ICS 33.040.40
CCS L78

DB1310

廊 坊 市 地 方 标 准

DB 1310/T 338—2024

数字乡村 县域医疗机构网络数据安全管理规范

2024－06－28 发布　　2024－07－28 实施

廊坊市市场监督管理局　　发 布

前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

本文件由中共廊坊市委网络安全和信息化委员会办公室提出。

本文件起草单位：廊坊市人民医院、中共廊坊市广阳区委网络安全和信息化委员会办公室、中共廊坊市安次区委网络安全和信息化委员会办公室、廊坊市市场监督管理局、中国软件与技术服务有限公司、河北东方学院、中国移动通信集团河北有限公司廊坊分公司、中国电信集团有限公司廊坊分公司、中国联合网络通信有限公司廊坊分公司、中国广电河北网络股份有限公司廊坊市分公司、润泽科技发展有限公司、河北兰科网络工程集团有限公司。

本文件主要起草人：刘顺海、王栩、刘朔、高继伟、穆学武、苏玉军、马群、郭睿、赵志滨、刘欣羽、刘安然、提文英、张健飞、焦跃振、张海付、张建平、李时、李晓英。

数字乡村 县域医疗机构网络数据安全管理规范

1 范围

本文件规定了县域医疗机构网络数据安全管理的安全管理要求、数据处理活动要求、安全运营要求和应急管理要求。

本文件适用于廊坊市各县（市、区）、廊坊开发区域内医院、中医院、妇幼保健院等二级（及以下）医疗机构的网络数据安全日常管理工作。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 25069 信息安全技术 术语

GB/T 35273 信息安全技术 个人信息安全规范

GB/T 37988 信息安全技术 数据安全能力成熟度模型

GB/T 43697 数据安全技术 数据分类分级规则

3 术语和定义

GB/T 25069、GB/T 35273、GB/T 37988和GB/T 43697界定的以及下列术语和定义适用于本文件。

3.1

数据

任何以电子或者其他方式对信息的记录。

3.2

网络数据

网络空间中产生、存储、传输和处理的数据。

3.3

核心数据

对领域、群体、区域具有较高覆盖度或达到较高精度、较大规模、一定深度的，一旦被非法使用或共享，可能直接影响政治安全的重要数据，主要包括关系国家安全重点领域的数据，关系国民经济命脉、重要民生、重大公共利益的数据，经国家有关部门评估确定的其他数据。

3.4

一般数据

核心数据、重要数据之外的其他数据。

3.5

个人信息

以电子或者其他方式记录的与已识别或者可识别的自然人有关的各种信息，不包括匿名化处理后的信息。

3.6

网络数据处理者

在数据处理活动中自主决定处理目的、处理方式的组织、个人。

3.7

数据活动

组织、机构针对数据开展的一组特定任务的集合，数据活动主要包括收集、存储、使用、加工、传输、提供、公开等。

3.8

数据提供

数据提供是指机构在数据管理过程中，向其他机构或个人提供所需的数据支持和服务。

3.9

监测预警

对数据安全状态进行实时监测，并对可能发生的威胁进行预警的过程。

3.10

数据安全

通过采取必要措施，确保数据处于有效保护和合法利用的状态，以及具备保障持续安全状态的能力。

4 总体要求

统筹规划、统一策略、分级建设，构建一体化网络数据安全保障体系，将数据安全能力贯穿于医疗机构数据管理的各领域和全过程，实现数据可知、风险可视、安全可控、问题可追。

5 安全管理要求

5.1 制度管理

5.1.1 应建立健全数据安全保护制度体系，明确机构对数据的态度、保护数据的责任以及处理数据的安全措施，确保数据的合规性、隐私性、完整性和可用性。

5.1.2 应至少包含数据安全管理、数据分类分级保护、数据安全风险评估、数据安全应急处置、数据安全培训 5 个部分。

5.1.3 应定期对数据安全管理制度的合理性和适用性进行论证和审定，对存在不足或需要改进的制度进行修订。

5.2 人员管理

5.2.1 应设立数据安全管理部门，明确数据安全责任人，落实数据安全保护责任，保障数据安全工作正常开展。

5.2.2 应建立完善的数据安全培训体系，提高员工的数据安全意识和技能水平，增强机构的数据安全保障能力。

5.2.3 应定期开展数据安全审计工作。

5.2.4 人员离任后，应及时回收相应的管理权限，并确保完成工作交接。

5.3 合作方管理

5.3.1 应建立对合作方的遴选、管理、监督、评价机制。
5.3.2 应与合作方签订合作协议，协议中明确规定双方在网络数据安全和日常行为等方面的责任和义务，确保合作过程中不发生任何违反法律法规或损害对方利益的行为，同时加入保密要求相关条款。
5.3.3 应对合作方的安全能力进行评估，对合作方履行安全责任义务的情况进行监督和检查，每年不低于一次审核合作方资质背景、网络数据安全保障能力等。
5.3.4 合作方应保证接入的系统、接入方式、使用的技术工具的安全。
5.3.5 合作方应在合作结束后，清除相关权限和介质，按要求对数据进行妥善处理，遵守保密义务。

5.4 分类分级

5.4.1 应明确数据分类标准，依据数据资源属性特征，将数据合理划分类别。
5.4.2 在分级时，应考虑数据的敏感度和重要性，以及医疗机构对数据的依赖程度等因素，制定相应的保护措施。
5.4.3 应定期评审数据对象的类别和级别，如需变更数据所属类型或级别，应在履行相应的变更审批流程后进行变更。

5.5 个人信息保护

5.5.1 应指定专人对个人信息进行处理，承担接收、存储等相关环节数据和个人信息安全的指导监督、督促检查责任。
5.5.2 传输和存储敏感个人信息时，应采用加密等安全措施，禁止未授权访问和非法使用用户个人信息。
5.5.3 内部人员不得以非工作原因查询、使用个人信息，防止造成信息泄露。
5.5.4 涉及公开展示个人信息的，应对展示的个人信息采取去标识化处理等措施，降低个人信息在展示环节的泄露风险。
5.5.5 个人信息保存期限应为实现目的所必需的最短时间，超出保存期限后，应对个人信息进行删除或匿名化处理。
5.5.6 在境内收集和产生的重要数据和个人信息，应当在境内存储。因业务需要确需向境外提供的，应通过网信部门组织的安全评估，获得专业机构进行个人信息保护认证，并应符合相关法律法规。

6 数据处理活动要求

6.1 数据收集

6.1.1 应明确目的和范围、确定数据来源、规范流程、确保安全性和保密性。
6.1.2 收集外部数据前，应确保收集的数据不含有恶意代码或恶意软件。
6.1.3 应建立数据管理和监控手段，对发现的异常数据及时处置。
6.1.4 应及时更新和维护收集到的数据，及时删除过期信息。
6.1.5 通过人工方式收集数据时，应对数据收集人员严格管理，保证将收集到的数据直接报送至相关人员或系统，收集任务完成后及时删除采集人留存的数据。

6.2 数据存储

6.2.1　数据存储管理应建立完善的备份和恢复机制，确保数据的可靠性和可用性。
6.2.2　应采取合适的技术和措施，如数据备份、数据恢复、加密等，确保数据的完整性和安全性。在选择存储介质时，需要考虑其可靠性、可扩展性和性能等因素。
6.2.3　应符合相关法规的要求，包括数据保护、隐私管理和数据安全等方面。
6.2.4　应定期进行数据备份与恢复，确保能够在必要时迅速恢复。

6.3　数据使用

6.3.1　应明确数据使用的目的、范围、审批流程、人员岗位职责等，在保证安全的条件下开展数据的使用。
6.3.2　应遵循数据安全和隐私保护的原则，基于合法的授权和权限控制，并获得必要的授权和许可。
6.3.3　仅在获得合法的数据许可和使用权的情况下使用数据。遵守数据提供方的规定和约束，不得超越许可范围进行数据的使用。
6.3.4　应建立数据跟踪和审计机制，以监测和控制数据的访问和使用，及时发现和处理异常行为。
6.3.5　应建立数据使用策略，明确访问控制和权限分配。

6.4　数据传输

6.4.1　应确保数据的完整性和安全性，满足传输速度和效率的要求。
6.4.2　在选择传输协议和加密方式时，应考虑数据的重要性和敏感性，定期更新加密协议和轮换密钥。
6.4.3　应对数据的传输进行监控和管理，以防止未经授权的数据访问和使用。
6.4.4　应对敏感数据的传输进行额外的身份验证和授权。
6.4.5　应采用校验技术保证数据在传输过程中的完整性。
6.4.6　应建立数据传输日志，以便于监控数据传输活动的安全与合规。

6.5　数据提供

6.5.1　提供的数据应符合法律法规和相关政策要求，提供给第三方之前，应取得数据提供方的同意或授权。
6.5.2　应明确可开放数据的用途和范围，完善各敏感程度数据的开放管理规定。
6.5.3　应与公共数据使用单位签署相关协议，明确数据使用目的、供应方式、保密约定、共享范围和数据保护要求等内容。
6.5.4　应采取必要的授权和权限控制措施，确保数据的合法使用和保护个人隐私。
6.5.5　应采用国家相关标准规定的密码技术，保障数据共享过程的保密性和完整性。

6.6　数据公开

6.6.1　数据公开前应采取严格的隐私保护和安全管理措施，包括数据脱敏、数据审核、数据控制、数据匿名化和防截屏技术等，确保数据公开的安全性和合规性。
6.6.2　对非涉密但涉及敏感信息的公共数据，按照国家有关规定，进行脱敏、清洗处理后向社会公开。
6.6.3　数据公开时，需要注意保护个人隐私和敏感信息。对于包含个人身份信息的数据，进行脱敏处理或其他隐私保护措施，以防止个人信息的泄露。
6.6.4　包含但不限于以下数据不得公开：

——涉及国家秘密、工作秘密等重要数据不得公开；
——涉及个人隐私等敏感数据，未经被收集者同意不得公开；

——已公开数据不得含有相关法律法规定义的违禁内容。

6.7 数据销毁

6.7.1 应建立数据销毁相关工作方案，包括定期审查、使用安全销毁方法、建立销毁规程、及时销毁控制的数据、要求合作方销毁数据、及时删除数据等流程。
6.7.2 应在中国境内对介质存储的数据进行销毁或删除，采取无法恢复的方式进行数据销毁与删除，并按照规定执行个人信息删除操作等。
6.7.3 信息系统存储介质需要外送维修或者直接报废的，应先进行存储数据检查过程，对于检查发现存储有重要业务数据的，应在条件允许的情形下首先执行数据清除作业。
6.7.4 因客观原因确实无法清除的(如访问失败等)，应经维修单位或带出人员签订数据保密承诺书、明确数据保密义务和泄密责任后方可送出。

6.8 数据委托

6.8.1 委托他人处理网络数据时应履行审批手续和监督受托方数据安全保护义务。受托方应依照法律、法规的规定和合同约定履行数据安全保护义务，不得擅自留存、使用、泄露或者向他人提供数据。
6.8.2 委托方应定期审查受托方的数据保护措施等，确保符合法律要求和双方约定。

6.9 数据出境

6.9.1 应评估数据出境的风险和影响，采取必要的安全措施和管理办法，确保个人隐私和单位的信息安全。
6.9.2 在数据出境过程中，应对数据进行必要的加密和保护措施，防止数据泄露和滥用。

7 安全运营要求

7.1 风险评估

7.1.1 应对数据及相关系统面临的安全威胁和潜在风险进行评估和识别，制定相应的防范措施和应对策略。
7.1.2 通过对数据的保密性、完整性和可用性进行评估，以及对系统面临的威胁、攻击和漏洞进行识别和分析，帮助机构了解其数据安全现状，制定相应的安全策略和措施，提高数据安全保障能力。

7.2 监测预警

7.2.1 通过对数据采集、传输、存储和处理等环节进行实时监控，对威胁进行分析和预警，帮助机构及时发现并应对潜在的安全威胁，防止数据泄露、篡改或丢失等安全事件的发生。
7.2.2 应建立数据安全风险监测预警机制，制定合理有效的风险监测指标。

7.3 风险处理

7.3.1 应制定和不断完善相关的网络数据安全风险处置方案和信息通报机制，在发生网络数据安全风险时迅速响应，及时处置，及时通报。
7.3.2 应建立事件监测和预警机制，对潜在的网络数据安全威胁进行监控，并根据不同级别的预警采取相应的预警响应措施。
7.3.3 在事件处理结束后，应对事件进行回顾分析，总结经验，并对预防措施和处置流程进行优化

8 应急管理要求

8.1 应急预案

8.1.1 应制定本地网络数据安全应急预案，并明确启动条件，包括应急处理流程、系统恢复流程、个人数据恢复和敏感数据恢复等方面的详细内容。

8.1.2 应急预案应包括应急组织构成、资源保障、处置流程、事后的教育与培训等方面核心内容。

8.1.3 应定期对系统相关人员进行应急预案培训，并定期进行应急预案的模拟演练。

8.1.4 应定期对应急预案进行重新评估，并对其进行修订和完善。

8.2 应急处置

8.2.1 应急组织

8.2.1.1 应建立应急组织，包括决策层、指挥层和执行层，各层级应职责明确，相互配合。

8.2.1.2 在应急处置过程中，应加强与各相关部门的协调，确保信息畅通，资源共享。

8.2.2 应急预案启动

8.2.2.1 发生网络数据安全事件时应立即启动应急预案，采取相应的应急处置措施，及时告知相关权利人，并按照有关规定向相关行业主管部门报告。

8.2.2.2 在应急预案启动后，应急组织应迅速展开处置工作。应根据突发事件的具体情况，采取相应的处置措施。在处置过程中，应加强信息报告和沟通，及时反馈进展情况，以便于决策层做出正确的判断和决策。

8.3 总结和评估

在突发事件处置完成后，应进行总结和评估。分析事件发生的原因、影响范围、损失程度以及应急处置的效果等。总结经验教训，提出改进措施，不断完善应急处置管理体系。