



## 中国数据安全专家

亿赛通成立于2003年，是数据安全领域专业的综合数据安全厂商，为各行各业超万家企事业单位、800余万终端用户提供数据安全服务与解决方案。作为拥有完全自主知识产权并取得多项国家资质认定的双高新技术企业，亿赛通现拥有产品资质200余项、企业资质150余项、荣誉奖项300多个，取得国家级“专精特新”小巨人企业认证，获得CCID、IDC、中国信通院等专业机构的高度认可，并连续多年保持数据泄露防护产品在中国市场占有率领先的地位。

**解决方案名称：医疗行业数据安全解决方案**

**提供单位：北京亿赛通科技发展有限责任公司**

**方案介绍：**

一、案例背景

医疗行业关系国计民生，医疗数据一旦遭到篡改、破坏或泄露，势必对医疗机构的正常运转及医患双方的隐私安全构成严重威胁，甚至影响社会的安定和谐。伴随医疗信息化系统的广泛应用，数据已成为医院等医疗结构发展的重要资产；同时，医疗数据因包含病例、处方等大量患者信息，也面临着敏感数据管理方面的重重难题。

二、方案简介

方案参考《数据管理能力成熟度评估模型》以及《数据安全能力成熟度模型》，将数据安全建设作为一个体系化的工程，医疗机构在进行数据安全建设时要符合法律法规、行业准则以及内部数据安全管理办法，坚持管理和

技术并重的原则，明确了数据全生命周期每个节点应该具备什么样的防护能力，通过统一的管控，实现数据安全持续运营的最终目标。

1、合规要求

随着医疗大数据建设的不断深入，医疗机构对患者信息的掌握越发详细，数据合规的重要性也日益凸显。为了确保数据安全，医疗机构必须遵守一系列的政策法规和行业监管要求，包括法律法规遵守、数据分类管理、访问权限控制、数据加密保护、数据备份恢复、数据安全审计、防范黑客攻击、终端设备安全、安全意识培训、合规监测与报告等。

2、管理体系

数据安全管理体系是数据安全技术体系真正有效发挥保护作用的重要保障，数据安全管理体系的设计立足于企业总体安全战略，并与安全技术体系相互配合，增强技术防护体系的效率和效果，同时也弥补当前技术无法完全解决的安全缺陷。

### 3、技术体系

针对数据安全的风险点，用户侧、终端侧、网络侧、业务侧以及数据中心，都要做好技术防护措施，外防攻击、防入侵、防篡改，内防滥用、防伪造、防泄露。针对不同安全级别的数据，结合自身数据安全管理制度应用不同的技术措施。

### 4、统一安全管控

以数据安全全生命周期管理为核心，通过多维度量化指标，精准描述数据安全的实时风险及整体状况，利用海量数据分析引擎及模型实现对风险的主动发现、精准定位、智能研判、快速处置、严格审计，完成对数据安全保护工作的闭环处置流程。

### 5、运营体系

安全运营是保障业务在安全环境下稳定运行的基础。数据安全作为组织整体安全运营的一部分，具有整体性和独立性。整体性强调与整体运营工作的结合，如事前的漏洞检测，事中的安全处置，事后的复盘分析。

### 三、方案收益

1、数据安全合规：满足国家和各行业多个法规和标准的要求。能够帮助医疗机构快速通过各种安全保密检查和评测。

2、数据安全可视：实时显示医疗机构敏感数据的分布情况、访问情况、风险状况，及时并预测可能的数据异常活动状况和风险，实现数据安全最基本的要求。

3、数据安全可控：通过控制对医疗机构数据的活动和访问，防止敏感信息部分或全部被偷窥、拖库或者镜像，防止敏感信息被非法修改或者删除。

4.完善防御体系：将非结构化和半结构化数据，作为数据安全建设中的重点，在保障信息安全的前提下，实现高效办公。有利于机构完善纵深防御体系，提升整体安全防护能力。

5、避免数据泄露：实现数据安全的可视性和可控性，并最终减少核心数据资产被侵犯的可能性，保障正常的业务连续性，降低或避免核心数据资产泄露发生。



中国数据安全专家