**金华市中心医院医联体**

**数据中心建项目院内市场调研需求书**



**2019年8月**

**目 录**

[第1章 医联体数据中心建设需求 3](#_Toc16341396)

[1.1 妇保院区数据中心建设需求 3](#_Toc16341397)

[1.1.1 数据中心建设目标及需求 3](#_Toc16341398)

[1.1.2 架构整体要求 4](#_Toc16341399)

[1.2 金华市中心医院数据中心主机及存储系统规划 5](#_Toc16341400)

[1.2.1 金华市中心医院外网业务系统规划需求 5](#_Toc16341401)

[1.2.2 金华市中心医院核心业务系统存储规划 6](#_Toc16341402)

[1.2.3 金华市中心医院应用系统数据对存储系统的要求 6](#_Toc16341403)

[1.3 金华市中心医院网络系统规划 8](#_Toc16341404)

[1.3.1 金华市中心医院网络系统建设需求 8](#_Toc16341405)

[1.4 金华市中心医院医联体网络安全规划 11](#_Toc16341406)

[1.4.1 医联体网络安全建设需求 11](#_Toc16341407)

[第2章 集成及服务要求 17](#_Toc16341408)

# 医联体数据中心建设需求

## 妇保院区数据中心建设需求

### 数据中心建设目标及需求

本次妇保院区网络系统项目规划，目标如下：

* 妇保院为金华中心医院医联体的一部分，此次项目建设需要考虑妇保院区核心HIS、LIS、PACS、EMR等核心业务系统的服务器资源，在规划时除考虑满足未来妇保院5年以上服务器性能及扩展需求外，还需要核心应用的安全性、扩展性，要求核心系统能够7\*24小时不间断提供服务，任意单点故障，业务不会受到影响； //计算资源、扩展性、高可用
* 在考虑上述核心业务系统的同时，还需要规划妇保院其它非核心业务系统的服务器资源，在规划时除考虑满足未来妇保院5年以上服务器性能及扩展需求外，要求非核心业务系统还需要满足安全性、扩展性的需求，同时能够支持资源的快速扩展，能够7\*24小时不间断提供服务；
* 规划建设妇保院区核心存储系统，存储系统除满足核心应用系统及非核心应用系统的数据存储外，需要考虑未来5年的存储空间扩展需求，同时由于核心应用系统与非核心应用系统对存储空间的性能要求不同，因此需要对存储系统单独规划，要求核心应用系统采用SSD存储介质，非核心应用系统可采用SSD+SAS介质。
* 由于存储系统承载在业务系统的所有医院数据，任何系统的故障均有可能造成医院业务系统的停机，因此要求存储系统除满足空间的需求外，还需要考虑系统的稳定与安全，要求此次系统双活设计，同时能够与应用主机、数据库结合，任意单点故障，对业务系统的运行不会造成影响，同时需求考虑与金华中心医院本院的建设的双活系统进行兼容与扩展；
* PACS系统除考虑数据库主机及存储系统外，还需要考虑大量的影像数据的存储，PACS影像数据由于数据体量大，规范采用大容量PACS存储系统，整体满足未来5年的PACS影像数据的存储需求，同时要求该存储系统具有安全性、稳定性及扩展性的需求
* 数据安全对于医院来说是信息化建设中的核心之一，如何保障妇保院的数据安全是此次项目必须考虑的问题，此次规划建设的数据保护系统能够提供对所有业务系统的数据保护（影像数据除外），同时要求RTO约等于零，RPO在5分钟内，同时需求考虑与金华中心医院本院数据保护系统的互为灾备与扩展，避免极端情况下的数据丢失的风险；
* 建设妇保院至金华中心医院的核心应用系统的灾备应急系统，当妇保院出现不可预见的故障时，能够通过金华中心医院快速提供服务；

### 架构整体要求

妇保院区在构建数据中心时需求综合考虑两个因素：

1、整体设计应能够满足本院信息化五年的业务需求，以高可用高扩展的建设思路来构建妇保院区的数据中心，但整体建设以满足当前5年业务需求出发，未来可随时根据业务需求进行动态的扩展，且对业务运行不能造成影响；

2、能够与金华市中心医院现有信息化架构进行有效整合，实现资源的共享与业务系统互联互通，数据中心能够实现对金华市中心医院的容灾扩展需求，即妇保院区数据中心即为本院的业务支撑平台，又为金华市中心医院的容灾平台，对整个数据中心资源实现充分的利用，同时为未来业务全面整合打下基础

## 金华市中心医院数据中心主机及存储系统规划

### 金华市中心医院外网业务系统规划需求

此次数据中心需要规划整合医联体金华市中心医院与金华市妇幼保健院两院业务系统，规划将妇保院的相关业务整合到中心医院主机基础架构平台，目前金华中心医院核心业务系统主机资源经过2016年数据中心更新项目及2018年虚拟化扩容项目建设后，核心业务系统主机资源相对充裕，但外网主机资源由于前期主机依靠软件供应商提供的一些主机资源，存储单点故障、管理复杂，故障后恢复业务系统慢的问题，需要对外网应用主机进行资源整合，满足未来医联体外网业务访问规划要求。

* 在规划时除考虑满足未来5年以上服务器性能及扩展需求外，要求非核心业务系统还需要满足安全性、扩展性的需求，同时能够支持资源的快速扩展，能够7\*24小时不间断提供服务；
* 存储系统除满足外网应用系统数据存储外，需要考虑未来5年的存储空间扩展需求
* 由于存储系统承载着外网所有业务系统的医院数据，任何系统的故障均有可能造成医院业务系统的停机，因此要求存储系统除满足空间的需求外，还需要考虑系统的稳定与安全，要求任意单点故障，对业务系统的运行不会造成影响，同时需求考虑与金华中心医院本院原业务系统的兼容与扩展；

### 金华市中心医院核心业务系统存储规划

金华中心医院此次项目急需对核心存储系统进行升级改造，以解决以下一些主要问题：

* 存储系统的数量较多，但年限久远使用规划比较乱，且数据分布较广，很多存储均为现在停产的老设备，目前或多或少存在问题，继续使用存在数据丢失的风险；
* 老存储基本单台运行，任何存储故障均会造成相关业务停机，甚至数据丢失的风险

需要对原有老存储系统进行重新评估、改造，并尽可能的将重要业务系统或数据迁移至新平台。

### 金华市中心医院应用系统数据对存储系统的要求

从金华市中心医院目前存储系统数据的分布来看，在业务系统数据对存储空间的需求主要来自于以下几个方面：

1. 核心应用系统对存储空间的要求；
2. PACS影像数据对存储空间的要求
3. 其它应用系统对存储空间的要求；
4. 存储系统要求双活设计，且能够与原有系统兼容，满足性能的同时，保证7\*24小时不间断运行；
5. 能够实现所有数据的保护，要求RPO与RTO均近等于0
6. 能够实现与妇保院的互为灾备。

具体要求如下：

* 存储系统除满足核心应用系统及非核心应用系统的数据存储外，需要考虑未来5年的存储空间扩展需求，根据各业务系统对存储空间的性能要求特点进行规划设计。
* 由于存储系统承载在业务系统的所有医院数据，任何系统的故障均有可能造成医院业务系统的停机，因此要求存储系统除满足空间的需求外，还需要考虑系统的稳定与安全，要求此次系统双活设计，同时能够与应用主机、数据库结合，任意单点故障，对业务系统的运行不会造成影响，同时需求考虑与妇保院进行兼容与扩展；
* PACS系统除考虑数据库主机及存储系统外，还需要考虑大量的影像数据的存储，PACS影像数据由于数据体量大，规范采用大容量PACS存储系统，整体满足未来5年的PACS影像数据的存储需求，同时要求该存储系统具有安全性、稳定性及扩展性的需求；
* 数据安全对于医院来说是信息化建设中的核心之一，如何保障金华中心医院的数据安全是此次项目必须考虑的问题，此次规划建设的数据保护系统能够提供对所有业务系统的数据保护（影像数据除外），同时要求RTO、RPO均近等于零，同时需求考虑与妇保院数据保护系统的互为灾备与扩展，避免极端情况下的数据丢失的风险，同时能够实现金华中心医院与妇保院间的互为灾备。
* 其于金华市中心医院不同应用系统对存储的空间及性能的要求不同，此次项目要求对存储系统根据不同业务类型及要求单独规划，且必须与原有系统整合优化，以满足双活数据中心要求，能够满足医院7\*24小时不间断运行要求。
* 建设金华中心医院至妇保院的核心应用系统的灾备应急系统，当金华中心医院核心系统故障时，能够通过网络访问妇保院的灾备应急系统。

## 金华市中心医院网络系统规划

### 金华市中心医院网络系统建设需求

本次金华市中心医院网络系统项目规划，主要建设需求：

* 建设金华市中心医院网络云平台，满足业务系统及医联体网络系统要求，并满足医疗多业务发展，向集中化、平台化、大数据化业务方向规划设计。
* 网络云平台网络设备与现有设备及平台无缝兼容，与现有设备实现统一管理及统一安全策略下发，将现有设备作为远程线卡加入云平台网络设备系统，使其虚拟为一套逻辑设备，进行端口扩展及集中管控，简化架构、简化业务部署和自动编排、方便维护。
* 网络云平台核心设备部署虚拟化技术，实现网络云平台高可用架构体系，在两个双活机房分别部署两台核心节点共计四台核心设备虚拟化设计，搭建网络云平台系统，满足双活机房业务及医联体业务互联互通要求，四节点核心设备4：1虚拟化部署，形成一套网络系统内所有核心设备同时转发数据且跨设备端口聚合，网络系统内设备具有统一转发表项，实现业务负载均衡和高可用性，如果其中一台设备或一条链路故障，对业务无任何影响，业务访问无感知，数据不停顿不丢失，保证整体业务系统可靠性和安全性。
* 医院有上百个业务系统，网络系统有多个网络域（数据中心区域、安全区域、终端接入区域、内外网互联区域、专线区域等等，其中专线区域又分：社保专线、银联专线、卫生局专线、区域医疗专线、医联体专线等等），每个业务系统及对应的网络域有不同业务访问需求，业务特点也不同，安全业务要求也不同，针对每块业务系统及对应网络安全域进行针对性安全划分和安全策略部署，保障整体业务安全，从网络系统划分角度需要网络核心设备具备一虚多技术（1:N），即把一台物理交换机虚拟成N台互相独立的虚拟交换机，每台虚拟交换机之间物理隔离、安全隔离，每台虚拟交换机有独立的硬件资源和管理权限，每台虚拟交换机独立配置、重启互不影响，满足医疗多业务共享核心设备的需求。且核心设备支持扩展硬件防火墙业务板、入侵防御系统业务板等安全业务板卡，为各隔离虚拟交换机间业务互联互通提供安全策略部署及深度数据包检测和入侵防范的硬件安全平台，同时将核心设备多虚拟一（4:1）和一虚多（1:N）相结合，按照业务及安全域划分，业务架构清晰，业务流程明确，实现对业务安全隔离，满足业务网络高可用架构，且充分利用核心设备交换能力，降低了用户投资成本。
* 网络云平台与现有设备及平台无缝兼容，保证业务高可靠高稳定运行。核心设备需满足多种业务类型互联，服务器区，需满足各种类型服务器接口：千兆光口、千兆电口、万兆光口、万兆电口，安全互联区，需满足各种安全设备接口：千兆光口、千兆电口、万兆光口，汇聚/接入层区，需满足各种接入设备接口：千兆光口、万兆光口，核心网络区：每节点核心设备间通过2\*40G接口部署虚拟化（支持100G线卡扩展）。每台核心设备需同时满足所有服务器节点、安全设备节点、汇聚/接入设备节点的互联，以上因端口数量统计不足导致设备无法互联，服务商按照方案要求免费提供线卡扩容端口，并保留一定端口冗余，满足未来业务扩展需求，并进行扩展能力说明（线卡扩展能力、安全线卡扩展能力、最大端口扩展数等）。
* 对金华市中心医院每大楼每楼层进行网络系统梳理统计，对整体网络（核心层、汇聚层、接入层）系统评估优化，运行多年设备及过保设备需更新替换，各网络节点单设备部署、单链路互联进行双机双链路更新完善，实现整体网络系统高可用架构，减小网络设备/链路互联不稳定运行给业务系统带来风险。以上未考虑周全及设备更新数量统计不足的，服务商免费补齐。
* 以上完整性方案规划涉及到各模块及线缆数量，请根据规划设计方案统一配置，如项目实施过程模块及线缆材料不足，服务商免费补全。

方案及技术设计要点说明：

* 对金华市中心医院网络系统内各网络设备配置策略进行详细梳理，整理各网络设备互联互通情况，统计各网络设备端口及光纤使用情况，满足各网络系统高可用互联要求，利于整体网络系统项目实施、核心设备割接、风险评估及保障措施等等。
* 针对医院各业务系统及特点进行方案说明，需分别针对不同业务系统进行网络系统规划设计，业务系统如：HIS、EMR、PACS、集成平台、医联体等等。
* 网络系统方案规划设计均可依据科学有效的算法，提供以数字为基础的计算方式，明确计算网络系统架构内：设备数量（配置情况）、端口数量、扩展能力、交换容量、包转发率、网络收敛比、模块数量、光纤数量等等内容，满足业务系统高性能、高密度、低延时、线速转发及高扩展性等要求，并结合实际业务能力的流量模型进行方案设计说明。
* 每核心设备节点满足正交CLOS架构（独立的交换网板和独立的主控板，交换网板与主控板硬件槽位分离，非主控芯片和业务板芯片分离，业务板卡与交换网板采用完全正交设计即槽位互相垂直）。核心设备支持FCoE技术，解决数据中心LAN网络和SAN网络异构，实现数据中心前端网络和后端网络架构的融合。支持SDN技术，将网络控制层和数据层分离，简化网络管理和维护难度，实现网络流量灵活控制，扩展以应用为中心的网络云平台。
* 医院业务系统需7\*24小时不间断提供服务，针对金华市中心医院本次网络系统方案设计、方案实施和方案割接（包括停机次数和停机时间窗口等）等内容，需有具体针对性方案内容，并提供对应风险预案和保障措施。以上实施内容如造成计划外业务系统停机，服务商承担一切损失。

## 金华市中心医院医联体网络安全规划

### 医联体网络安全建设需求

网络安全形势日益严峻，网络安全对信息化的威胁无处不在，因此此次金华中心医院医联体信息化项目网络安全的规划是否合理，也是本次项目考虑的重点，金华市妇幼保健院是金华市中心医院医联体中的重要组成部分，因此网络安全的规划除了要满足妇保院本身的信息安全要求外，还需要与金华市中心医院信息安全组成一个大的网络安全保障体系，统一规划统一管理，本次医联体安全项目规划建设目标如下：

* 建立完善的医联体安全技术防护体系，整合现有金华市中心医院网络安全平台相关设备、软件平台，根据网络安全等级保护的要求，结合医院网络安全信息现状，建立满足等级保护要求的安全技术防护体系，在满足安全合规基础上实现医院网络安全持续保护。
* 建立符合医联体要求的安全管理组织机构，健全信息系统安全管理制度。根据网络安全等级保护的要求，制定各项信息系统安全管理制度，对安全管理人员或操作人员执行的重要管理操作建立操作规程和执行记录文档。
* 制定医联体网络安全应急预案。应急预案是网络安全等级保护的重要组成部分，按照可能出现问题的不同情形制定相应的应急措施，在系统出现故障和意外且无法短时间恢复的情况下能确保生产活动持续进行。
* 提供针对性网络安全培训。为医联体信息化技术人员提供信息安全相关专业技术知识培训和全员安全意识培训。

金华市中心医院医联体网络安全主要建设需求：

* 本次网络安全主要内容是建立医联体的总体网络安全等级保护体系，根据金华市中心医院及妇保院医院业务系统及网络安全现状，进行安全风险分析及等保差距分析和安全需求分析，方案设计按照安全域划分，结合等级保护相关标准（落实安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心、安全管理制度、安全管理机构、安全管理人员、安全建设管理和安全运维管理等层面的要求）。建设总体网络安全体系，保障医院总体业务安全。
* 总体网络安全体系建设，符合相关国家政策文件要求：《中华人民共和国网络安全法》、《中华人民共和国计算机信息系统安全保护条例》等，符合相关等级保护标准要求：《信息安全技术 网络安全等级保护定级指南》、《信息安全技术 网络安全等级保护基本要求》、《信息安全技术 网络安全等级保护设计技术要求》、《信息安全技术 网络安全等级保护测评要求》、《信息安全技术 网络安全等级保护实施指南》等，符合相关卫生政策文件要求：《关于全面开展卫生行业信息安全等级保护工作》、《卫生行业信息安全等级保护工作的指导意见》等。
* 医院根据《信息安全技术 网络安全等级保护安全设计技术要求》（GB/T 25070-2019）以及业务系统管理的相似性、业务相近性，将安全域划分为互联网接域、对外服务器器域、内外网终端接入域、内外网运维管理域、核心业务域及其他业务域等。
* 针对医联体信息系统架构进行安全域划分，按照网络安全等级保护基本要求安全通用要求内的技术要求分类：安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心，各安全域内针对性的安全加固，满足一个管理中心三重防护安全体系，由安全通信网络到安全区域边界再到安全计算环境从外部到内部纵深防御路径，从传统被动防御到主动防御安全建设思想，完善网络安全分析能力、未知威胁的检测能力、安全工作的执行能力。

医联体互联网接入（包含中心医院与妇保院互联网出口域、中心医院与妇保院业务内网外联域、中心医院与妇保院两院互联域）网络安全需求：

* 安全通信网络需求：1.应避免将重要网络区域部署在边界处，重要网络区域与其他网络区域之间应采取可靠的技术隔离手段，2.应提供通信线路、关键网络设备和关键计算设备的硬件冗余，保证系统的可用性。
* 安全区域边界需求：1.应保证跨越边界的访间和数据流通过边界设备提供的受控接口进行通信，2. 应在网络边界或区域之间根据访问控制策略设置访问控制规则，默认情况下除允许通信外受控接口拒绝所有通信，3. 应删除多余或无效的访间控制规则，优化访问控制列表，并保证访问控制规则数量最小化，4. 应对源地址、目的地址、源端口、目的端口和协议等进行检查，以允许／拒绝数据包进出，5. 应能根据会话状态信息为进出数据流提供明确的允许／拒绝访间的能力，6. 应对进出网络的数据流实现基于应用协议和应用内容的访问控制，7. 应在关键网络节点处检测、防止或限制从外部发起的网络攻击行为，8. 应在关键网络节点处检测、防止或限制从内部发起的网络攻击行为，9. 当检测到攻击行为时，记录攻击源IP、攻击类型、攻击目标、攻击时间,在发生严重入侵事件时应提供报警。
* 安全计算环境需求：应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。

内外网终端接入域网络安全需求：

* 安全区域边界需求：1. 应能够对非授权设备私自联到内部网络的行为进行检查或限制，2. 应能够对内部用户非授权联到外部网络的行为进行检查或限制，3.与现有安全产品及平台无缝兼容。
* 安全计算环境需求：1.应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制，2. 应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换，3. 应采用两种或两种以上组合的鉴别技术对用户进行身份鉴别，且其中一种鉴别技术至少应使用动态口令、密码技术或生物技术来实现，4. 应对登录的用户分配账户和权限。

核心业务域网络安全需求：

* 安全计算环境需求：1.医院上百个业务系统，有BS/CS架构，访问方式有IP/域名访问，对业务系统负载均衡，提高业务系统的高可用性，2. 应提供重要节点设备的硬件冗余，保证系统的可用性，3. 应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换，4. 应采用两种或两种以上组合的鉴别技术对用户进行身份鉴别，且其中一种鉴别技术至少应使用动态口令、密码技术或生物技术来实现，5. 应对登录的用户分配账户和权限。

网络安全管理需求：

* 网络安全等级保护基本要求安全通用要求内的管理要求分类：安全管理制度、安全管理机构、安全管理人员、安全建设管理、安全运维管理，从要素到活动的综合管理思想。安全管理需要的“机构”、“制度”和“人员”三要素缺一不可，同时还应对系统建设整改过程中和运行维护过程中的重要活动实施控制和管理。
* 完善安全保护设施，建立安全管理制度，落实安全管理措施，形成信息安全技术防护体系和信息安全管理体系，有效保障医院信息系统安全。

等级保护评测需求：

* 协助医院业务系统开展等级测评，配合被测单位及时开展整改工作，消除网络安全隐患，提升网络安全保护能力，确保被测评系统达到网络安全等级保护的要求。

此次规划必须要根据目前金华市中心医院现有网络安全建设情况，结合妇保院相关网络安全建设需求，整合现有网络安全设备软件等相关资源，统一规划统一设计，建立一个满足医联体信息化安全未来5年规划需求、满足相关等级保护要求、满足信息化相关法律法规的网络安全保障系统。

# 集成及服务要求

|  |  |
| --- | --- |
| 条目 | 内容 |
| ▲系统实施 | 提供所有硬件设备的上架，系统的安装、调试。涉及到核心存储、核心网络的所有设备安装调试，包括与原有系统或平台的整合必须需要对应原有原厂工程师现场实施，所有涉及到原厂工程师相关费用包含在此次项目中。 |
| 需要负责协调现有应用软件（HIS、EMR、LIS、PACS等）的迁移工作，包括与应用软件厂商的交流和方案确定。所产生的所有费用均包含在此次项目中。 |
| 投标人需要根据目前硬件系统现状，结合此次项目的建设情况，设计并实施一个适合医院的高可靠的双活系统，在关键设备出现故障时不影响正常工作，同时又能够使系统的运行达到最佳状态。  投标人在系统升级割接过程中需确保过程顺利进行，系统割接过程须具有可回溯性，确保应用割接失败的回退。 |