安企神医疗行业

数据防泄密与终端安全

解决方案

面向医院 · 医药企业 · 医疗器械 · 基因检测与医疗大数据机构

让诊疗数据安全流转，让每一次访问有迹可循

目 录

01 项目背景 1

02 需求分析 2

03 方案设计 4

04 解决方案 5

第一部分以数据防泄密为导向 5

第二部分以终端安全为支撑 8

05 方案优势 9

06 方案价值 10

公司简介 12

01　项目背景

一次完整的诊疗，会在信息系统里留下一条长长的轨迹：挂号与分诊记录、门诊与住院病历、检验检查报告、医学影像、手术麻醉记录、护理文书、处方与医保结算信息。这些数据分散在 HIS、EMR、LIS、PACS、医保接口与互联网医院平台等数十个系统里，由医生工作站、护士站终端、移动查房车、自助一体机、影像阅片工作站等形态各异的终端承载。一家三级医院一年新增的诊疗数据以 TB 计，医药企业的临床试验数据、基因检测机构的测序数据，同样是一份份价值连城的档案。

医疗数据的敏感程度，在各行各业里排在最前列。病历上有真实姓名、身份证号、住址、诊断与用药，基因数据更是伴随一个人一生的生物特征。这些数据一旦流出，损害的不只是一道新闻或一次通报，而是患者的隐私、尊严乃至人身安全，而且这种损害无法像重置密码那样补救——数据收不回来。

合规的绳索也在持续收紧。《网络安全法》《数据安全法》《个人信息保护法》构成了数据保护的基本框架，《医疗卫生机构网络安全管理办法》对诊疗数据、人口健康信息的管理提出了明确要求，等保 2.0 测评、医保基金飞行检查、卫健部门的安全通报，都在把"数据怎么管的"变成一道必须当场作答的题。答不出记录、拿不出制度的机构，轻则整改，重则通报。

更棘手的是医疗行业自己的特有风险。勒索软件盯上了"停不起诊"的医院——近年多家医院因勒索攻击导致 HIS、PACS 瘫痪，被迫停诊甚至手工挂号；"统方"成了药品耗材回扣链条上的关键数据，一个科室的历史处方被导出一次，就能养活一条利益链；实习生、进修生、外包运维、设备厂商工程师在院内网络里进进出出，谁该看到什么，多数时候只靠一张门禁卡和一句口头交代。

医疗数据资产的三点特征

01 敏感度极高	02 主体多而杂	03 链路长且旧
病历、处方、影像、基因数据直接指向个人身份与健康状态，一份外流即构成对具体患者的侵害。	医护、技师、行政、实习进修、外包运维、厂商工程师同网工作，账号权限与实际身份常常对不上。	老旧系统仍在服役，医疗专用终端、自助设备、国产化与 Windows 环境并存，防护很难一刀切。

医疗行业的数据安全不是"再装一套杀毒软件"，而是让诊疗数据与科研成果从产生到归档的每一次流转都处在可控范围内：谁能打开、能不能拷、能不能打印、能不能发出去、发出去之后还能不能追。方案要做的，是把零散的管控动作收敛成一套规则、一个平台、一份随时拿得出的记录。

02 需求分析

结合医院、医共体、医药与医疗器械企业、基因检测机构的终端环境和业务流程，我们把医疗行业的共性问题归纳为五个方面。它们不是五个孤立的缺口，而是同一条链路上的五个环节：数据散在终端和系统里，从多条出口流出，事后又说不清楚。

诊疗数据散落在各类终端，谁看过、谁拷过没有统一口径

- 电子病历、检验报告、影像文件、科研数据以明文存放在医生工作站与共享存储里，同一份资料在多台终端、多个目录存在副本。
- 科室之间的资料传递依赖共享目录、即时通讯和邮件，文件离开科室网络后去向无人掌握。
- 病案室、科研科、基因分析等核心部门的数据没有密级区分，一台通用账号的终端可以打开全院范围的敏感文件。

终端形态繁杂、桌面混乱，成了风险的集散地

- 医生工作站常年开机不做维护，系统补丁常年缺失；护士站终端被安装购物、直播、股票软件的情况并不少见。
- 移动查房车、自助一体机、门口机等专用设备缺乏统一管理，谁的账号在用、用了什么，底数不清。
- 弱口令、共用账号普遍存在，出问题时无法把操作落到具体的人。

数据出口多，打印、外发、远程运维各有各的通道

- 病历复印件、检验报告、诊断证明的打印是日常业务，纸张一旦离开病案窗口就没有任何约束。
- 科研数据出院、论文投稿数据外发、向申办方递交试验数据，缺少统一的审批与受控通道。
- 设备厂商的远程运维接入、外包人员的维护通道直接伸进内网，权限多大、做过什么，多数机构答不上来。
- 移动硬盘、U 盘在影像拷贝、数据备份场景大量使用，介质本身不受控。

人员结构复杂，统方与批量带离缺少预警

- 医护轮转、实习进修、外包驻场使得账号与人的对应关系频繁变化，离职离院时的数据处置往往被忽略。
- 统方行为藏在正常业务查询里：一个账号反复导出特定药品的历史处方，如果不做专门识别，与日常报表没有肉眼可见的差别。
- 离院前的批量下载、集中压缩、上传个人网盘，事后只能看到结果，看不到过程。

审计与举证能力薄弱，等保测评与上级检查吃力

- 日志分散在 HIS、影像系统、服务器、交换机各处，缺少按科室、按患者、按时间维度的统一检索入口。

- 被问到"某患者的病历过去半年被谁调阅、拷贝过"，只能靠各系统人工排查，答复周期以天计。
- 等保测评要的访问控制、安全审计证据，靠测评前突击整理，无法常态化输出。

03　方案设计

医疗行业的数据安全问题，本质是三句话：数据要锁住、终端要管住、行为要留痕。因此方案不追求功能项的堆叠，而是围绕一条主线展开——让诊疗数据与核心资产始终处于可控状态，让每一次访问与流转都可追溯，让管控动作嵌进原有诊疗流程而不添堵。

围绕这条主线，方案以"一个平台、三层纵深"组织能力：数据层解决"带走也没用"，行为层解决"出不去、进不来不该进的"，管理层解决"发生了能查、检查时拿得出"。

一个平台 · 三层纵深

层级	能力	解决的问题	实际效果
数据层	**文档加密与外发受控**	可用不可带走	病历、科研、基因数据院内正常流转，离开授信环境即为乱码
行为层	**终端安全与通道管控**	管住承载与出口	资产、软件、外设、准入、防勒索，一台终端一张底账
管理层	**审计溯源与合规支撑**	查得到、拿得出	记录、检索、报表与取证，把"说不清"变成"当场出"

三条设计原则

- **临床零打扰**——加密在驱动层完成，HIS、EMR 的操作方式与响应速度不变，护士站不因安全软件多等一秒；策略按科室灰度上线。
- **按域隔离、按密级授权**——以科室与数据类型划分安全域，病案、科研、基因数据各自成域；账号权限跟着岗位走，跨域访问在客户端侧即被拦截。

- **合规优先、记录先行**——管控动作同步生成可核查记录，等保测评、医保飞检、上级检查要什么，平台就能出什么。

实施路径：三步走

第一步核心科室试点	第二步全域推广	第三步制度固化
选择病案室、科研科等核心科室先行部署，跑通加密、外发、审计三条主链路，同步完成性能基线测试。	覆盖临床、医技、行政与分支机构终端，自助设备与专用终端统一纳管，策略由信息科集中下发。	把策略与病历管理制度、科研数据管理制度、等保要求逐条对应，形成可季度复核的闭环。

04 解决方案

方案能力分为两层：第一层是数据防泄漏主线，解决"医疗数据怎么管"；第二层是终端安全底座，解决"数据靠什么终端承载、从哪条通道进出"。两层共用一个客户端与一个管理平台，按需启用、逐步扩展。

第一部分以数据防泄密为导向

这一组能力回答"诊疗与科研数据怎么管"：从透明加密、业务环境适配、外发与通道管控、打印与屏幕防护、敏感识别到行为审计，六个动作串成一条从产生到归档的链路，任何一个环节都不单独成立。

1.1 医疗数据透明加密

病历和科研数据的价值在内容本身。第一个动作是让文件自带锁：加密在驱动层完成，保存即密文，在授信环境内正常打开、编辑、调阅，一旦离开授信环境，打开就是乱码。

加密模式	适用岗位与场景	实际效果

加密模式	适用岗位与场景	实际效果
透明加密	病案室、科研科、基因分析等核心岗位	新建与保存即密文，院内正常使用，外发为乱码
智能加密	临床医护等调阅多、产生敏感文件少的岗位	按进程与文件类型判定，命中敏感规则才加密
只读授权	提供给协作机构、申办方的资料	可看不可改、不可另存，防止二次扩散
落地加密	外部机构回传数据、厂商交付件	落到本机即转为密文，转发到别处无法打开

密钥采用国密算法并分级管理，按科室与密级划分，既满足等保对存储机密性的要求，也为检查提供可说明的技术口径。HIS 系统的缓存目录、影像设备的临时目录经审批后加入例外清单，避免误伤业务。

1.2 医疗业务环境适配

医院终端环境复杂，安全措施必须迁就业务，而不是反过来。

- 兼容并蓄：客户端同时覆盖 Windows、国产操作系统与信创环境，老旧门诊终端等在支持范围内，医疗专用软件的调用方式一律不改。
- 共享存储几乎无感：影像归档、病案共享目录内的文件以密文落盘，授权终端正常访问，不改变原有权限模型。
- 性能可观测：上线前后对比同一业务系统的响应耗时形成基线，出现劣化可定位到具体策略并单机回退。

1.3 数据外发与通道管控

医疗数据必须流动：科研数据要出院、试验数据要递交、医保数据要上报。管控的目标不是"不出门"，而是"出门的那一份可控"。外发走"申请—审批—受控—留痕"四步：发起时自动带出文件清单，科室负责人与信息科分级审批；通过后生成受控文件，限定打开

次数与有效期、绑定设备、禁止打印、叠加水印；每一次打开行为回传审计。医保、卫健等固定上报对象列入白名单直通，其余外发一律审批；厂商远程运维经审批限时开通，全程录屏，到期自动收回。

1.4 打印与屏幕输出管控

诊疗数据落到纸面、落到屏幕上，就没有技术约束了。方案对打印实施审批、水印、内容留存三件事：病历复印件、检验报告打印时自动叠加操作人、时间与患者标识，纸张流出后能锁定到人；病案室外印一律审批留档。屏幕是另一条出口——电子病历与影像阅片界面叠加屏显水印，评审会、教学查房场合拍照即留痕；截屏行为受控记录，剪贴板与拖拽禁止把患者数据带入外部程序。

1.5 敏感内容识别与分类分级

先回答三个具体问题：哪些文件含患者隐私，它们躺在哪台终端上，现在是不是明文。

环节	做什么	输出
数据源	扫描医生工作站、共享存储、病案服务器	待检文件清单与分布
识别	关键词、正则、文件指纹匹配	命中规则的文件与置信度
标记	打上科室、数据类型、密级标签	敏感文件台账
处置	补加密、告警、阻断外发	处置结果与责任人

识别规则可按机构自定义：患者姓名与身份证号组合、住院号与诊疗记录特征、基因序列文件指纹、特定药品处方统计特征等。识别是起点，把清单变成规则——哪些目录必须加密、哪些岗位只能只读、哪些外发必须审批——才是终点。

1.6　行为审计与统方预警

审计的价值不在"都记下来"，而在要的时候找得到。文件操作、打印、外发、邮件、即时通讯、网页、剪贴板行为统一采集，按人、时间、科室、关键词组合检索，从一条记录还原整条事件链。

针对医疗行业专门设置三类预警信号：一是统方特征——同一账号高频导出特定药品或耗材的历史处方统计，立即告警并阻断；二是离院前行为——离职离院流程发起前批量下载、集中压缩、上传个人网盘；三是越权访问——跨科室调阅病案、非诊疗时段批量查询患者信息。检查、举证、追责时当场调出记录、说清路径，处理成本完全不同。



第二部分以终端安全为支撑

数据能被带走，前提是有终端承载、有通道进出。终端与网络管不清，数据防线就是空中楼阁。

能力	解决什么

能力	解决什么
资产台账与准入控制	全网扫描生成软硬件底账；身份、设备、安全状态三重校验，不合规终端接不进内网
桌面标准化与软件管控	工作站桌面统一分发，禁止私装无关软件；破解版工具远程清理
违规外联与专用设备管理	私接互联网、私搭热点立即告警阻断；自助机、查房车按设备身份单独授权
防勒索与数据备份	文件加密变形即告警、进程加密行为管控，文档删除修改自动备份，勒索事件可回滚恢复
补丁与远程运维	系统漏洞补丁统一管控，弱口令强制整改；信息科远程处理故障，不必逐个科室跑腿

其中防勒索值得单独强调：医疗是勒索攻击重灾区，一旦 HIS 与 PACS 被加密，医院面对的不是数据问题而是停诊问题。终端侧对加密变形行为实时告警、对可疑进程的批量改写动作直接阻断，配合文档自动备份，把"被勒索后付赎金"变成"回滚恢复继续接诊"。

05　方案优势

医疗机构选型时最关心的三件事：会不会影响看病的速度、要不要改动现有系统、检查的时候能不能拿出东西。对应的答案，构成了这套方案的基本盘。

优势	说明
一体化：一个客户端，一个平台	加密、审计、终端管控、准入、备份在同一客户端内实现，信息科不必为每类需求维护一套系统

优势	说明
不影响诊疗：临床零打扰	加密在驱动层完成，HIS、EMR 操作方式与响应速度不变；策略可灰度、可回退
闭环：事前、事中、事后	事前加密预防、事中通道阻断、事后审计取证，三段能力串成一条链
分域：科室制隔离	以科室与数据类型划安全域，权限跟着岗位走，跨域访问客户端侧即拦截
可举证：对标监管要求	访问控制、安全审计、数据保密性措施可映射等保 2.0 条款，支持国密算法
可扩展：多院区统一纳管	总院、分院、互联网医院在同一平台分级授权，策略统一制定、分级下发

06 方案价值

价值	具体表现
患者隐私"可用不可带走"	病历与敏感数据院内自由流转，离开授信环境即为乱码，"拷一份出去"从技术上失效
统方与内部违规"看得见"	统方特征、批量调阅、异常导出实时告警，把藏在正常业务里的动作暴露出来
停诊风险"降下来"	防勒索管控加自动备份，勒索事件从支付赎金变成回滚恢复，诊疗连续性有保障
检查举证"拿得出"	等保测评、医保飞检、上级督查要的记录与报表当场调取，不必突击整理
信息科"从救火到管理"	资产、软件、补丁、故障在同一平台处理，几个人也能管住上千台

价值	具体表现
	终端
制度"落得下去"	保密制度、病历管理规范与技术策略逐条对应，制度写在纸上，机制跑在终端上

这六条价值指向同一件事：把过去依赖保密协议、依赖人盯人、依赖事后排查的管理方式，换成可持续运行的技术机制。制度写在纸上，机制跑在终端上，两者合起来才叫"管得住"。

公司简介

石家庄安企神网络科技有限公司成立于 2015 年，是一家以研发信息安全类产品以及提供相关服务为主营业务的技术驱动型公司。

安企神软件是由该公司研发的终端安全管理系统，打造全生命周期一站式信息安全整体解决方案平台，集文档加密、电脑行为审计、终端安全管理、网络准入控制、敏感内容识别、IT 运维管理等 200+ 功能于一体，有效防护不当办公行为造成的数据泄露。

安企神软件深耕终端安全与数据防泄密领域十余年，拥有 300 余家合作伙伴，服务万余家政企客户，累计覆盖终端超 1000 万台，广泛应用于政府、金融、运营商、制造、能源、教育、医疗等行业的大型知名单位和机构，涵盖衣食住行各行各业。

ANQISHEN
400-666-2563
www.wgj7.com
河北·石家庄
安企神软件®