南山区医疗集团总部敏感数据管理系统项目需求

# **建设背景**

随着国家《个人信息保护法》、《数据安全法》等数据安全相关法律条令以及《深圳市公共数据安全要求》等规范实施，医疗行业重要敏感数据资产数量繁多、复杂多样，医疗监管机构需要确保其数据的安全和合规性，及时发现数据安全风险，结合南山医疗集团总部数据安全建设规划，拟建设敏感数据管理系统，主要功能包含对敏感数据资产管理发现、数据分类分级、风险评估等功能，同时通过建设企业微信安全网关，提供基于企业微信访问下的终端数据安全加固，包括敏感信息过滤、水印和反入侵能力，帮助医疗集团解决合规应对、敏感数据排查数据安全风险检测等多方面的数据安全问题，及时定位数据安全风险，提高数据安全保障能力。

# **建设依据**

建设依据以国家发布的相关通知和标准规范为主，包括但不限于：

1. 《信息安全等级保护管理办法》
2. 《中华人民共和国数据安全法》
3. 《中华人民共和国网络安全法》
4. 《健康医疗数据安全指南》
5. 《医院信息互联互通标准化成熟度测评方案（2020年版）》
6. 《信息技术软件生存周期过程》GB/T8566-2007
7. 《计算机软件文档编制规范》GB/T8567-2006
8. 《信息技术软件工程术语》GB/T11457-2006
9. 《信息技术系统及软件完整性级别》GB/T18492-2001

# **需求分析**

**1.数据操作风险难以控制**

运维人员、第三方人员，由于拥有数据库的用户权限，导致通过内部环境对数据库的越权访问，敏感数据访问、导出数据、在线数据沉淀、数据删除等，造成通过内部的敏感数据泄露的安全风险。

**2.数据丢失难以追溯，无法定责**

由于可以接触的数据的人员比较多，而且操作数据库的人员技术水平不一，当各类人员对数据库进行操作时，他们对数据库的操作行为无法可视化的展示，而有些操作可能会导致数据修改，或者删除，发生这种事后，无法进行追溯，也无法定则。

**3.缺乏数据安全监测和管理能力**

参考《大数据安全管理指南》（征求意见稿）《GB/T35274大数据服务安全能力要求》《GB/T22239信息安全技术网络安全等级保护基本要求》等数据安全管理要求，对数据进行全生命周期的安全监测监管。

随着医院应用系统不断增多，数据库以及数据库中的数据不断集中、不断增长，在数据集中之后的大数据量的数据场景下，如何快速定位保护对象，掌握敏感数据分布，清晰了解保护对象数据如何被处理和流转，如何感知当前数据存在的风险，以及及时响应防护，需要一套数据安全管控平台实现保护对象的精确定位、动态流转监控、风险实施监测、数据安全集中管理、策略下发、联动防护。

**4.企微端接入人员终端，终端数据安全风险高**

当前面向全院职工和第三方人员在企业微信下的访问缺乏有效的安全管控手段，人员可通过互联网访问企微工作台业务从而触达集团内网系统，存在终端数据泄露和攻击风险。且传统的VPN登录方式很难满足企微场景下的数据安全管控需求，运维管理工作量大。

# **分阶段建设规划**

围绕南山医疗集团数据安全建设现状和需求，拟分三期进行数据安全建设，最终实现集团数据安全的可观可控。数据安全三期建设如图所示：

图示

描述已自动生成

在第一期建设中，重点落地数据安全中心（数据安全大脑）、API风险监测预警和数据库防火墙。通过构建集团本地的数据安全大脑，建设数据安全管理系统的平台，各类数据安全风险均收集于数据安全大脑进行整体的数据安全态势分析，为集团后期细分数据安全防御奠定基础。

本方案为数据安全一期规划的重要组成部分，拟在建设集团数据安全大脑同时，通过联动企业微信数据安全能力，实现企业微信业务访问场景下的数据和业务访问管控，并实现集团中心和企微客户端之间的数据安全联防联控。

# **本次建设内容**

依据南山医疗集团数据安全建设需求分析，本次拟从数据安全管理中心（数据安全大脑）和企业微信安全网关两个角度，分别从集团数据中心安全和企微终端数据安全方面，进行数据安全建设和加固。

**1.数据安全管理中心（数据安全大脑）**

数据安全中心DGSC致力于为用户提供数据安全治理体系技术支撑工具，定位为一款企业级的数据安全管理平台，从企业数据安全治理、数据安全合规出发，提供数据资产管理、数据分类分级、风险评估等能力，帮助企业解决合规应对、敏感数据排查数据安全风险检测等多方面的数据安全问题，降低数据安全治理TCO，提高数据安全保障能力。

下图所示为DSGC 产品功能架构图：

图形用户界面, 网站

描述已自动生成

### 资产发现

资产发现是数据安全管理的第一步。数据安全中心支持对Mysql 、Oracle、SQL Server、GaussDB、MongoDB、MariaDB、PostgreSQL、Db2、达梦、TiDB等常见数据库资产的发现及管理。DSGC支持两种资产发现方式：

* 手动资产同步

手动资产同步支持对接现有CMDB（配置管理数据库）的资产信息，实现资产的同步录入。

* 自动发现资产

通过端口探活对目标IP地址段和端口范围进行定期或不定期的主动嗅探，发现数据资产

### 敏感数据发现

数据安全中心DSGC敏感数据识别引擎内置丰富的分类分级模版，支持多维度数据项规则配置，基于多模态匹配、校验算法、NLP、AI等多种识别方法，能够从海量数据中快速、准确发现数据特征。

* 字典匹配：通过模式匹配式（如正则表达式、关键字符等），对数据进行逐一匹配，当搜索到满足模式匹配式的片段时，定义数据为敏感数据。
* 多模态匹配：基于文件名称、文件格式、文件内容等信息，通过关键字、正则表达式、自然语言处理等方法匹配标签规则。
* AI语义：提取文档指纹特征，采用语义分析的技术对敏感文档和目标文档进行分词，基于不同的指标计算文本相似度，最后根据预设的相似度阈值判定目标文档是否为敏感信息文档；
* 引擎底层的分层服务架构、预处理、水平扩容、并行计算、采样检测等机制，保障了高并发场景下的高吞吐和高可用。

### 数据分级分类

数据分级分类是数据确权和访问控制的基础和依据，数据安全管理中心（数据安全大脑）支持自定义数据分级、分类标签功能，用户可根据行业标准或者自身业务场景、数据价值、数据影响、数据用途、数据来源等确定数据分级分类标准，进而形成企业专属标签库。

通过基于AI算法的智能标签功能与人工辅助相结合方式，可极大地减轻人员的低效工作、缩短数据治理周期。企业可依照数据标签属性用户可以制定精细的安全策略和数据授权机制，最终确保敏感信息的扩散范围和权限粒度。

图片包含 表格

描述已自动生成

### 数据资产风险评估

基于识别引擎生成的数据资产梳理结果，风险评估引擎将围绕核心数据资产，从数据库账号权限、配置风险、脆弱性风险、泄漏风险等多角度进行数据安全风险评估，提供风险关联资产、风险级别、风险缓解建议等多维度分析结果助力数据安全风险收敛，并持续监控风险处置状态，持续推进风险治理。

图示

描述已自动生成

### 安全能力协同

数据安全中心（平台版）提供数据安全策略统一管理和运营的能力，动态监控资产分级与保护措施情况，如重要数据、敏感数据是否加密、脱敏等；实时查看资产防护状态，通过资产安全评分体现资产安全水位，支持一键开启数据审计、态势分析等。

日程表

描述已自动生成

**2.企业微信安全网关**

作为移动办公的领先产品，企业微信当前已被大量医院选择并为医院提供从“智慧管理”到“智慧服务”再到“产业互联”的数字化能力。但便捷和安全一向是矛盾的两面，《医疗卫生机构网络安全管理办法》明确要求医院加强网络安全管理，强化信息系统自行开发或外包开发过程中的安全管理，全面落实安全保护措施。如何发挥企业微信便捷服务优势的同时，提供安全可靠地访问医院重要的业务应用，是摆在众多医院面前的首要问题，企业微信安全网关（简称“企微网关”）能够一站轻量式地解决医院在跨网访问内部应用时的安全防控问题。部署网关后，医院仅需将内网业务接入企业微信的「企微网关」组件，院内职工通过企业微信访问内网业务时，就会自动建立安全加密通道，在恶意威胁进入医院网络之前监测和阻止，有效保护医院核心业务和数据，切实解决医院在企业微信访问场景下的数据安全问题。

### 敏感信息过滤

企业微信用户股访问安全网关代理的页面时，页面展示的内容会按照后台配置的敏感规则进行数据保护脱敏，以保证内部数据的安全性。默认对手机号码和身份证号码进行数据脱敏，同时支持自定义敏感词。

图形用户界面, 文本, 应用程序, 电子邮件

描述已自动生成

### 访问水印

企业微信用户在访问站点应用时，若该站点资源选择了开启水印功能，则站点页面会带有水印，以防止内部机密外传、方便回溯泄密源头。

图形用户界面, 文本

描述已自动生成

### 工作台应用管理和控制

对web应用、API进行集中管控，可直观展示各应用/API接口对外提供哪些服务、应用状态，及安全防护策略等信息，并提供紧急关停功能（一键实现应用批量下线控制）。

图形用户界面, 应用程序

描述已自动生成

图形用户界面

描述已自动生成

图形用户界面, 应用程序

描述已自动生成

对自建应用及API接口进行鉴权和访问控制。可对应用进行用户访问权限的分配达到管控目的，仅有授权用户可访问。

图形用户界面, 文本, 应用程序

描述已自动生成

图形用户界面, 应用程序

描述已自动生成

### 身份认证和授权

网关支持多种认证方式，包括企业微信扫码认证、密钥对认证等（当添加的资源是web业务系统时，可采用企业微信扫码认证；当添加的资源是API接口时，可采用密钥对认证的方式）。

* 企业微信扫码认证

随着办公移动化，企业微信越来越多的进入企业用户的日常工作中，企微网关集成企业微信认证方式， 为企业提供一体化的集成方案。

* 密钥认证

API接口的密钥对认证也是常见的鉴权方式之一。网关会对每个访问请求进行身份验证，即每个请求都需要在参数中包含签名信息（Signature）以验证请求者身份。签名信息由安全凭证生成，安全凭证包括 SecretId 和 SecretKey，二者内容没有关系、无法相互推算。当请求的签名和服务器的签名计算进行相等验证通过时，则放行此请求。该验证方式的安全性高，且占用计算资源和网络资源都很少。

### 日志和审计功能

全面记录用户日志、管理员日志等，用户使用网关中所有产生的请求信息都会有记录，管理员可以用过管理后台直接查看所有的访问日志，支持回溯审计。

* 用户登录日志

图形用户界面, 应用程序

描述已自动生成

* 后台操作日志

图形用户界面, 表格

描述已自动生成

* 业务访问日志

图形用户界面, 应用程序

描述已自动生成

图形用户界面, 文本, 应用程序, 电子邮件

描述已自动生成

### 企业微信联动

企业微信和网关集成助力企业微信 ，通过企业微信工作台，打通企业内网应用，提高企业移动办公效率。

# **优势亮点**

**1.系统化数据安全治理技术支持**

为了解决数据安全合规治理问题，集团首先需要建立一个符合自身业务特点的治理框架，按照框架落地数据安全治理工作。在技术工作层面，最核心最关键的就是通过自动化工具识别出敏感数据，以及相应的安全合规的风险点，它是数据安全治理工作的前置条件。本方案结合数据安全治理最佳实践，提供了数据发现、分类分级、风险评估、统一策略管理、持续监测与告警等一站式的数据安全治理技术工具，帮助用户落地数据安全治理难题。

图示, 箭头

描述已自动生成

**2.高度灵活的分级分类策略**

产品内置了个人信息、个人金融信息、汽车等行业的数据分类分级模版及超过224个数据识别规则。然而不同业务属性、不同行业标准的数据分类分级不尽相同；甚至即便相同的数据项，在不同的场景中，对应的数据敏感级别分级也不尽相同。通过将数据识别规则、数据分类、敏感分级进行解耦，并支持用户以任意组合制定满足业务不同业务及管理需求场景的分类分级模版，满足多样化的数据分类分级及数据安全治理管理需求。



**3.细粒度数据资源鉴权体系**

细粒度的用户、角色、组织架构及资产域管理，精确地控制不同用户和角色对数据安全中心及数据资产的管理权限，帮助集团建立更加清晰、高效的数据安全管理流实现工作职责的明确划分，提高数据安全治理效率。同时，合规的数据访问控制有助于降低集团因数据安全不合规而面临的法律风险和经济损失。

**日程表

描述已自动生成**

**4.企业微信的原生结合**

改变传统以网络为基础的信任，通过与企业微信深度融合，建设以企微工作台应用为基础基于身份的信任机制。无差别对待从特定网络连接的用户，信任机制与其获得的服务和权限的高低无关；并针对用户的适度风险感知能力，全面过滤非法访问；同时实现动态访问控制，即所有对服务的访问行为必须经过认证、授权和加密处理。同时提供基于终端数据安全防护能力，包括但不限于敏感信息过滤、水印、防入侵等安全能力。