数据标准、安全和服务管理办法（试行）》、《全国医院信息化建设标准与规范》、GB/T 22239—AAAA《信息安全技术　网络安全等级保护基本要求》等管理要求。

11.8.2 涉及的相关方

此场景适用于医疗机构与商业保险公司建立合作，医疗机构的医院信息系统（HIS）等医疗信息系统与商业保险公司的系统双方建立系统对接与数据传输的场景。

此场景涉及的相关方如下：

a) 医疗机构：依法定程序设立的从事疾病诊断、治疗活动的卫生机构，作为控制者；

b) 商业保险公司：销售保险合约、提供风险保障的公司，作为使用者。

11.8.3 涉及的数据

本场景中涉及到的健康医疗数据分为：个人属性数据、健康状况数据、医疗应用数据、医疗支付数据、卫生资源数据，具体内容如表13所示。

表13 商保对接场景所涉及的健康医疗数据

数据类型	具体内容
个人属性数据	可能包括但不限于姓名、性别、证件号、证件类型、出生日期、电话/手机号码、 职业、现住址、婚姻状况等
健康状况数据	可能包括但不限于主诉、现病史、既往史、输血史、过敏史、预防接种史、个人史、家族史、婚姻生育史、生命体征、体格检查结果、辅助检查结果、治疗计划、就诊历史、检查报告、手术信息列表、出院情况、住院医嘱、疾病代码、疾病名称、检验报告等
医疗应用数据	可能包括但不限于： （1）药品及诊疗服务信息 通用名称（主要成分名）、商品名称、剂型、规格、单价、数量、金额医疗目录类型、医疗目录类别、医疗目录类别名称、医疗目录类型名称、自负比例等 （2）医疗服务信息 医疗类别、社保机构 （3）病案首页信息 住院次数、联系人姓名、联系人与本人关系、联系人电话、门急诊诊断（名称+疾病编码）、入院途径、入院时情况、入院科别、入院病室、转科科别、入院诊断（名称+疾病编码、入院后确诊日期、出院日期、出院科别、出院病室、出院诊断（名称+疾病编码）、实际住院天数、出院情况、损伤中毒的外部原因、损伤中毒的外部原因编码、病理疾病编码、病理号、病理诊断、是否手术、输血品种、输血数量、癌症分期、颅脑损伤患者入院后昏迷时间、日常生活能力评定、科主任、主治医师、住院医师等 （4）手术信息 手术名称、麻醉方式等 （5）组学相关信息 基因组、蛋白组、转录组、疾病基因组、药物基因组、代谢组、病源微生物组数据。包括样本、序列、家族遗传分析、特异位点分析结果、功能分析测定结果等
医疗支付数据	可能包括但不限于发票号（业务标识码）、住院号、医保类型、住院起始日期、住院截止日期、住院天数、住院次数-结算单（不区分医院、全年）、合计金额、本年度统筹基金的累计支付、报销比例、缴款日期、支付账户类型、支付账户金额、收费类别代码、收费类别名称、项目收费金额
卫生资源数据	可能包括但不限于医院名称、医院等级、医院类别等

11.8.4 重点安全措施

11.8.4.1 对接前

a) 医疗机构：

1） 评估商业保险公司的资质,针对与商业保险公司进行数据对接的方案进行安全评估；
2） 通过合同/协议等形式约定与商业保险公司针对所披露的健康医疗数据各自承担的安全责任，以保障健康医疗数据的保密性、完整性、抗抵赖性和可用性；
3） 建立衡量合同履行情况和终止合同的流程，定期进行安全评估，建立衡量合同履行情况的标准；
4） 在向商业保险公司披露健康医疗数据前，应确定将用于保护健康医疗数据的传输方法（例如系统接口、传输加密等方式),并明确将用于支持传输安全策略的相关工具和安全技术，同时应明确向商业保险公司披露健康医疗的信息内容与范围,包括健康医疗数据的使用范围、健康医疗数据的种类、健康医疗数据的使用方式、健康医疗数据的使用期限等；
5） 通过合同/协议等形式要求商业保险公司获取主体的明确授权，并基于业务需要的最小化原则进行健康医疗数据的采集和使用；
6） 应要求商业保险公司所属信息系统对接参与人员签署保密协议；
7） 医疗机构在信息系统对接上线前应进行充分的安全测试、安全扫描及评审。

b） 商业保险公司：

1） 应评估医疗机构的资质及级别；
2） 应取得医疗机构相关数据的披露授权，授权内容应包括：获取数据的时间范围、数据的种类或字段、数据使用范围、数据使用方式、数据使用期限等信息，且应是由主体与医疗机构进行书面授权或用户直接发起的电子授权；
3） 对接方案应双方共同进行安全评估，评估通过才可执行；
4） 应符合国家、监管机关和对接双方的安全要求，确保披露数据的安全性。

11.8.4.2 对接中

a） 数据传输：

1） 双方应在专线、VPN等链路上，采用数据加密或链路加密等安全传输方式，确保健康医疗数据在传输过程中的保密性；
2） 双方通过数字签名等方式实施完整性控制,确保通过网络传输过程的健康医疗数据的完整性；
3） 双方应对涉及健康医疗数据传输的医疗信息系统的登录用户进行身份鉴别；
4） 双方应对医疗信息系统与数据源、建模工具以及外围相关的医疗信息系统的数据传输建立数据同步管理模块，对数据同步范围、进度进行监控管理和记录，防止数据在传输过程中丢失和被篡改，需建立数据丢失重传策略。若数据传输异常发生后，由处理者技术人员评估影响程度，知会医院医保，共同分析异常原因，制定修复方案，恢复数据传输；
5） 双方应对传输操作进行分权管理,即设置不同岗位人员进行数据服务器访问控制列表（ACL）设置、加密数据传输、秘钥传输与管理、数据获取导入及验证等操作；
6） 商业保险公司与医疗机构的数据环境无专线的，建议采用加密移动数据存储介质传输数据，且商业保险公司应对加密移动数据存储介质的操作和使用进行分权管理，即设置不同岗位的人员进行加密移动数据存储介质一次性临时密钥生成、加密移动介质披露数据拷入、数据服务器访问控制列表（ACL）设置、加密移动介质中披露的加密健康医疗数据拷出上传等操作。

b） 数据使用：

1） 双方应为不同角色访问健康医疗数据制定适当的访问控制规则、访问权限和限制，授权策略和信息的分发应遵循“最小授权”、“职责分离”、“角色分离”、“默认拒绝”等原则；

2) 双方应对涉及通过界面展示环节（例如信息系统展示、打印等）的健康医疗数据，在不影响相关业务开展的情况下，采取脱敏、去标识化处理等措施，降低其在展示环节的泄露风险；
3) 商业保险公司使用者应提交健康医疗数据使用申请，申请需包括：健康医疗数据使用合作内容，数据范围、使用数据时间；
4) 商业保险公司应审核健康医疗数据使用申请的有效性、可行性，并制定相关实施方案；审核通过后需建立符合申请审批的数据接口；
5) 商业保险公司应在安全、合法的情况下，通过系统提供的专用接口，进行健康医疗数据的使用；
6) 商业保险公司应对使用者进行合法性校验。

c) 数据存储：

1) 商业保险公司数据中心应基于国家标准设计与建设，并通过监管机构审核认证,原始数据全量存储至历史数据库，经数据脱敏后形成脱敏数据；
2) 商业保险公司应对数据平台设置数据冗余与数据副本(不少于3份),保证存储系统可用性，避免单点故障，确保数据存储可用性；
3) 商业保险公司应通过安全加密技术,确保健康医疗数据在健康医疗信息系统中数据存储的保密性；
4) 商业保险公司应通过安全哈希或其他保护措施,保证健康医疗数据在健康医疗信息系统中数据存储的完整性；
5) 商业保险公司应定期进行数据备份，备份介质场外存放，配备灾难恢复所需的通信线路，建立介质存取、验证和转储管理制度，按介质特性对备份数据进行定期的有效性验证，保证健康医疗数据在健康医疗信息系统中数据存储的可用性。

11.8.4.3 对接后

数据销毁：

a) 商业保险公司应根据业务需求明确健康医疗数据的使用期限；健康医疗数据使用完毕后，确保通过安全措施（例如：消磁等措施）实现安全销毁，防止数据被恢复或有备份数据没有销毁，造成数据的泄露；
b) 商业保险公司使用移动介质进行数据传输的，数据传输结束后，应对移动介质采取数据分区低级格式化，利用无关数据将该分区写满并再次低级格式化的方式进行数据销毁。

11.9 器械维护数据安全

11.9.1 概述

医疗器械维护的目标是确保器械安全、有效和功能正常。医疗器械维护数据安全主要参考了ISO 13485—2016《医疗设备质量管理》。

a) 医疗器械包括：
1) 生命攸关或高风险器械或系统,这类器械或系统失败可能会导致患者或操作人员死亡或受伤；
2) 非生命攸关或低风险器械或系统,此类器械或系统失败不会导致患者或操作人员死亡或受伤；
3) 生命支持器械或系统，此类器械或系统用于维护患者生命，当按厂商的指南或医疗流程操作时，主要功能失效会引起患者死亡；

4) 非生命支持器械或系统，此类器械或系统不用于维护患者生命，当按厂商的指南或医疗流程操作时，主要功能失效不会引起患者死亡。

b) 医疗器械维护涉及的策略包括：

1) 仅恢复功能维护：使不能正常工作的医疗器械或系统正常工作的维护；
2) 计划维护：指在医疗器械或系统丧失功能前进行的维护；
3) 预见性维护：根据医疗器械或系统已知的或可以预见的运行状态或历史记录进行维护；
4) 预防性维护；和当前器械或系统的运行状态无关，进行组件替换、大修或软件版本更新。

11.9.2 涉及的相关方

涉及的相关方包括：远程维护人员、医疗器械厂商、医疗机构、医疗机构医疗器械操作人员及患者。

其中，患者扮演主体的角色，医疗机构扮演控制者的角色，医疗器械厂商根据和医疗机构签署的医疗器械维护合同，承担处理者的角色。

11.9.3 涉及的数据

不同的医疗器械可能涉及不同的数据，影像系统可能涉及患者的影像和影像诊断报告，检验系统可能涉及患者的检验检查报告和检验结果。

除此以外，医疗器械为了维护的目的，还应保存器械的维护历史记录。维护历史记录包括：维护的内容、维护的原因、维护的时间、维护的操作人员。

为了维护的目的，操作人员可能需要获得日志信息，但不限于：

a) 医疗机构名称；
b) 用途；
c) 物理环境参数；
d) 关键部件信息；
e) 器械的可靠性，具体包括器械失败的频率和类型，器械维修所需时间；
f) 维修趋势；
g) 如果含有电池，电池性能；
h) 其他易耗品的检验；
i) 器械的寿命。

11.9.4 重点安全措施

11.9.4.1 概述

医疗器械厂商应与医疗机构签署维护合同，双方的权利和义务，并根据GB/T 35273—2017《信息安全技术　个人信息安全规范》和医疗安全准则ISO8001，进行数据安全评估。

如果在医疗器械维护过程中涉及到个人数据，原则上不需要获得主体同意，如果需要将涉及的数据用于其他目的，应获得主体同意。

11.9.4.2 数据采集

医疗器械厂商进行远程维护，可能会读取器械的维护记录和日志报告，分析医疗器械失败原因；也可能读取医疗器械产生的数据，分析应用的安全性和有效性。

在此阶段，应建立以下安全措施：

a) 建立安全远程接入机制：建立维护人员授权访问机制，只有经过安全认证的维护人员才可以远程访问被授权的医疗器械；根据需要建立安全链接获取维护记录和日志信息；

b） 数据隐私保护：如果需要导出医疗器械产生的数据，分析应用的安全性和有效性，数据涉及到个人信息，应对数据进行去标识化处理；
c） 基于角色和位置的访问控制：不同职能的维护人员可能需要访问不同的医疗器械信息，建议进一步强化只有来自特定公司的特定维护人员可以访问；
d） 应用信息安全：通过远程桌面访问应用信息应得到医疗器械操作人员或医疗机构工作人员的授权。

11.9.4.3 操作权限

保证医疗器械的安全可靠工作，维护人员还可能进行以下操作：
1） 进行性能验证测试，获得测试结果；
2） 医疗器械自检；
3） 医疗器械校准；
4） 医疗器械系统补丁、软件重装或版本更新。
在此阶段，应建立以下安全措施：
a） 建立安全远程接入机制：建立维护人员授权访问机制，只有经过安全认证的维护人员才可以远程访问被授权的医疗器械；
b） 基于角色和位置的访问控制：不同职能的维护人员可能需要访问不同的医疗器械信息，建议进一步强化只有来自特定公司的特定维护人员可以访问；
c） 应得到医疗器械操作人员授权。

11.9.4.4 数据保存

医疗器械厂商采集医疗器械的维护记录和日志报告。建议医疗器械厂商在数据存储阶段采取以下安全措施保护数据安全。
在医疗器械厂商端：
a） 建立基于角色的访问控制机制，只有被授权维护人员才可以访问数据；
b） 应对数据进行完整性验证，保证数据的完整性及不被篡改。

11.9.4.5 数据使用

医疗器械厂商在数据使用阶段建立以下安全措施：
a） 建立基于角色的数据访问控制机制，只有被授权的角色可以访问被授权的数据对象，维护人员只能访问指定产品的维修记录和日志信息；
b） 数据传输应使用加密技术、身份验证技术和数据完整性校验技术保证数据以安全的方式传输给指定的对象；
c） 建立安全审计制度，记录人、程序在什么时间、地点、场景访问了什么数据，记录安全事件。

11.9.4.6 组织管理要求

医疗器械厂商在数据使用阶段建立以下组织管理措施：
a） 建立安全策略、规程和管理流程；
b） 定期进行安全风险评估和管理；
c） 制定和执行安全运维；
d） 制定应急管理策略并定期演练；
e） 确定安全责任；
f） 对员工进行安全管理、安全培训和考核。

附 录 A
（资料性附录）
个人健康医疗数据范围

个人健康医疗数据可能包括：

a) 提供健康医疗服务时登记的个人信息；
b) 出于健康医疗目的，例如治疗、支付或保健护理等，分配给个人的唯一标识号码或符号等；
c) 在向个人提供健康医疗服务过程中采集的有关个人的任何数据，例如既往病史、社会史、家族史、症状和生活方式等各类病历记载的数据；
d) 来自身体部位或身体物质，例如组织、体液、血、尿、便、气体，以及 DNA、RNA、蛋白质等生物大分子、代谢小分子、肠道微生物等检查或检验的结果数据；
e) 可穿戴设备采集的与个人健康相关的数据，并且该种数据：
    1) 本身或者明显为健康医疗相关数据；
    2) 或是由传感器采集的，并且可以单独或者与其他数据结合用来对可穿戴设备的用户的健康状况或者疾病风险进行判断的数据；
    3) 或是可穿戴设备采集的数据并且为对用户的健康状况或者疾病风险进行判断后的结论；
    4) 或是通过可穿戴设备相连的 APP 或者系统进行传送的，并非可穿戴设备使用者另行提供的；
f) 接受的健康医疗服务相关数据，例如检验检查医嘱、诊断、操作、药物、医疗效果等；
g) 为个人提供健康医疗服务的服务者身份数据；
h) 关于个人的支付或医保相关数据；
i) 医学科研相关数据，例如临床研究病例数据、生物样本库、全基因组等多种生物组学测序结果、医学相关队列研究结果等；
j) 公共卫生与预防医学数据，例如疾控中心、公共卫生管理部门收集的疾病卫生监测个人数据。

附 录 B
（资料性附录）
卫生信息数据集分类与标准

为了规范卫生信息系统建设和卫生信息的互联互通，参考 HL7 相关标准，结合我国实际情况，通过信息建模，国家卫生标准委员会信息标准专业委员会制定了一系列卫生信息数据集标准，这些标准在指导医院信息化以及互联互通等方面起了很重要的规范和指导作用。详见表 B.1 所示。

表 B.1 数据集标准

大类	小类	序号	数据集名称	标准
公共卫生基本数据集	基本档案	1	城乡居民健康档案基本数据集	WS 365-2011
		2	基本信息基本数据集个人信息	WS 371-2012
	疾病管理基本数据集	3	乙肝患者管理	WS 372.1-2012
		4	高血压患者健康管理	WS 372.2-2012
		5	重性精神疾病患者管理	WS 372.3-2012
		6	老年人健康管理	WS 372.4-2012
		7	2 型糖尿病病例管理	WS 372.5-2012
		8	肿瘤病例	WS 372.6-2012
	医疗服务基本数据集	9	门诊摘要	WS 373.1-2012
		10	住院摘要	WS 373.2-2012
		11	成人健康体检	WS 373.3-2012
	卫生管理基本数据集	12	卫生监督检查与行政处罚	WS 374.1-2012
		13	卫生监督行政许可与登记	WS 374.2-2012
		14	卫生监督监测与评价	WS 374.3-2012
		15	卫生监督机构与人员	WS 374.4-2012
	疾病控制基本数据集	16	艾滋病综合防治	WS 375.1-2012
		17	血吸虫病患者管理	WS 375.2-2012
		18	慢性丝虫病患者管理	WS 375.3-2012
		19	职业病报告	WS 375.4-2012
		20	职业性健康监护	WS 375.5-2012
		21	伤害监测报告	WS 375.6-2012
		22	农药中毒报告	WS 375.7-2012
		23	行为危险因素监测	WS 375.8-2012
		24	死亡医学证明	WS 375.9-2012
		25	传染病报告	WS 375.10-2012
		26	结核病报告	WS 375.11-2012
		27	预防接种	WS 375.12-2012
		28	职业病危害因素监测	WS 375.13-2017
		29	学校缺勤缺课监测报告	WS 375.14-2016
		30	托幼机构缺勤监测报告	WS 375.15-2016
		31	疑似预防接种异常反应报告	WS 375.18-2016
		32	疫苗管理	WS 375.19-2016
		33	脑卒中登记报告	WS 375.20-2016

		34	脑卒中患者管理	WS 375.21-2016
		35	宫颈癌筛查登记	WS 375.22-2016
		36	大肠癌筛查登记	WS 375.23-2016
	儿童保健基本数据集	37	出生医学证明	WS 376.1-2013
		38	儿童健康体检	WS 376.2-2013
		39	新生儿疾病筛查	WS 376.3-2013
		40	营养性疾病儿童管理	WS 376.4-2013
		41	5 岁以下儿童死亡报告	WS 376.5-2013
	妇女保健基本数据集	42	婚前保健服务	WS 377.1-2013
		43	妇女常见病筛查	WS 377.2-2013
		44	计划生育技术服务	WS 377.3-2013
		45	孕产期保健服务与高危管理	WS 377.4-2013
		46	产前筛查与诊断	WS 377.5-2013
		47	出生缺陷监测	WS 377.6-2013
		48	孕产妇死亡报告	WS 377.7-2013
电子病历基本数据集	病历概要	18	电子病历基本数据集 第 1 部分 病历概要-患者基本信息子集	WS 445.1-2014
		19	电子病历基本数据集 第 1 部分 病历概要-基本健康信息子集	WS 445.1-2014
		20	电子病历基本数据集 第 1 部分 病历概要-卫生事件摘要子集	WS 445.1-2014
		21	电子病历基本数据集 第 1 部分 病历概要-医疗费用记录子集	WS 445.1-2014
	门（急）诊病历	22	电子病历基本数据集 第 2 部分 门（急）诊病历-门（急）诊病历子集	WS 445.2-2014
		23	电子病历基本数据集 第 2 部分 门（急）诊病历-急诊留观病历子集	WS 445.2-2014
		24	电子病历基本数据集 第 3 部分 门（急）诊处方-西药处方子集	WS 445.3-2014
		25	电子病历基本数据集 第 3 部分 门（急）诊处方-中药处方子集	WS 445.3-2014
	检查检验记录	26	电子病历基本数据集 第 4 部分 检查检验记录-检查记录子集	WS 445.4-2014
		27	电子病历基本数据集 第 4 部分 检查检验记录-检验记录子集	WS 445.4-2014
	一般治疗处置记录	28	电子病历基本数据集 第 5 部分 一般治疗处置记录-治疗记录子集	WS 445.5-2014
		29	电子病历基本数据集 第 5 部分 一般治疗处置记录--一般手术记录子集	WS 445.5-2014
		30	电子病历基本数据集 第 5 部分 一般治疗处置记录-麻醉术前访视记录子集	WS 445.5-2014
		31	电子病历基本数据集 第 5 部分 一般治疗处置记录-麻醉记录子集	WS 445.5-2014
		32	电子病历基本数据集 第 5 部分 一般治疗处置记录-麻醉术后访视记录子集	WS 445.5-2014
		33	电子病历基本数据集 第 5 部分 一般治疗处置记录-输血记录子集	WS 445.5-2014
	助产记录	34	电子病历基本数据集 第 6 部分 助产记录-待产记录子集	WS 445.6-2014
		35	电子病历基本数据集 第 6 部分 助产记录-阴道分娩记录子集	WS 445.6-2014

		36	电子病历基本数据集 第 6 部分 助产记录-剖宫产手术记录子集	WS 445.6-2014
	护理操作记录	37	电子病历基本数据集 第 7 部分 护理操作记录-一般护理记录子集	WS 445.7-2014
		38	电子病历基本数据集 第 7 部分 护理操作记录-病危（重）护理记录子集	WS 445.7-2014
		39	电子病历基本数据集 第 7 部分 护理操作记录-手术护理记录子集	WS 445.7-2014
		40	电子病历基本数据集 第 7 部分 护理操作记录-生命体征测量记录子集	WS 445.7-2014
		41	电子病历基本数据集 第 7 部分 护理操作记录-出入量记录子集	WS 445.7-2014
		42	电子病历基本数据集 第 7 部分 护理操作记录-高值耗材使用记录子集	WS 445.7-2014
	护理评估与计划	43	电子病历基本数据集 第 8 部分 护理评估与计划-入院评估记录子集	WS 445.8-2014
		44	电子病历基本数据集 第 8 部分 护理评估与计划-护理计划记录子集	WS 445.8-2014
		45	电子病历基本数据集 第 8 部分 护理评估与计划-出院评估与指导记录子集	WS 445.8-2014
	知情告知信息	46	电子病历基本数据集 第 9 部分 知情告知信息-手术同意书子集	WS 445.9-2014
		47	电子病历基本数据集 第 9 部分 知情告知信息-麻醉知情同意书子集	WS 445.9-2014
		48	电子病历基本数据集 第 9 部分 知情告知信息-输血治疗同意书子集	WS 445.9-2014
		49	电子病历基本数据集 第 9 部分 知情告知信息-特殊检查及特殊治疗同意书子集	WS 445.9-2014
		50	电子病历基本数据集 第 9 部分 知情告知信息-病危（重）通知书子集	WS 445.9-2014
		51	电子病历基本数据集 第 9 部分 知情告知信息-其他知情同意书子集	WS 445.9-2014
	住院病案首页	52	电子病历基本数据集 第 10 部分 住院病案首页-住院病案首页子集	WS 445.10-2014
	中医住院病案首页	53	电子病历基本数据集 第 11 部分 中医住院病案首页-中医住院病案首页子集	WS 445.11-2014
	入院记录	54	电子病历基本数据集 第 12 部分 入院记录-入院记录子集	WS 445.12-2014
		55	电子病历基本数据集 第 12 部分 入院记录-24h 内入出院记录子集	WS 445.12-2014
		56	电子病历基本数据集 第 12 部分 入院记录-24h 内入院死亡记录子集	WS 445.12-2014

	住院病程记录	57	电子病历基本数据集 第 13 部分 住院病程记录-首次病程记录子集	WS 445.13-2014
		58	电子病历基本数据集 第 13 部分 住院病程记录-日常病程记录子集	WS 445.13-2014
		59	电子病历基本数据集 第 13 部分 住院病程记录-上级医师查房记录子集	WS 445.13-2014
		60	电子病历基本数据集 第 13 部分 住院病程记录-疑难病例讨论子集	WS 445.13-2014
		61	电子病历基本数据集 第 13 部分 住院病程记录-交接班记录子集	WS 445.13-2014
		62	电子病历基本数据集 第 13 部分 住院病程记录-转科记录子集	WS 445.13-2014
		63	电子病历基本数据集 第 13 部分 住院病程记录-阶段小结子集	WS 445.13-2014
		64	电子病历基本数据集 第 13 部分 住院病程记录-抢救记录子集	WS 445.13-2014
		65	电子病历基本数据集 第 13 部分 住院病程记录-会诊记录子集	WS 445.13-2014
		66	电子病历基本数据集 第 13 部分 住院病程记录-术前小结子集	WS 445.13-2014
		67	电子病历基本数据集 第 13 部分 住院病程记录-术前讨论子集	WS 445.13-2014
		68	电子病历基本数据集 第 13 部分 住院病程记录-术后首次病程记录子集	WS 445.13-2014
		69	电子病历基本数据集 第 13 部分 住院病程记录-出院记录子集	WS 445.13-2014
		70	电子病历基本数据集 第 13 部分 住院病程记录-死亡记录子集	WS 445.13-2014
		71	电子病历基本数据集 第 13 部分 住院病程记录-死亡病例讨论记录子集	WS 445.13-2014
	住院医嘱	72	电子病历基本数据集 第 14 部分 住院医嘱-住院医嘱子集	WS 445.14-2014
	出院小结	73	电子病历基本数据集 第 15 部分 出院小结-出院小结子集	WS 445.15-2014
	转诊（院）记录	74	电子病历基本数据集 第 16 部分 转诊（院）记录-转诊（院）记录子集	WS 445.16-2014
	医疗机构信息	75	电子病历基本数据集 第 17 部分 医疗机构信息-医疗机构信息子集	WS 445.17-2014
卫生统计指标		76	卫生统计指标第 1 部分：总则	WS/T 598.1-2018
		77	卫生统计指标第 2 部分：健康状况	WS/T 598.2-2018
		78	卫生统计指标第 3 部分：健康影响因素	WS/T 598.3-2018
		79	卫生统计指标第 4 部分：疾病控制	WS/T 598.4-2018
		80	卫生统计指标第 5 部分：妇幼保健	WS/T 598.5-2018
		81	卫生统计指标第 6 部分：卫生监督	WS/T 598.6-2018
		82	卫生统计指标第 7 部分：医疗服务（含中医）	WS/T 598.7-2018
		83	卫生统计指标第 8 部分：药品与材料供应保障	WS/T 598.8-2018
		84	卫生统计指标第 9 部分：医疗保障新农合	WS/T 598.9-2018
医院人财物运营管理		85	医院人财物运营管理基本数据集第 1 部分：医院人力资源管理	WS 599.1-2018
		86	医院人财物运营管理基本数据集第 2 部分：医院财务与成本核算管理	WS 599.2-2018
		87	医院人财物运营管理基本数据集第 3 部分：医院物资管理	WS 599.3-2018
		88	医院人财物运营管理基本数据集第 4 部分：医院固定资产管理	WS 599.4-2018

附 录 C
（资料性附录）
医院数据使用管理办法参考

第一章 总则

第一条 为规范医院数据使用流程，根据国家相关法律法规及相关规定，特制定本办法。

第二条 制定本办法所参考的主要法律法规及办法指南包括《中华人民共和国网络安全法》、《中华人民共和国保守国家秘密法》、《关于国家秘密载体保密管理的规定》、《科学数据管理办法》、《关于促进和规范健康医疗大数据应用发展的指导意见》、《卫生工作中国家秘密范围的规定》、《教育工作中国家秘密及其密级具体范围的规定》、《中华人民共和国计算机信息系统安全保护条例》、《信息安全等级保护管理办法》、《国家健康医疗大数据标准、安全和服务管理办法》、《卫生行业信息安全等级保护工作的指导意见》、《信息安全技术 大数据安全管理指南》、《信息安全技术 个人信息安全规范》、《信息安全技术 信息安全风险评估规范》、《信息安全技术 数据出境安全评估指南》、《个人信息和重要数据出境安全评估办法》、《人类遗传资源采集、收集、买卖、出口、出境审批行政许可服务指南》、《医疗机构病历管理规定》、《涉及人的生物医学研究伦理审查办法》、《人口健康信息管理办法（试行）》、《加强医疗卫生行风建设“九不准”》、《关于加强医疗卫生机构统方管理的规定》等。

第三条 本办法决策主体为医院数据委员会，执行机构为医院数据使用管理工作组，申请主体为院内需要申请数据使用的科室、项目组和个人（详见第二章）。原则上申请人为项目负责人，申请人对所有申请数据的安全使用全权负责，即申请人应保证其本人及其项目组成员对申请数据均有信息安全及数据保密义务、承担由于数据及信息安全问题造成的所有不良后果。

第四条 本办法中的数据资源包括但不限于医院 HIS、LIS、PACS 等医院系统平台产生的业务数据、医疗保险数据、死亡人口数据等。

第五条 本办法制定原则为“促进利用、规范流程、安全可控、明确责任”。在确保数据安全的前提下，参考国家数据使用相关法律法规，结我院医疗、教学、科研工作实际，本着责权利一致原则，推进数据资源管理与利用。

第六条 本办法涉及单位如下：

（一）医院。

（二）数据提供单位。

（三）数据申请使用单位及个人。

第二章 组织管理与职责

第七条 医院数据使用管理工作机构设置

医院成立数据委员会，下设数据使用管理工作组执行推进。

1. 数据委员会组成如下：

主任委员：1 名

副主任委员：2 名

委员：若干名

顾问：若干名

秘书：1 名

（建议：负责人为院主要领导，成员由党委办公室（保密）、院长办公室、临床研究管理部、大数据中心、信息中心、伦理办公室、审计处、成果转化部、科技部、国有资产管理部、医务部等相关部门负责人及遴选的临床学者担任。同时，组织临床专家/科研人员、数据安全专家、法律专家形成顾问组。）

2. 数据使用管理工作组组成如下：

组　长：大数据中心主任
副组长：大数据中心平台工作组组长（兼安全管理员）
成　员：若干

第八条 医院数据使用管理机构职责

（一）数据委员会职责

1.界定数据使用范围及数据使用权限；
2.审批及决策医院数据使用相关流程；
3.审批不同来源科研数据的脱敏、加密方案；
4.审批科研成果发表规范；
5.审批科研数据项目申请；
6.审批科研数据合作研究申请；
7.审批数据使用账号申请；
8. 审批与数据出境的安全评估；
9.其他需要研究与决策的问题。

（二）数据使用管理工作组职责

1.按数据委员会要求编制及修订数据使用工作流程；
2.负责初审数据使用申请单位提交的材料；
3.负责收集与汇总全院数据使用及合作需求，定期上报数据委员会；
4.定期组织数据使用及合作审批工作会议；
5.审批同意后，根据审批结果，负责将相应数据移交给申请方或监督申请方在安全环境内使用；
6.负责建立并管理数据的存储和使用环境，确保数据采集、存储和使用各环节的安全保密；
7.数据使用及安全工作的日常协调；
8.完成数据资源评估专家委员会交办的其他工作。

第三章　数据申请及审批流程

第九条 申请单位申请使用相关数据的，应提出明确的使用目的和范围，经数据使用管理工作组初审后，将相关资料提交数据委员会审批。

第十条 数据原则只在院内提供的安全环境中使用。数据原则上只与有相应保密资质的境内单位开展合作研究。在未获得政府行业主管或监管部门批准合作项目批文的情况下，数据不予境外单位（含外国组织和个人以及在我国注册的外商独资企业和中外合资、合作企业）使用。在未获得政府行业主管或监管部门批准同意的情况下，数据不能出境。

第十一条 数据使用申请及审批流程

（一）院内科室部门的境内项目（数据不与其他单位使用）

1.申请单位申请使用医院数据，应向数据使用管理工作组提交下列申请材料，所有材料一式三份。
（1）数据使用申请表；
（2）项目批准文件、委托函、任务书或其他能够说明使用目的的相关文件；
（3）经办人有效身份证明（身份证或胸牌卡）及复印件。

2.数据使用管理工作组对材料进行初审。初审不通过，将材料退回申请单位；初审通过，将材料提交数据委员会审批。

3.数据委员会对申请进行集体决议，超过三分之二委员表决同意，视为审批通过，由表决同意的全体委员会签。

4.数据委员会审批通过后，申请人将材料一式一份分别交由数据使用管理工作组和数据提供单位。数据使用申请人与数据提供单位签署保密协议，由数据提供单位负责数据安全移交。

（二）院内部门境内项目（数据要与境内有相关保密资质的其他合作单位使用）

1.申请单位申请使用医院数据，应向数据使用管理工作组提交下列申请材料，所有材料一式三份。

（1）数据使用申请表；

（2）项目批准文件、委托函、任务书、合作协议或其他能够说明使用目的的相关文件；

（3）境内合作单位数据保密能力证明材料；

（4）经办人有效身份证明（身份证或胸牌卡）及复印件。

2.数据使用管理工作组对材料进行初审。初审不通过，将材料退回申请单位；初审通过，将材料提交数据委员会审批。

3.数据委员会对申请进行集体决议，超过三分之二委员表决同意，视为审批通过，由表决同意的全体委员会签。

4.数据委员会审批通过后，申请人将材料一式一份分别交由数据使用管理工作组和数据提供单位。数据使用申请人与数据提供单位签署保密协议，由数据提供单位负责数据安全移交。

（三）院内部门境内项目（数据要与境外其他合作单位（含外国组织和个人以及在我国注册的外商独资企业和中外合资、合作企业）使用）

1.申请单位应向数据使用管理工作组提交下列申请材料，所有材料一式三份。

（1）数据使用申请表；

（2）政府批准合作项目批文；

（3）外方身份证明材料；

（4）外方单位数据保密能力证明材料；

（5）经办人有效身份证明及复印件。

2.数据使用管理工作组对材料进行初审。初审不通过，将材料退回申请单位；初审通过，将材料提交数据委员会审批。

3.数据委员会对申请进行集体决议，超过三分之二委员表决同意，视为审批通过，由表决同意的全体委员会签。

4.数据委员会审批通过后，申请人将材料一式一份分别交由数据使用管理工作组和数据提供单位。数据使用申请人与数据提供单位签署保密协议，由数据提供单位负责数据安全移交。

第四章　数据移交及使用流程

第十二条 数据提供单位负责划出项目专用安全应用环境，并对项目申请数据进行脱敏加密处理后，移交到专用安全应用环境内。如果数据提供单位不具备相关能力，可向数据使用管理工作组提出申请，由工作组报数据委员会协调。

第十三条 申请单位在确定项目数据使用人员后向数据使用管理工作组提交数据使用账号申请，获批后原则上只能在数据提供单位提供的专用安全应用环境中使用所申请的数据。

第十四条 数据使用账号申请及审批流程

1.数据使用人员申请账号，应向数据使用管理工作组提交下列申请材料，所有材料一式三份。

（1）数据使用账号申请表；

（2）账号申请人员有效身份证明（身份证或胸牌卡）及复印件。

2.数据使用管理工作组对材料进行初审。初审不通过，将材料退回申请单位；初审通过，将材料提交数据委员会审批。

3.数据委员会对申请进行集体决议，超过三分之二委员表决同意，视为审批通过，由表决同意的全体委员会签。

4.审批通过后，将材料一式一份分别交由数据使用管理工作组和数据提供单位。由数据提供单位开通专用安全应用环境中相应账号及权限，数据提供单位负责对数据使用全过程进行安全管控。

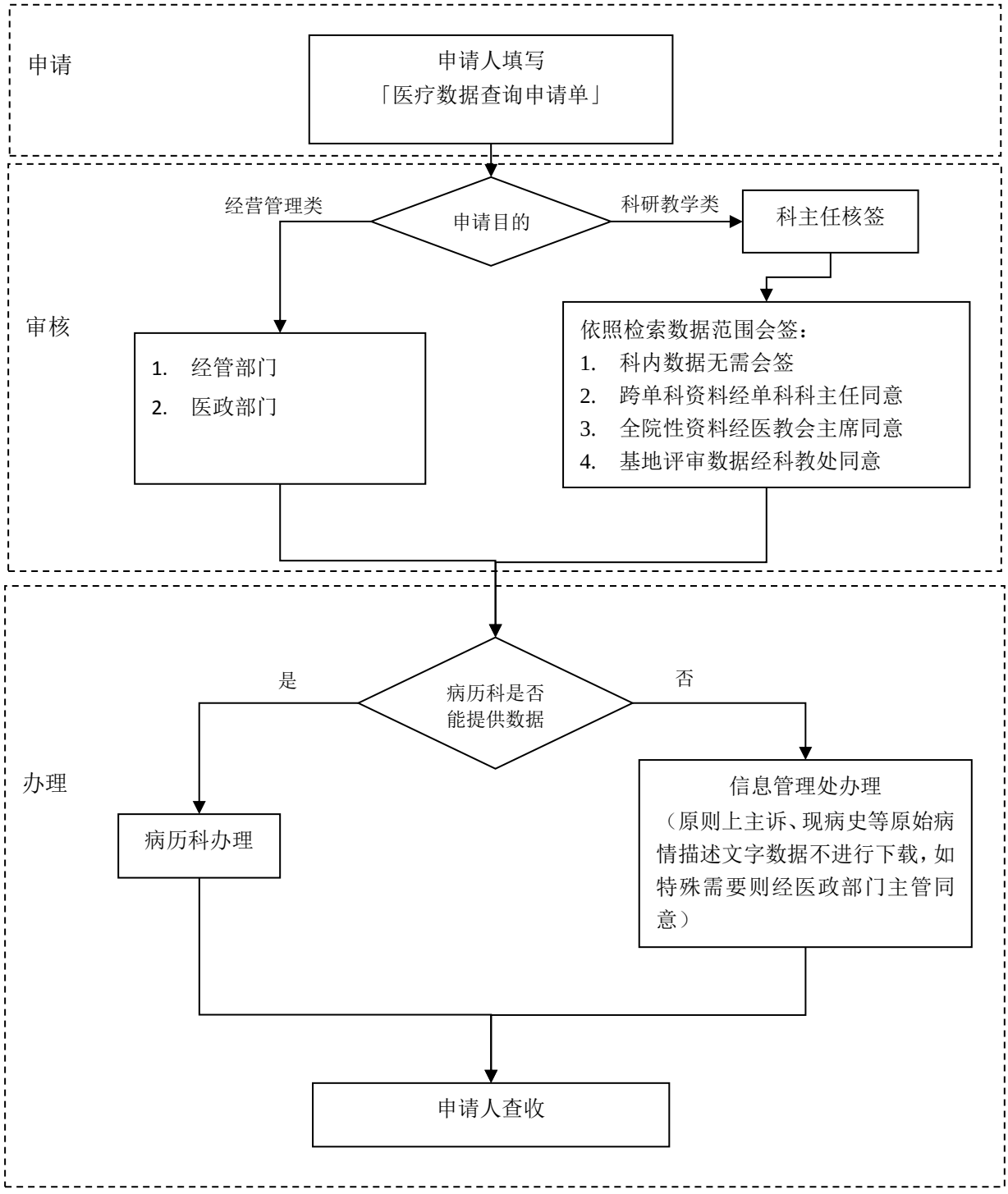
第十五条 项目结束或数据申请使用期满，账号自动注销，如果要继续使用，需重新申请。在项目进行过程中，若账号使用人员发生变更，需提前以书面形式告知数据使用管理工作组。

第五章 附则

第十六条 本办法自发布之日起执行，由数据委员会负责解释和修订。

附 录 D
（资料性附录）
数据申请审批参考

医疗数据查询传签流程参考



医院数据使用申请表参考

<table>
<tr><td colspan="4">本单编号</td><td colspan="6"></td></tr>
<tr><td>申请人</td><td colspan="2"></td><td>申请科室</td><td colspan="6"></td></tr>
<tr><td>申请人电话</td><td colspan="2"></td><td>申请人邮箱</td><td colspan="6"></td></tr>
<tr><td>需要日期</td><td colspan="2"></td><td>申请日期</td><td colspan="6"></td></tr>
<tr><td>目的说明</td><td colspan="9"></td></tr>
<tr><td rowspan="5">科研教学类数据</td><td colspan="5">☐ 科内数据：科主任</td><td colspan="4">签名：</td></tr>
<tr><td colspan="5">☐ 跨科别数据：科主任→相关科室科主任</td><td colspan="4">签名：</td></tr>
<tr><td colspan="5">☐ 医学部&中心数据：科主任→医学部及中心部长</td><td colspan="4">签名：</td></tr>
<tr><td colspan="5">☐ 全院数据：科主任→医教会主席</td><td colspan="4">签名：</td></tr>
<tr><td colspan="5">☐ 基地评审数据：科主任→科教处</td><td colspan="4">签名：</td></tr>
<tr><td rowspan="2">经营管理类数据</td><td colspan="5">☐ 经管组→医院经管主管</td><td colspan="4">签名：</td></tr>
<tr><td colspan="5">☐ 医政组→医政组一级主管</td><td colspan="4">签名：</td></tr>
<tr><td>主诉、现病史等原始病情描述文字数据</td><td colspan="5">☐ 部门主管→医院行政主管</td><td colspan="4">签名：</td></tr>
<tr><td>数据时间范围</td><td colspan="9">年 月 日—— 年 月 日</td></tr>
<tr><td>查询诊断/手术名称，建议附 ICD 编码</td><td colspan="9"></td></tr>
<tr><td rowspan="4">查询数据内容</td><td>☐</td><td colspan="8">一、病历科可查询数据项目（病历科联系电话 XXXXX）</td></tr>
<tr><td>1.</td><td>门诊</td><td></td><td>急诊</td><td colspan="5"></td></tr>
<tr><td></td><td>病历号</td><td></td><td>就诊号</td><td></td><td>姓氏</td><td></td><td>性别</td><td></td><td>看诊日期</td></tr>
<tr><td></td><td>医师</td><td></td><td>第一诊断名称</td><td></td><td>全部诊断名称</td><td></td><td>第一诊断排名</td><td></td><td>全部诊断排名</td></tr>
</table>

<table>
<tr><td rowspan="6"></td><td colspan="14">2. 住院</td></tr>
<tr><td></td><td>病历号</td><td></td><td>就诊号</td><td></td><td>姓名</td><td></td><td>性别</td><td></td><td>年龄</td><td></td><td>入院日期</td><td></td></tr>
<tr><td></td><td>入院科室</td><td></td><td>出院时间</td><td></td><td>出院科室</td><td></td><td>出院病区</td><td></td><td>离院方式</td><td></td><td>住院天数</td><td></td></tr>
<tr><td></td><td>来源</td><td></td><td>主治医师</td><td></td><td>第一诊断名称</td><td></td><td>全部诊断名称</td><td></td><td colspan="3">有创操作及手术名称</td><td></td></tr>
<tr><td>☐</td><td colspan="13">二、 信息处辅助查询其他内容：</td></tr>
<tr><td colspan="14"></td></tr>
<tr><td>备注说明</td><td colspan="14"></td></tr>
<tr><td colspan="15">申请人声明：☐ 同意不同意遵守下列各事项
1. 在使用数据或发表时，不因任何理由侵犯个人隐私权及泄漏医院之业务机密，亦不作为营利目的使用。
2. 遵守数据仅拷贝于必要之工作电脑，且不以任何方式将数据文件提供给参与本研究以外之他人使用。
3. 数据文件仅提供给共同参与之研究人员，申请人负责监督其遵守本 1.2 之规定，申请人愿意担负连带保证责任如违反上述规定所致一切后果，由申请人负全部责任。
4. 数据不允许出境,若有出境需求,必须以签呈形式获得院务会批准。</td></tr>
<tr><td>申请人签字</td><td colspan="14"></td></tr>
</table>

附 录 E
（资料性附录）
数据处理使用协议参考

E.1 概述

当一个控制者需要引入处理者帮助或者代为处理数据，或者将数据披露给使用者使用时，应通过协议明确各方责任及相应要求。C.2 给出了控制者-处理者间数据处理协议模板，C.3 给出了控制者-使用者间的数据使用协议模板。

E.2 数据处理协议模板

协议主体条款

甲方：【公司名称】（以下简称“**数据控制者**”）

乙方：【公司名称】（以下简称“**数据处理者**”）

数据使用目的、方式及范围：

1) 目的：为实现“【 】项目”（以下简称合作项目）的合作目的，数据控制者须提供相关数据，就该等数据的提供和处理事宜，在本协议中做出特别说明。

2) 范围：本数据处理协议条款适用于出于合作项目的合作目的，数据处理者从数据控制者处收集、获取及产生的任何个人健康医疗数据的处理、使用和保护。

数据使用条款

基于本协议，数据处理者仅可将从数据控制者接收到的数据用于履行本协议的目的，包括：

1) 【根据实际情况填写】

保密以及数据保护义务条款

1) 数据备份。数据处理者同意在提供服务必要之时或收到数据控制者通知时为已录入信息系统的项目数据创建备份。数据处理者应采取一切必要措施，确保备份过程的保密性。

2) 确保数据安全。数据处理者应采取技术措施和其他必要措施，确保数据安全性、保密性、隐私性，防止个人健康数据在提供本协议项下所述及本数据安全条件项下要求的服务所需的所有操作过程中发生任何泄露、损坏或丢失。如发生任何实际或潜在的数据泄露、损坏或丢失，数据处理者应立即采取补救措施并立即通知数据控制者。

3) 确保数据的机密性和安全性。数据处理者网络安全人员应对在履行职责时所知晓的所有数据严格保密，不得向任何第三方非法泄露、出售或提供。此外，数据处理者应防止数据处理者员工盗取或以其他方式非法获取任何数据，向第三方出售、提供任何项目数据，或以其他方式非法使用项目数据。

定义

1) 本数据处理合同条款中的个人健康医疗数据，指能够单独或者与其他信息结合识别特定自然人或者反映特定自然人生理或心理健康的相关数据，涉及个人过去、现在或将来的身体或精神健康状况、接受的医疗保健服务和支付的医疗保健服务费用等。

基本义务

1) 数据控制者义务，数据控制者同意并保证：

a）个人健康医疗数据的处理（包括转移本身）已在并且将在不违反所适用的该国数据保护法相关规定的情况下进行；

b）它会依照指示进行操作，并且在健康医疗数据处理服务的过程中，指导数据处理者只处理由数据控制者传输的健康医疗数据，并且会遵守所适用的数据保护法律以及本合同；

c）数据处理者将依照适用数据保护法的要求在技术和组织安全措施方面提供充分的保障，防止个人健康医疗数据免受意外事件或是非法损毁或是意外丢失、更改、未经授权公开或访问，以及所有非法形式数据处理，尤其是将个人健康医疗数据传输至数据处理者的过程。

2) 数据处理者义务，数据处理者同意并保证：

a）只处理由数据控制者提供的个人健康医疗数据，并且会遵守数据控制者的指示，遵守本合同的约定，如果它不能够保证遵守，基于任何理由，它都应当及时将它的缺乏实施能力的情况告知数据控制者，在此情形下，数据控制者应当有权终止数据传输行为以及/或者终止合同；

b）它有理由认为其应当遵守的法律法规、应履行的合同义务、或法律规定中出现的变化导致对其履行其对合同条款的承诺和义务造成的实质上不利的影响妨碍了其履行数据控制者的指示，一经发现有何变故，其应当及时告知数据控制者，在此情况下，数据控制者应当有权终止数据传输并且/或者终止合同；

c）它在处理传输的个人健康医疗数据之前已经配置了相应技术和组织安全保障措施；

d）它将会及时告知数据控制者以下内容：

①除非法律禁止，其应告知所有执法机关有法律约束力的要求披露健康医疗数据的请求，例外情形有刑法中的禁止泄露机密性执法调查；

②任何意外或是未授权的访问；

③任何直接由数据主体发出的尚未响应的请求，除非已被授权去那么做。

e）迅速妥善处理数据控制者请求的与其处理的被传输的健康医疗数据相关的问题，并且遵守监管机构对于处理被传输数据的相关建议；

f）应数据控制者的要求提交其审理本合同所指应由数据控制者实施的或是有相应专业资质的独立检查机构应实施的，相应数据处理活动的数据处理设施，并受到保密义务的约束，由数据控制者选择实施方式，并在可实现的情况下，与监管机构订立相应协议；

g）根据数据主体的要求，提供合同副本，或是任何现有的第三方处理合同副本，除非该条款或是合同包含了商业信息，数据处理者可以选择删除该商业信息，或者在数据主体不能从数据控制者方得到合同副本时提供安全措施的主要描述；

h）在第三方进行数据处理的情形中，数据处理者应当提前通知数据控制者，并在此之前获得数据控制者的事前书面同意；

i）保证第三方数据处理者会遵守本合同约定进行数据处理；

j）根据合同约定及时发送任何现存第三方处理者的合同副本给数据控制者。

下游数据处理者

1） 未经数据控制者事先书面同意，数据处理者不得转包其代表数据控制者实施的任何数据处理行为。对于数据控制者同意签订转包合同的，数据处理者应通过合同或者其他方式确保对于第三方处理者的义务应当与数据处理者在本协议下所承担的义务相一致。

数据处理服务终止后的义务

1） 双方同意，在数据处理服务终止后，数据处理者以及下游数据处理者，基于数据控制者的选择，应当返还所有传输的健康医疗数据及其副本，或者应当销毁所有健康医疗数据，并且应向数据控制者证明其已经完成了销毁，除非法律明确规定数据处理者不应返还或销毁被传输的全部或者部分的健康医疗数据。在此情况下，数据处理者以及下游数据处理者应对被传输的健康医疗数据保证其承担保密义务，并且再也不会主动处理被传输的健康医疗数据。

2） 数据处理者以及下游数据处理者保证，基于数据控制者以及/或者其监管机构的请求，它将会提交它的数据处理设施以完成对它的设施进行的审计。

E.3 数据使用协议模板

当一个控制者希望以公共卫生研究、科学研究和/或医疗保健业务为目的披露受限制数据集时，应在合同中对数据使用的情况以及相关的数据保护义务进行约定，以便在控制者作为数据提供方与数据接收方之间分配受限制数据集的使用或披露的责任，保护受限制数据集的安全，通过有约束力的合同形式要求双方遵守相关法律法规和标准的规定。

以下为本指引提供的数据使用条款模板，双方可以将模板条款直接加入《数据使用协议》，也可以根据本指引和实际情况自行编写《数据使用协议》中的相关条款。

数据使用条款

1) 数据接收方希望使用受限制数据集进行公共卫生研究、科学研究和/或医疗保健业务（“**目的**”），并且该等使用的计划以及为实现其目的所需的信息（例如：诊断结论，性别和年龄）在本协议附件 A 中列出。除本协议项下数据接收方使用该等受限制数据集应仅用于实现任何一项或者多项目的以外，数据接收方同意遵循所适用法律、法规和独立审核小组对分析所提出的要求。独立审核小组确定的要求（如果有）在附件 B 中列出。

2) 在向数据接收方披露受限制数据集前，数据提供方应根据国家法律法规以及相关的国家标准对数据接收方要求的数据进行去标识化处理，并且该等去标识化的过程应至少去除如下的个人标识信息。数据提供方内部参与去标识化的个人须来自独立的部门，不得有与本协议有关的人员参与。

个人可识别信息种类	姓名、工作单位、地址（工作地址或者住宅地址）、手机号码、邮箱（工作邮箱或者私人邮箱）、银行账号、支付宝账号、微信账号、社保账号、身份证号码、医院住院卡账号、驾驶证账号、车牌号码、个税号码、IP 地址、手机 Device ID、生物可识别信息（用于识别目的，例如指纹、声纹等）、人脸照片

3) 基于本协议，数据接收方不得将接收到的数据用于协议外的其他任何目的，包括但不限于：
   a) 对数据集中个体进行重标识；
   b) 与外部数据集或信息进行关联。

保密以及数据保护义务条款

1) 数据接收方同意仅将数据提供方保密信息以及受限制数据集用于实现目的以及其他相关的义务。未经数据提供方的事前书面允许，数据接收方不得将根据本协议或者在履行本协议过程中获得的受限制数据集以及数据提供方保密信息再进一步披露给任何第三方。数据接收方可以将数据提供方保密信息以及受限制数据集传输作为数据使用的一部分、代表数据接收方或为其提供服务的处理者，但该等传输仅在数据提供方出具书面确认，并且数据接收方确保该等处理者至少受到与本协议中的保密规定同等约束的情况下才被允许。

2) 本条第 1）款规定的保密义务和使用限制不适用于如下信息：
   a) 除违反本协议外，已公开或可公开获得的信息；

b) 数据接收方可以证明其数据提供方在依据本协议进行披露之前数据接收方已拥有或独立开发的信息；
c) 数据接收方从非法律上禁止披露此类信息的第三方收到的信息；
d) 法律要求数据接收方披露，前提是数据提供方被告知任何此类要求，并有足够的时间寻求保护令或对要求进行其他修改。

3) 除非获得数据提供方的事先书面同意，数据接收方同意其不会尝试重新识别或联系数据集中包含的主体。此外，数据接收方同意不尝试重新识别研究中的参与者以及其他可以根据本协议提供的（包括但不限于临床研究人员和参与者的亲属）研究数据中可被识别的人。数据接收方进一步同意不以可能导致识别任何个人的方式将访问数据与其他数据源相结合。本条规定的义务此后继续有效并无限期延长。

4) 本条的义务在本协议终止后后的六（6）年内有效，法律另有规定的，以法律规定的保存期限为准。

5) 数据接收方同意使用合适、适当并且必要的安全措施来防止使用或披露受限制数据集以及数据提供方保密信息，包括但不限于：

a) 实施管理、物理和技术保护措施，合理适当地保护其代表数据提供方处理、接收、维护或传输的受限制数据集和数据提供方保密信息的保密性、完整性和可用性；
b) 确保任何向其提供此类受限制数据集的数据适用者（包括任何其分包商或者供应商）同意实施合理和适当的保护措施来保护此类信息；
c) 其他法律法规或者国家标准要求使用者（包括任何其的分包商或者供应商）应采取的管理、物理和技术保护措施。

6) 数据接收方同意，如果在使用受限制数据集的过程中发现任何数据泄露事件，将立即通知数据提供方。数据接收方同意数据提供方可以对数据泄露事件采取措施，包括通知监管机构或医疗服务提供者，或以其他方式对数据泄露事件进行处理。

7) 数据接收方同意，如果在使用或披露受限制数据集的过程中违反本条所列数据保护义务，导致数据提供方遭受侵权指控、处罚或其他不利后果的，数据接收方应向数据提供方赔偿其因此承担的全部损失、成本、支出（包括合理的法律支出）或责任等。

8) 数据提供方有权在如下的任何情形下单方终止本协议：
a) 数据接收方违反本协议的规定；
b) 数据接收方因为未采取相应的管理、物理和技术保护措施导致数据泄露或者导致被政府调查或者行政处罚；或者
c) 数据接收方在使用受限制数据的过程中发生了数据泄露事件。

9) 双方承认并同意，向数据接收方提供受限制数据集的前提条件是本协议具有完全效力。因此，在本协议终止后，双方同意数据提供方将不再向数据接收方提供受限制数据集，并且数据接收方将不会继续使用该等受限制数据集。本协议终止后，数据接收方同意及时返还或销毁所有受限制数据集以及数据提供方保密信息（包括数据接收方已向其处理者及其供应商披露的任何受限制数据

集，除非其已进行了完全的匿名化处理或销毁，并出具书面的证明）。如果无法返还或销毁部分或全部受限制数据集，数据接收方将继续将本协议的保护范围扩展至未归还或销毁的此类受限制数据集信息。本协议项下的任何到期或终止后，该条义务将继续有效。

协议附件

附件A：受限制数据集使用计划

【备选条款：附件B：独立审核小组要求】

附 录 F
（资料性附录）
健康医疗数据安全检查表

表 D.1 给出了健康医疗数据安全检查表，可用于控制者进行健康医疗数据安全工作自查。“是”和“否”分别表示是否采取了相应的安全控制措施，“备注”用于记录未采取相应安全措施的替代方案或整改计划或者不适用情况说明等。

表 D.1 健康医疗数据安全检查表

安全措施	是	否	备注
使用披露			
非医疗目的使用数据，是否获得主体同意？			
非医疗目的使用，获取主体授权，是否明确了用途、使用的方式、到期日期、法定权利、以及控制者采取的保护措施等具体信息？			
非医疗目的使用数据是否限定在与个人授权的用途具有直接或合理关联的范围内？			
超出授权范围使用数据，是否再次征得主体同意？			
未经个人主体授权的受限制数据是否仅限于科学研究、医学/健康教育、公共卫生或医疗保健操作目的？			
未经个人主体授权的受限制数据使用是否经过了相关委员会审批？			
未经个人主体授权的受限制数据使用是否严格限制在有权使用人员范围？			
进行市场营销活动的数据使用是否获得了个人主体授权？			
市场营销活动的数据使用是否书面告知个人主体相关权利例如撤销授权？			
是否将市场目的的数据使用授权独立，未作为主体获得任何公共服务、医疗服务或者捆绑于其他的服务条款之中？			
是否应主体要求披露其相关信息？			
是否提供了允许主体或其授权代表访问其数据的方式？			
是否提供了允许主体复查并获得其数据副本的方式？			
是否为主体提供请求更正或补充信息的方法？			
是否提供了允许主体回溯查询其数据使用披露情况的方式？			
是否支持主体最少回溯 6 年查询其数据使用披露情况？			
和个人主体关于数据访问使用另有约定的，是否按照约定执行？除非法律法规要求以及医疗紧急情况。			
未经个人授权使用治疗笔记用于内部培训或学术研讨，是否进行了必要的去标识化处理？			
引入处理者代为或帮助处理数据是否确认其具备相应数据安全能力？			
引入处理者代为或帮助处理数据是否通过协议对数据处理相关工作进行了约定，包括明确了安全责任？			
数据处理结束是否确认处理者未留存数据？			
向政府授权的第三方控制者传送数据前，是否获得加盖政府公章的相关文件？			
数据使用申请审批中是否确认了数据使用的合法性、正当性和必要性？			
数据使用申请审批中是否确认了相应数据安全能力？			
数据交付第三方使用是否通过协议约定了目的、安全责任和安全要求？			
数据使用结束后是否确认数据已彻底销毁？			

表 D.1　健康医疗数据安全检查表

安全措施	是	否	备注
数据聚合结果的发布是否经过数据安全委员会审批？			
境外传送数据是否经过了数据安全委员会评审或者得到个人主体授权？			
境外传送数据是否确保其不属于重要数据或涉密数据？			
境外传送数据是否限定在 250 条以内？			
境外传送数据是否仅限于个人主体授权或者学术研讨？			
境外传送数据必要时是否提请相关部门审批？			
不能识别个人的健康医疗数据使用是否符合重要数据管理相关要求？			
是否确定数据没有存储在境外的服务器上？			
是否确定没有租赁、托管境外的服务器？			
生物识别信息的存储是否经过了处理，例如只存储了摘要？			
健康医疗数据的传输是否进行了加密处理？			
使用介质进行健康医疗数据传输的，是否对介质使用进行了管控？			
涉及人类遗传资源数据的，是否经过了相关部门审批？			
涉密数据是否符合涉密信息系统分级保护的管理规定和技术标准？			
安全技术			
是否对健康医疗数据进行分类分级管理？			
是否制定并实施了合理的策略和流程，将使用和披露限制在最低限度？			
受否对登录的用户进行身份标识和鉴别，身份标识具有唯一性，鉴别信息具有复杂度要求并定期更换？			
是否具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施？			
当进行远程管理时，是否采取了必要措施，防止鉴别信息在网络传输过程中被窃听？			
是否对登录的用户分配了账户和权限？			
是否重命名或删除默认账户，修改默认账户的默认口令？			
是否及时删除或停用多余的、过期的账户，避免共享账户的存在？			
是否授予管理用户所需的最小权限，实现管理用户的权限分离？			
是否启用安全审计功能，并覆盖到每个用户，对重要的用户行为和重要安全事件进行审计？			
审计记录是否包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息？			
是否对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等？			
是否基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警？			
是否遵循最小安装的原则，仅安装需要的组件和应用程序？			
是否关闭了不需要的系统服务、默认共享和高危端口？			
是否通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制？			
是否提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求？			
是否能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞？			

表 D.1　健康医疗数据安全检查表

安全措施	是	否	备注
是否安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库？			
是否采用校验技术保证重要数据在传输过程中的完整性？			
是否提供重要数据的本地数据备份与恢复功能？			
是否提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地？			
是否保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除？			
是否仅采集和保存业务必需的用户个人信息？			
是否禁止未授权访问和非法使用用户个人信息？			
采购的云服务是否通过了云安全审查？			
自建云是否按云安全审查标准进行了安全保护？			
是否按照规划、开发、部署到运维的系统生命周期各阶段特点采取了必要的安全管控措施？			
是否采用密码技术保证数据在传输和存储过程中的保密性？			
密码技术使用是否符合国家密码管理相关要求？			
数据出境是否进行了出境安全评估？			
是否满足重要数据管理、关键信息基础设施安全管理等政策的相关通用要求？			
去标识化			
去标识化数据是否只应用于受控公开共享或领地公开共享？			
领地公开共享的安全环境是否得到评估确认？			
是否通过数据使用协议约定数据使用目的、期限等？			
去标识化策略、流程和结果是否由数据安全委员会审批？			
是否去除可以唯一识别到个人的信息或披露后会给患者造成重大影响的信息？			
模糊化后仍有医学意义的数据是否进行了模糊化处理，例如泛化？			
是否删除医护人员姓名以及其他身份标识信息？			
数据集中所有属性值相同的人数是否最低在 5 人以上？			
对需要追溯到患者的情况，是否由控制者内部建立患者代码索引？			
去标识化过程中使用的各种参数配置，例如时间漂移范围、患者代码索引、各种个人代码生成规则等是否严格保密，仅限于控制者内部专人管理？			
在需要进行重标识确定主体时，是否只能由控制者内部专人处理，处理过程严格保密？			
去标识化使用者是否没有参与去标识化相关工作？			
在受控公开共享模式下，数据接收者是否具备数据使用情况审计的能力，并接受控制者审计？			
安全管理			
是否建立健康医疗数据安全委员会并对健康医疗数据安全工作全面负责，讨论决定健康医疗数据安全重大事项？			
委员会是否包含组织高层管理人员和各业务口负责人？			
委员会是否涵盖信息安全、伦理、法律、统计、审计、保密等相关专业人员？			
委员会负责人是否由组织最高负责人担任？			
委员会是否每月至少开一次会？			
是否指定专人负责健康医疗数据安全日常工作？			

表 D.1　健康医疗数据安全检查表

安全措施	是	否	备注
是否有明确的健康医疗数据安全工作范围界定？			
是否建立了健康医疗数据安全策略？			
是否建立了数据安全相关规章制度？			
是否建立了数据使用审批流程？			
相关机构、负责人、策略、制度、流程等是否通告全组织？			
是否进行了必要的元数据管理？			
是否进行了数据或系统供应链管理？			
是否明确了去标识化的策略和流程？			
是否建立了健康医疗数据安全风险评估方案？			
是否梳理清楚健康医疗数据相关业务及涉及的系统和数据？			
是否可以识别健康医疗数据安全风险并评估影响？			
是否评审并通过风险处置方案？			
是否配备了适当的资源，包括人力、物力、资金，支撑健康医疗数据安全工作开展？			
是否开展必要的信息安全教育、培训和考核？			
是否对开展的信息安全工作和投入信息安全工作的各项资源实施有效的管控？			
是否针对信息安全事件有有效应对措施？			
对选定的安全措施的实施过程是否有监管流程？			
是否定期评审风险处置方案实施的有效性，包括评估实施相应安全措施后剩余风险的可接受程度等？			
是否根据情况定期实施自查，或是请第三方检查机构进行检查？			
自查每年是否至少全面覆盖 1 次？			
是否将检查过程纳入监管？			
是否会根据检查结果建立针对性的整改计划，并按计划实施？			
是否制定应急预案。应急预案应包括启动应急预案的条件、应急处理流程、系统恢复流程、事件报告流程、事后教育和培训等内容？			
是否对网络安全应急预案定期进行评估修订？			
是否每年至少组织 1 次应急演练？			
是否有专门的网络安全应急支撑队伍及专家队伍，保障安全事件得到及时有效处置？			
是否制定灾难恢复计划，确保健康医疗信息系统能及时从网络安全事件中恢复，并建立安全事件追溯机制？			
如果发生网络安全事件，是否按应急预案进行处置？			
如果发生网络安全事件，事件处置完成后是否及时按规定向主管监管部门书面报告事件情况，内容应至少包括：事件描述、原因和影响分析、处置方式等信息？			
是否就健康医疗数据使用情况进行审计，并适时调整改进安全措施？			
是否监测预警数据安全状态，并实施调整改进安全措施？			

参 考 文 献

[1] U.S. Department of Health & Human Services, Security Rule Guidance Material, https://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html, 2018.10.31.

[2] 国家卫生健康委员会, 国家中医药管理局, 关于印发互联网诊疗管理办法（试行）等3个文件的通知, 2018年7月17日.

[3] 国家卫生健康委员会, 国家健康医疗大数据标准、安全和服务管理办法（试行）, 2018年7月12日.

[4] General Data Protection Regulation, 2018.5.25.

[5] 国务院办公厅, 国务院办公厅关于促进“互联网+医疗健康”发展的意见, http://www.gov.cn/zhengce/content/2018-04/28/content_5286645.htm, 2018年04月28日.

[6] Data in the EU: Commission steps up efforts to increase availability and boost healthcare data sharing, http://europa.eu/rapid/press-release_IP-18-3364_en.htm, 2018.4.25.

[7] 国务院办公厅, 科学数据管理办法, http://www.gov.cn/zhengce/content/2018-04/02/content_5279272.htm, 2018年3月17日.

[8] 何晓琳. 健康医疗可穿戴设备数据安全与隐私保护问题研究[D]. 北京协和医学院, 2017.

[9] 赵新蓉. 在健康数据助推健康产业发展环境下医疗数据安全开放应用框架研究[D]. 北京协和医学院, 2017.

[10] 中华人民共和国全国人民代表大会常务委员会, 中华人民共和国网络安全法, 2017年6月1日.

[11] 全国信息安全标准化技术委员会秘书处，关于开展国家标准《信息安全技术 数据出境安全评估指南（草案）》征求意见工作的通知，https://www.tc260.org.cn/front/postDetail.html?id=20170527173820，2017年5月27日.

[12] 国家互联网信息办公室，个人信息和重要数据出境安全评估办法（征求意见稿），http://www.cac.gov.cn/2017-04/11/c_1120785691.htm，2017年4月11日.

[13] GB/T 22081—2016 信息技术 安全技术 信息安全控制实践指南，2017年3月1日.

[14] 国家卫生计生委办公厅, 国家中医药管理局办公室, 电子病历应用管理规范（试行）, 2017年2月15日.

[15] 国家卫生计生委, “十三五”全国人口健康信息化发展规划, 2017年1月24日.

[16] 中共中央 国务院印发《“健康中国2030”规划纲要》, http://www.gov.cn/zhengce/2016-10/25/content_5124174.htm, 2016年10月25日.

[17] 国家卫计委，涉及人的生物医学研究伦理审查办法，http://www.gov.cn/gongbao/content/2017/content_5227817.htm，2016年10月12日.

[18] 食品药品监管总局，总局关于发布临床试验数据管理工作技术指南的通告，https://www.cfdi.org.cn/resource/news/8011.html，2016年7月27日.

[19] 食品药品监管总局，总局关于发布药物临床试验数据管理与统计分析的计划和报告指导原则的通告，https://www.cfdi.org.cn/resource/news/8012.html，2016年7月27日.

[20] 食品药品监管总局，总局关于发布临床试验的电子数据采集技术指导原则的通告，https://www.cfdi.org.cn/resource/news/8013.html，2016年7月27日.

[21] ISO 27799:2016 Health informatics -- Information security management in health using ISO/IEC 27002, 2016.7.

[22] 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, http://www.gov.cn/zhengce/content/2016-06/24/content_5085091.htm, 2016年06月24日.

[23] 国家食品药品监督管理局，国家卫生和计划生育委员会，医疗器械临床试验质量管理规范，https://www.cmde.org.cn/CL0020/5511.html，2016年6月1日.
[24] 科技部，关于发布《人类遗传资源采集、收集、买卖、出口、出境审批行政许可事项服务指南》的通知，http://www.most.gov.cn/tztg/201507/t20150703_120547.htm，2015年07月03日.
[25] Office of the National Coordinator for Health Information Technology (ONC)，Guide to Privacy and Security of Electronic Health Information，https://www.healthit.gov/sites/default/files/pdf/privacy/privacy-and-security-guide.pdf, 2015.4.
[26] Article 29 Working Party a letter that responds to a request of the European Commission to clarify the scope of the definition of health data in connection with lifestyle and wellbeing apps. https://ec.europa.eu/justice/article-29/documentation/other-document/files/2015/20150205_letter_art29wp_ec_health_data_after_plenary_annex_en.pdf, 2015.2.5.
[27] 国家卫生计生委,国家中医药管理局, 关于加强医疗卫生机构统方管理的规定, 2014年11月20日.
[28] 国家卫生计生委, 国家卫生计生委关于推进医疗机构远程医疗服务的意见, 2014年8月21日.
[29] 国家卫生计生委, 人口健康信息管理办法（试行）, 2014年5月5日.
[30] 国家卫生和计划生育委员会、国家中医药管理局，国家卫生计生委、国家中医药管理局关于印发加强医疗卫生行风建设“九不准”的通知，2013年12月26日.
[31] 国家卫生计生委、国家中医药管理局，医疗机构病历管理规定， 2013年11月20日.
[32] 中华人民共和国全国人民代表大会常务委员会，中华人民共和国消费者权益保护法，http://www.npc.gov.cn/npc/xinwen/2013-10/26/content_1811773.htm，2013年10月25日.
[33] 中华人民共和国工业和信息化部，电信和互联网用户个人信息保护规定，http://www.miit.gov.cn/n1146285/n1146352/n3054355/n3057724/n3057729/c4700145/content.html ，2013年9月1日.
[34] 中华人民共和国全国人民代表大会常务委员会，中华人民共和国精神卫生法，http://www.gov.cn/flfg/2012-10/26/content_2253975.htm，2013年5月1日.
[35] 全国人民代表大会常务委员会，全国人民代表大会常务委员会关于加强网络信息保护的决定，http://www.gov.cn/jrzg/2012-12/28/content_2301231.htm，2012年12月28日.
[36] 国务院法制办公室，国务院法制办公室关于《人类遗传资源管理条例（送审稿）》公开征求意见的通知，http://www.gov.cn/gzdt/2012-10/31/content_2254379.htm，2012年10月30日.
[37] 卫生部，卫生部关于印发《卫生行业信息安全等级保护工作的指导意见》的通知，http://www.gov.cn/gzdt/2011-12/09/content_2016113.htm，2011年12月09日.
[38] 卫生部，健康体检管理暂行规定，http://www.gov.cn/zwgk/2009-08/21/content_1398269.htm，2009年8月5日.
[39] NIST SP 800-66 Rev. 1, An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule, 2008.10.
[40] 国务院，艾滋病防治条例，http://www.gov.cn/ziliao/flfg/2006-02/12/content_186324.htm，2006年3月1日.
[41] 科技部，人类遗传资源管理暂行办法，http://www.most.gov.cn/bszn/new/rlyc/wjxz/200512/t20051226_55327.htm，2005年12月26日.
[42] 全国人民代表大会常务委员会，中华人民共和国传染病防治法，http://www.gov.cn/banshi/2005-08/01/content_19023.htm，2004年12月1日.
[43] 国家食品药品监督管理局，医疗器械临床试验规定，https://www.cmde.org.cn/CL0094/2231.html，2004年4月1日.

[44] 全国人民代表大会常务委员会，中华人民共和国居民身份证法，http://www.npc.gov.cn/wxzl/gongbao/2011-12/30/content_1686368.htm，2004年1月1日.
[45] 中华人民共和国全国人民代表大会常务委员会，中华人民共和国执业医师法，http://www.gov.cn/banshi/2005-08/01/content_18970.htm，1999年5月1日.
[46] 全国人民代表大会常务委员会，中华人民共和国母婴保健法，http://www.npc.gov.cn/wxzl/gongbao/2000-12/05/content_5004627.htm，1995年6月1日.
[47] 国务院，医疗机构管理条例，http://www.gov.cn/banshi/2005-08/01/content_19113.htm，1994年9月1日.
[48] 卫生部，性病防治管理办法，http://www.gov.cn/banshi/2005-08/02/content_19262.htm，1991年8月12日.