北京融和医学发展基金会

数据隐私安全风险管理制度

第一章 总则

第一条制定目的

为规范网络数据处理活动，保障数据安全，促进数据依法合理利用，保护个人、组织合法权益，依据《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》《网络数据安全管理条例》等法律法规，结合基金会实际，制定本制度。

第二条适用范围

本制度适用于北京融和医学发展基金会所有数据处理活动，包括个人信息的收集、存储、使用、加工、传输、提供、公开、删除等全生命周期管理。

第二章 数据分类分级

第三条数据分级标准

根据数据敏感程度，实行四级分类管理：

绝密级：涉及国家秘密、基金会核心商业秘密或患者敏感医疗信

息的数据；

机密级：涉及捐赠人隐私、科研项目、救助患者核心数据等敏感信息；

秘密级：一般内部工作数据及非敏感个人信息；

公开级：可对外披露的非敏感信息。

第四条标识与管控

1.各类数据应标注明确标识，存储介质、传输通道需匹配相应安全级别；

2.绝密/机密数据访问权限实行分级审批制，仅限授权人员接触。

第三章 数据处理原则

第五条合法正当原则

禁止从事以下行为：

1.窃取、非法获取或交易基金会数据；

2.提供用于非法数据处理的技术工具或服务；

3.明知他人违法仍提供技术支持或协助。

第六条责任主体原则

1.基金会为数据处理主体责任方，承担数据安全法律责任；

2.第三方合作方需签订数据安全协议，明确权利义务及违约责任。

第四章 安全管理措施

第七条技术防护体系

1.实施网络安全等级保护三级标准；

2.部署数据加密（AES-256）、动态脱敏、访问控制（RBAC 型）、日志审计等防护措施；

3.定期开展渗透测试及漏洞修复。

第八条数据生命周期管理

阶段	管理要求
收集	仅采集最小必要数据，明示隐私政策
存储	加密存储于合规云平台，双重备份
使用	基于角色授权（RBAC），操作留痕
共享	敏感数据脱敏处理，履行告知义务
销毁	物理逻辑销毁并行，出具销毁证明

第九条应急响应机制

1.建立三级应急响应体系（蓝-黄-红预警）；

2.数据泄露 4 小时内上报监管部门，24 小时内出具事件分析报告；

第五章 监督与责任

第十条内部监督

1.每年开展合规审计。

2.由专人抽查操作日志和权限管理，重点排查违规下载、越权访问等行为。

第十一条人员管理

1.关键岗位人员签署保密协议，定期开展安全意识培训；

2.对违反本制度造成数据泄露或损失的，依规追究内部责任；涉嫌违法的，依法承担相应法律责任。

第六章 附则

第十二条 本制度经2026年3月12日北京融和医学发展基金会第二届理事会第四次会议审议通过后施行。

主题词：数据隐私，制度

北京融和医学发展基金会　　2026年3月（第一版）印发