域智盾软件®

医疗行业

数据防泄密&终端安全解决方案



CONTENTS/目录

01 项目背景 ---------- 3

02 需求分析 ---------- 3

03 方案设计 ---------- 4

04 解决方案 ---------- 5

05 方案优势 ---------- 8

06 方案价值 ---------- 9

07 系统架构 ---------- 10

08 公司简介 ---------- 10

一、项目背景

伴随《中华人民共和国药品管理法》《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》等法规体系落地深化，医疗行业对商业秘密、个人隐私、科研数据的合规管控提出刚性要求。与此同时，医院终端类型复杂，U 盘摆渡、即时通讯外传、人员离职窃密等泄密通道多点迸发，亟需构建一体化终端安全与数据防泄密体系，筑牢医疗医药数据安全屏障。本方案面向综合医院、专科医院与医疗集团，围绕数据防泄密与终端安全两条主线，提供一套统一部署、统一管控、统一审计的综合解决方案。

二、需求分析

2.1 数据安全方面

- 患者病历、检验报告、影像资料在医生工作站本地长期留存，缺少加密与外发管控，离职、轮转、进修环节易发生数据外流。
- 护士站、医生办公室共用电脑，不同人员切换账号不及时，操作行为无法对应到具体自然人。
- 纸质病历、检查报告通过打印分发，缺少水印与回收登记，容易在科室间流转中丢失。
- 第三方厂商、运维人员、进修医生临时接入时，数据访问范围与留存周期缺乏约束。

2.2 终端安全方面

- 医院终端数量大、分布广，操作系统补丁长期不打，勒索病毒与远程漏洞利用可直接进入医疗内网。
- USB 外设、移动硬盘、手机接入缺乏管控，诊疗数据通过普通 U 盘被带出。
- 医生与行政人员私自安装软件、修改 IP 与计算机名、接入个人热点，破坏院内网络拓扑与终端基线。
- 外来设备随意接入医生办公室与行政办公网，未做安全检查即可获得网络访问权限。
- 终端发生硬件故障、误删、勒索加密时，病历与业务数据本地副本丢失，影响诊疗与日常办公。



三、方案设计

本方案围绕“医疗数据全流程可管、医疗终端全程可控”这一目标，提供数据防泄密与终端安全一体化的综合解决方案，从以下角度展开：

- 以患者数据为核心保护对象

将病历、影像、检验、处方、科研数据列为高保护级别，对历史文件批量加密，对新建文件自动加密，数据离开授权环境即不可读。

- 以医生与护士日常操作为边界

所有加密与管控动作在系统层完成，医生在 HIS、电子病历、PACS、LIS 等业务系统内的操作方式保持不变，不引入影响诊疗效率的额外弹窗。

- 以科室与岗位划分权限

按临床、医技、行政、科研、外包等不同岗位配置差异化的访问与外发权限，最小必要授权，避免跨科室越权访问。

- 以审计与证据链为交付标准

所有数据访问、外发、外设接入、终端变更动作集中留痕，满足医院内部审计、上级主管部门检查与事件取证的需要。

四、解决方案

解决方案由数据防泄密与终端安全两大板块组成。

4.1 数据防泄密板块

4.1.1 数据加密

针对新建文件，可以采取透明加密模式，文件在保存时自动、强制加密，无需用户手动操作，不影响办公效率，未经授权的外发会变为乱码。

针对终端历史文件加密，可以批量加密某个盘符内所有文件，无需手动依次打开、保存加密，设置加密策略。

4.1.2 用户模式



医护、科研人员登录专属账户后，进入独立安全工作域，实现按岗位分级授权，适配临床诊

疗、药物试验、科研办公多角色共用终端的精细化数据安全管理。

4.1.3 外发通道管控

对即时通讯、网盘、邮件、移动存储等各类数据外传通道实施统一策略管控，支持外发审批、通道阻断、受控解密，实现数据流转全通道可控。

4.1.4 水印震慑与溯源

支持多种水印类型，包括文字水印、图片水印、点阵水印、二维码水印，可以有效震慑违规拷贝、拍照、纸质外传行为，实现泄密事件可视化追溯。

4.1.5 操作审计与溯源

全量记录敏感数据的新建、删除、修改、查阅、重命名、打印、拷贝、外发、上传下载等动作，按医生、按终端、按关键词、按时间形成可检索的审计日志。

4.2 终端安全板块

4.2.1 终端准入与基线检查

所有接入院内网络的终端必须先通过安全检查：是否安装客户端、补丁是否达标、杀毒是否开启、是否存在违规软件。不满足基线的终端被引导至修复区，达标后才能访问医院内网、业务系统。

4.2.2 外设与网络管控



4.2.3 上网行为与程序管控

基于岗位维度定制化上网访问策略，对非业务相关网站分类实施访问阻断，对终端运行程序灵活管控，约束值班人员上网行为，遏制私装软件引发的病毒感染、挖矿程序入侵等安全隐患。

4.2.4 补丁与软件资产管理

统一统计 Windows、信创系统补丁，支持按风险等级自动分发、定向安装，实现系统漏洞自动化闭环处置。

自动采集终端硬件与软件清单作为资产基线，发生硬件更换、软件私装、安全软件被卸载时实时告警。

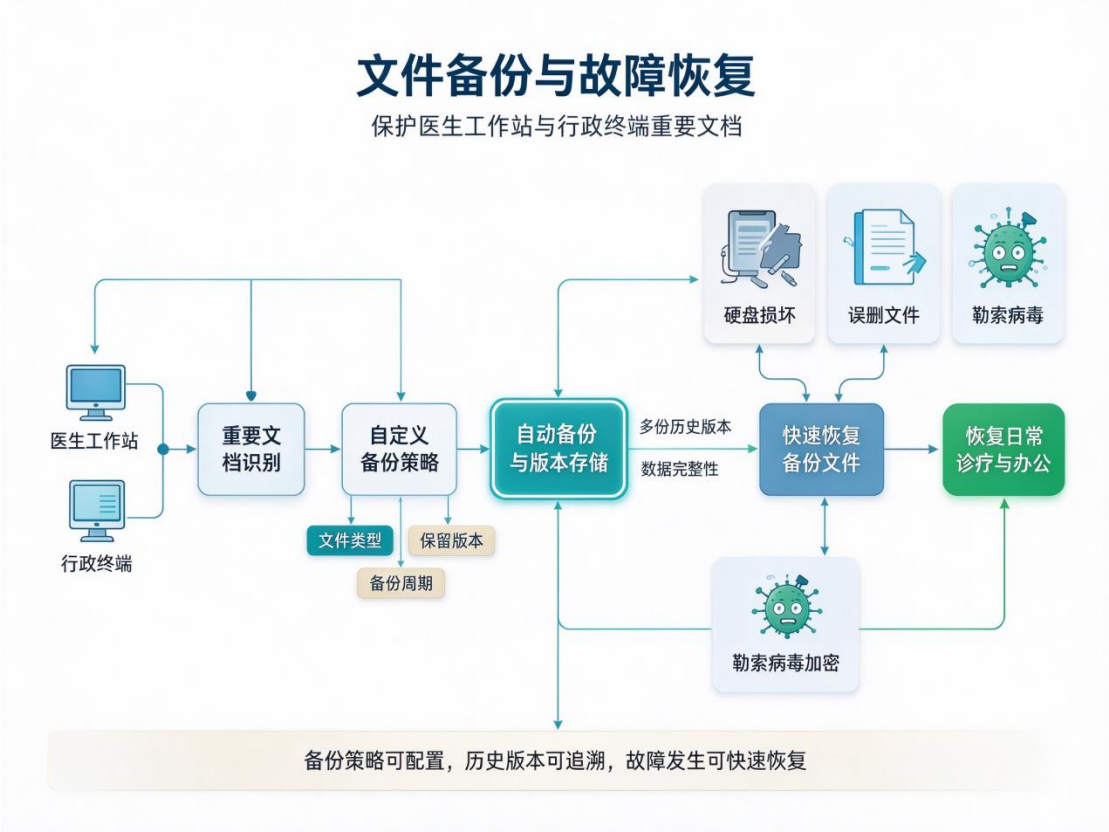
4.2.5 使用权限与配置锁定

对医生办公电脑与护士站工作站锁定关键配置：禁止使用 Guest 账户、禁止使用注册表编辑器、禁止修改敏感注册表项、禁止使用控制面板、禁止使用任务管理器、禁止使用安全模式、禁止使用计算机管理（包括服务器管理、组策略管理等）、禁止修改 IP 地址、禁止修改 MAC 地址、禁止修改计算机名、禁用 WSL/WSL2、禁用 Ipv6、禁用系统还原、禁用 PPPoE，保证终端基线一致。

4.2.6 文件备份与故障恢复

对医生工作站与行政终端上的重要文档做备份，可自定义设置保留多份历史版本，确保数据的完整性。

当终端发生硬盘损坏、误删、勒索病毒加密时，可快速恢复备份文件，不影响日常诊疗与办公。



五、方案优势

- 私有化部署：医疗核心数据留存院内，满足医疗数据合规要求，规避公有云托管风险。
- 一体化交付：数据防泄密与终端安全在同一后台完成，避免医院在多套安全系统之间做集成对接。
- 医疗业务适配：对医院常用业务系统做兼容适配，加密不影响医生开方与护士站工作。
- 分级部署：支持按门诊楼、住院楼、医技楼、行政楼、科研楼分区分域下发策略，新院区与新科室可快速纳入管理。
- 证据链完整：从识别、阻断、审批到取证全程留痕，事件发生后可按医生、按终端、按患者号还原全过程。

六、方案价值

✶ 合规价值——满足医疗行业数据合规要求

对齐《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》《医疗卫生机构网络安全管理办法》以及等级保护要求，形成可向主管部门提供的策略文档与审计记录。

✶ 业务价值——保护患者数据与科研资产

避免病历、影像、检验、科研数据因员工离职、轮转、终端丢失而外泄，保护医院多年积累的临床数据与科研成果。

✶ 管理价值——将制度要求转化为技术策略

把信息科与医务处的管理制度转化为终端上可执行、可考核的策略，医院对全终端与数据状态实现可见可控。

✶ 效率价值——减少信息科重复劳动

补丁分发、资产盘点、外发审批、事件排查线上化，降低信息科在日常运维中的重复投入。

✶ 更新价值——产品是与时俱进的

持续吸纳市场业务需求与客户反馈，以客户业务诉求为导向开展产品迭代研发，保持 1-2 个月稳定版本更新周期，赋能业务长期发展。

七、系统架构



八、公司简介

河北中视新研软件开发有限公司深耕终端安全与数据防泄漏赛道，过五关，斩六将，自主研发一体化终端安全管控平台，深度适配医疗机构、药企、临床科研机构业务场景，已在多家医疗机构与医疗集团落地，是医疗医药领域终端数据安全防护可靠的专业服务商。

公司总部坐落于全国性综合交通枢纽城市——石家庄，覆盖前期需求深度调研、试点验证部署、正式上线落地与长期运维保障全流程，为客户提供一体化闭环服务支撑，配套专属客服热线 400-097-8770，快速响应客户诉求。

官方网站 yzdsaas.com

电话： 400-097-8770

地址： 河北省石家庄市

——围绕患者数据安全与医疗终端合规，构建一体化防护体系

域智盾软件®