郑州澍青医学高等专科学校文件

校字〔2022〕34号

郑州澍青医学高等专科学校
数据安全与个人信息保护管理办法（试行）

第一章　总则

第一条　为加强学校网络与信息安全，规范数据管理，保护学校重要数据和个人信息，切实维护广大师生的合法权益，根据《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》等相关法律法规及《信息安全技术个人信息安全规范（GB/T　35273-2020）》等相关国家标准，按照《河南省教育厅办公室关于加强学生信息安全工作的通知》等相关文件要求，结合学校网络与信息安全工作实际，制定本办法。

第二条 适用范围。校内各单位通过信息化手段开展数据收集、存储传输、处理使用等活动（以下简称“数据活动”），以及数据安全的保护和监督管理，适用本办法。

涉及国家秘密信息的数据安全管理，按照国家相关标准和规定执行；非信息化手段采集的数据可参考本办法执行。

本办法所指各单位包括学校各系部、处室、附属医院等单位。

第三条 基本原则。本办法遵循安全合规、分级保护、最少够用、优先共享的原则，从管理和技术两个维度，重点保障个人信息安全，全面提高学校数据安全保障能力；并按照“谁主管谁负责、谁运维谁负责、谁使用谁负责”的原则，建立健全网络与信息安全责任体系。

第二章 管理机构与职责

第四条 网络安全和信息化领导小组是数据安全与个人信息保护工作的领导机构，主要职责是贯彻落实上级有关部门关于数据安全与个人信息保护工作的发展战略、宏观规划、重大政策和工作部署，统一领导、统一谋划、统一部署学校的数据安全与个人信息保护工作，统筹协调和决策学校数据安全与个人信息保护工作中的重大问题等。

第五条 信息管理中心负责组织落实网络安全和信息化领导小组的各项决议与工作部署，研究制定数据安全与个人信息保护工作发展规划、工作计划、规章制度和标准规范，建立覆盖数据采集、存储传输、处理使用、开放共享等全生命周期的数据安

全保障和监督检查机制，协调处理数据安全重大突发事件有关应急工作等。

第六条 各单位党政负责人是本单位数据安全与个人信息保护工作第一责任人，同时按照“谁收集，谁负责”、“谁使用，谁负责”、“谁发布、谁负责”的原则责任到人，落实本单位数据安全防护措施，保障数据安全。

第七条 信息管理中心负责组织开展数据安全评估，同时配合信息系统主管单位做好数据中心所承载信息系统的数据安全保障工作。

第三章 数据分级

第八条 学校的数据安全保障遵循分级保护的原则。基于数据重要性、敏感性确定数据级别，根据数据级别明确保障措施。

第九条 根据数据泄露、滥用、篡改、毁损可能对国家安全、社会秩序、学校及个人利益造成的影响程度，将数据分为公开数据、内部数据和敏感数据等 3 类。

1. 公开数据：公开数据是指学校可以主动公开的数据。

2. 内部数据：内部数据是指可在特定范围内无条件共享的数据，包括学校部门间共享和与政府部门间共享。信息管理中心制定学校部门间数据共享责任清单，明确学校部门间应共享的内部数据，制定政府部门数据共享责任清单，明确与政府部门间可共享的内部数据。

3. 敏感数据：敏感数据是指一旦遭泄露或篡改，可能对国家

安全、社会秩序、学校利益、个人人身与财产安全等造成损害的数据，包括个人敏感信息（如身份证信息、个人生物识别信息）及业务敏感数据（如学校人事、财务、科研数据等）。学校对敏感数据实施重点保护，以维护学校数据安全。

第十条 信息系统的使用单位根据数据的重要性、敏感性和对业务的影响程度对现有的数据进行分级。

第四章 数据采集的安全保障

第十一条 未经学校网络安全和信息化领导小组批准，校内任何单位和个人不得以任何理由，私自收集学校范围内的师生、聘用人员等个人信息；各单位未经单位负责人批准，任何人不得以任何理由，私自收集本单位师生、聘用人员等个人信息。

第十二条 数据采集应遵循最小够用原则，明确采集依据、范围、场景和用途，原则上不得超越各单位的工作职能采集数据。

第十三条 新建信息系统应在建设方案中明确数据采集内容和数据等级。由信息管理中心组织相关专家进行建设方案评审，对数据采集的必要性和数据分级的合理性进行审核。

第十四条 各单位对已建信息系统的数据采集项目建立信息资源目录，并报信息管理中心备案，由信息管理中心组织相关专家进行审核，如有新增数据采集项目应及时更新报备信息。

第十五条 各单位按照“一数一源”的原则，优先由学校数据共享平台匹配需求，原则上数据共享平台中已有数据应通过共享的方式获取数据。

第十六条 各单位原则上不得采集学生、家长、教师的个人生物识别信息。采集敏感数据或采集五百以上个人数据需报学校网络安全和信息化领导小组审核批准。

第五章 数据存储传输的安全保障

第十七条 学校的内部数据和敏感数据应保存在学校数据中心，禁止保存在校外数据中心（含云服务平台）；所有数据禁止保存于设置在境外的数据中心。

第十八条 各单位使用的信息系统应根据数据安全级别采用数据加密、访问控制、数据防泄漏等安全措施。个人信息或敏感数据应采用符合国家要求的密码算法进行加密存储。

第十九条 各单位使用的信息系统应制定数据备份恢复策略和操作规范。

第二十条 在线的内部数据和敏感数据传输应采用加密传输信道或专线，以保证数据传输的机密性和完整性；离线的内部数据和敏感数据应加密后传输，且不得使用社会电子邮件系统、聊天平台等方式传递。

第二十一条 根据国家有关数据出入境相关规定，内部数据和敏感数据禁止出境；严格遵守“涉密信息不上网，上网信息不涉密”。

第六章 数据使用处理的安全保障

第二十二条 信息系统使用单位应实现数据管理、数据使用

和数据审计的权限分离；数据管理人员负责分配数据使用权限、按最小化原则授予各级各类人员的相关权限；数据使用人员根据业务和权限需要使用数据；数据审计人员负责对各类人员的数据操作进行审计记录和分析。

第二十三条 学校鼓励在保障数据安全的前提下，充分发掘数据潜在价值。对数据开展统计分析、科学研究、决策分析时，需经业务职能部门同意，且确保不泄露敏感信息。敏感数据使用前应采用适当的脱敏技术进行脱敏处理。

第二十四条 信息系统使用单位应记录对业务数据的查询、修改、增加、删除、导出等操作日志，保留时间不少于180天。

第七章 数据共享公开的安全保障

第二十五条 根据数据分级确认数据共享策略。公开数据的共享和公开工作由网络安全和信息化领导小组办公室统筹负责，共享为原则、不共享为例外，根据相关法规确定公开属性。内部数据的共享由信息管理中心统筹负责，统一由学校网络安全和信息化领导小组办公室负责审核共享需求。敏感数据的共享由信息系统使用单位负责，自行决定是否共享。

第二十六条 内部数据和敏感数据不得用于商业用途。未经网络安全和信息化领导小组办公室同意，禁止与第三方共享。信息发布或共享使用前必须先经过脱敏处理，所有涉及人员身份、联系方式、学生学籍、人事、财务、资产、招生、科研、档案等中含有敏感信息数据的应采用屏蔽、变形、替换等多种手段来满

足不同的隐私数据匿名化的数据合规性。

第二十七条 根据“谁主管谁负责、谁批准谁负责、谁使用谁负责”的原则，信息系统的使用单位应明确本单位所采集数据的安全防护要求。数据共享审核单位负责与被共享单位通过协议等方式确定数据共享范围、用途和安全责任，并将安全防护要求告知被共享单位。被共享单位负责落实数据防护安全，保障数据不被窃取、滥用和篡改。

第二十八条 共享个人信息原则上通过接口方式实现，确需通过拷贝进行共享的，应报本单位领导同意，并由被共享方签订安全承诺书报网络安全和信息化领导小组办公室备案。

第八章 数据库的安全保障

第二十九条 数据库是数据的存储系统，对数据库的攻击是获取数据最为直接的方式，数据库安全风险主要包括拖库、刷库、撞库等，各单位应根据信息系统安全等级和数据级别采用必要的数据库安全防护措施以保障数据库安全。

第三十条 数据库系统原则上不应使用公网 IP 地址部署，如确需使用，应将具体情况说明上报信息管理中心审核，采用公网部署的数据库系统必须采用高强度的安全防护措施以保障数据库安全。

第三十一条 各单位应指定专人负责数据库的安全管理，制定严格的数据库访问控制权限，采用高强度的系统密码策略，检测数据库系统存在的安全问题，对数据库的安全状况进行持续化

监控，保持数据库的安全健康状态。

第三十二条 数据库系统负责人应对数据库系统存在的安全漏洞进行及时修补，以降低数据库攻击风险；同时须定期对数据库访问行为进行审计，对出现的异常访问行为要及时排查和处置。

第九章 自查整改

第三十三条 按照“谁发动采集、谁负责排查”、“谁共享数据、谁负责排查”的原则，各单位定期开展重要数据和个人信息收集与对外共享情况排查工作，做到数据底数清、去向明。数据采集与对外共享过程中，需签署数据安全保密协议，对数据共享和使用范围做出严格界定。

第三十四条 各单位对于自查中发现的问题需要及时整改，认真做好整改落实工作，坚持做到事故原因不查清不放过、整改措施未落实不放过，尽力杜绝类似事件再次发生。

第三十五条 各单位每年度向信息管理中心提交本单位采集、使用数据的情况报告，切实承担起数据安全和个人信息保护的责任与义务，落实本单位数据安全保障措施，提升个人信息保护水平。

第十章 监督检查

第三十六条 信息管理中心负责学校数据安全和个人信息保护工作落实情况的监督检查，建立健全数据安全监督检查机

制，联合相关单位定期组织开展学校数据安全风险评估检查工作，及时发现问题并督促相关部门进行整改。

第三十七条 信息管理中心负责对数据安全检查情况进行全面总结，并报网络安全和信息化领导小组。

第十一章 责任追究

第三十八条 各单位在收到网络安全限期整改通知书后，整改不力的，学校给予通报批评；造成严重安全后果，上级执法部门进行追责处罚的，本单位负责人为第一责任人。

第三十九条 各单位应按照学校网络安全事件应急预案和信息技术安全事件报告与处置流程，在发生网络安全事件时立即采取应急响应措施控制、降低损失，并及时、如实地报告和妥善处置网络安全事件。如有瞒报、缓报、处置和整改不力等情况的，将对本单位予以通报并追究单位负责人的责任。

第四十条 对于各单位所采集、共享的重要数据和个人信息数据，实行单位责任人全周期负责制度。

第十二章 附则

第四十一条 本办法自发布之日起施行，由学校网络安全和信息化领导小组负责解释和修订。

2022 年 6 月 10 日

、

郑州澍青医学高等专科学校校长办公室　2022年6月10日印发