项目方案

申报单位：威海市医疗保障局

项目名称：长护保险信息系统建设项目

目录

[第一章 项目背景及必要性 1](#_Toc23081)

[1.1 项目背景 1](#_Toc5002)

[1.2 建设目标 1](#_Toc22987)

[1.3 存在的主要问题和差距 2](#_Toc27724)

[1.4 项目建设的必要性 3](#_Toc4017)

[1.5 建设依据 4](#_Toc13500)

[第二章 现状与需求分析 8](#_Toc30748)

[2.1 现状 8](#_Toc13801)

[2.1.1 基础环境 8](#_Toc18027)

[2.1.2 网络系统 8](#_Toc21013)

[2.1.3 业务应用 8](#_Toc26289)

[2.1.4 业务数据 9](#_Toc29824)

[2.1.5 软硬件设备 9](#_Toc20700)

[2.1.6 运行维护情况 9](#_Toc12383)

[2.1.7 硬件列表 10](#_Toc25157)

[2.2 需求分析 10](#_Toc4278)

[2.2.1 功能需求分析 10](#_Toc22695)

[2.2.2 性能需求分析 12](#_Toc26616)

[2.2.3 安全需求分析 13](#_Toc8645)

[第三章 项目建设内容 13](#_Toc9616)

[第四章 项目设计方案 14](#_Toc3599)

[4.1 设计目标 14](#_Toc23856)

[4.2 设计原则 15](#_Toc24151)

[4.3 系统总体架构及技术路线 15](#_Toc1456)

[4.4 系统部署架构 16](#_Toc27624)

[4.5 应用系统设计 17](#_Toc20073)

[4.6 网络系统设计 18](#_Toc10647)

[4.7 安全系统设计 18](#_Toc2413)

[4.8 终端系统及接口设计 20](#_Toc27002)

[4.8.1 接口方式 20](#_Toc3997)

[4.8.2 关联系统及对接内容 21](#_Toc18767)

[4.9 其他系统设计 22](#_Toc26144)

[4.9.1 数据资源流程设计 22](#_Toc3329)

[4.9.2 数据资源规划设计 23](#_Toc28812)

[4.10 本项目产生的数据资源目录及与市信息资源共享交换平台对接要求 24](#_Toc3283)

[4.10.1 项目产生的信息资源目录列表 24](#_Toc13558)

[4.11 信创适配方案 27](#_Toc24752)

[第五章 项目组织管理 27](#_Toc27090)

[5.1 项目组织机构 27](#_Toc15104)

[5.2 项目进度安排 28](#_Toc14248)

[5.3 安全管理制度 29](#_Toc3914)

[5.3.1 安全管理体系 29](#_Toc1283)

[5.3.2 安全策略架构制定 30](#_Toc15784)

[5.4 人员培训 31](#_Toc22331)

[5.4.1 培训方式 31](#_Toc19758)

[5.4.2 技术文档提交 31](#_Toc15298)

[5.4.3 培训层次 32](#_Toc30062)

[5.4.4 培训课程 33](#_Toc5158)

[5.4.5 培训计划 33](#_Toc245)

[5.5 保障措施 33](#_Toc6927)

[5.5.1 技术保障 33](#_Toc14555)

[5.5.2 人才保障 43](#_Toc12829)

[5.5.3 制度及监理保障 44](#_Toc18838)

[5.5.4 检测保障 44](#_Toc18394)

[5.5.5 测试保障 44](#_Toc21430)

[5.5.6 日常运行维护保障 44](#_Toc24089)

[5.5.7 组织保障 46](#_Toc12087)

[5.5.8 管理保障 47](#_Toc15486)

[5.5.9 进度保障 47](#_Toc30715)

[5.5.10 售后服务 47](#_Toc32651)

[5.5.11 服务绩效评估标准及评估方式 50](#_Toc10761)

[第六章 项目投资 54](#_Toc8050)

[6.1 项目资金预算 54](#_Toc26810)

[6.2 项目资金来源和资金安排计划 60](#_Toc14280)

[第七章 项目绩效目标和风险分析 60](#_Toc5019)

[7.1 绩效目标 60](#_Toc2078)

[7.1.1 经济效益 60](#_Toc10704)

[7.1.2 社会效益 60](#_Toc16760)

[7.2 考核指标 61](#_Toc21753)

[7.2.1 服务绩效评估标准 61](#_Toc22774)

[7.2.2 服务绩效评估方式 61](#_Toc26545)

[7.3 项目风险与风险对策 62](#_Toc10461)

[7.3.1 人力资源风险 62](#_Toc9456)

[7.3.2 进度风险 63](#_Toc6887)

[7.3.3 质量风险 63](#_Toc16291)

# 项目背景及必要性

## 项目背景

为积极应对人口老龄化，妥善解决失能人员长期护理保障问题，2016年起国家组织承建了15个试点城市和吉林、山东2个重点联系省份，统一开展长期护理保险制度试点。2023年9月25号，山东省医疗保障局印发了《山东省长期护理保险模块省级集中工作方案》，方案提出：为推进全省长期护理保险业务健康平稳发展，在山东省医保业务基础子系统逐步省级集中的基础上，遵循国家版长期护理保险模块技术标准，规范推进各市长期护理保险模块省级集中工作，截止到2023年底，山东省已完成济宁、临沂、德州、滨州、菏泽、枣庄6个市的长期护理保险模块省级集中工作。今年我市也把长期护理保险制度的开展作为今年重点任务，为了进一步满足威海市长期护理保险制度实施和业务发展需求，确保长期护理业务经办的连续性、稳定性、安全性，保证各项政策业务需求变更响应的及时、有效，我市将积极推进完成长期护理保险模块省级集中工作。

## 建设目标

以长期护理保险制度的建设为核心，以信息化的建设为抓手，通过本项目，将大大提升威海市医疗保障局长期护理保险业务经办工作人员在业务经办时的工作效率，增强本地政策与信息化系统的适配度，以全面支撑长期护理保险全流程业务监管，全面支撑对护理人员、护理机构多层级、多机构、多角色的综合管理。针对挤占医保基金、护理过程监管不足等问题，构建起失能护理全过程监管体系，从而提高医保工作人员工作效率，更好的为失能人群提供优质服务，提高被护理对象幸福感，保障人民群众“老有颐养”。针对长期护理保险管理能力不足、产业发展产业协同动力不足等问题，建立方便、快捷、精细的服务管理和科学、精准、严密、全面的决策监管，推进建设安全、可靠的信息化平台，规范长期护理保险业务的经办流程、提升业务的办理效率、监控业务过程中发生的风险，配合监督部门对长护基金进行有效的事中和事后监管，有效促进长期护理保险业务健康开展，保障长护基金的健康持续运行。

## 存在的主要问题和差距

目前我市暂无可以支持长期护理保险业务全流程的信息化系统，无法全面支撑长期护理保险参保、待遇申请、失能评定、护理服务提供、服务评价、费用结算于一体的全流程线上业务管理，阻碍了我市长期护理保险制度的进一步开展，失能人员的长期护理保障问题不能更好的解决。

通过完成长期护理保险模块省级集中工作，将规范长期护理保险业务的经办流程、提升业务的办理效率、监控业务过程中发生的风险，有效促进业务稳定可持续发展，保障医保长护基金的健康持续运行。

## 项目建设的必要性

按照国家医保局和省医保局的要求，依据我市长期护理保险制度政策，对省局部署的国家版长期护理保险模块进行适配调整，以满足我市长期护理保险业务经办服务需要。

长期护理保险制度的落实作为全市重点工作内容，要求完善长期护理保险制度，加快实施养老服务高质量发展。持续提高城乡居民医保报销比例、扩大报销范围，促进基本医保和商业补充保险有效衔接。

根据上级主管部门指示，要求健全经办规程和服务标准，优化服务流程，加强对委托经办机构的协议管理和监督检查。加快长期护理保险系统平台建设，推进“互联网+”等创新技术应用，逐步实现与协议护理服务机构以及其他行业领域信息平台的信息共享和互联互通。

## 建设依据

1.《国家医保局 财政部关于扩大长期护理保险制度试点的指导意见》（医保发〔2020〕37号）

（1）基金管理。建立健全基金监管机制，创新基金监管手段，完善举报投诉、信息披露、内部控制、欺诈防范等风险管理制度，确保基金安全。

（2）服务管理。进一步探索完善对护理服务机构和从业人员的协议管理和监督稽核等制度。做好参保缴费和待遇享受等信息的记录和管理。建立健全长期护理保险管理运行机制，明确保障范围、相关标准及管理办法。引入和完善第三方监管机制，加强对经办服务、护理服务等行为的监管。加强费用控制，实行预算管理，探索适宜的付费方式。

（3）经办管理。引入社会力量参与长期护理保险经办服务，充实经办力量。同步建立绩效评价、考核激励、风险防范机制，提高经办管理服务能力和效率。健全经办规程和服务标准，优化服务流程，加强对委托经办机构的协议管理和监督检查。加快长期护理保险系统平台建设，推进“互联网+”等创新技术应用，逐步实现与协议护理服务机构以及其他行业领域信息平台的信息共享和互联互通。

2.《关于印发<长期护理失能等级评估标准（试行）>的通知》（医保办发[2021]37号）

按照文件要求，原有试点城市参照完善地方标准，原则上两年内统一到《评估标准（试行）》上来。

3.《国务院办公厅关于印发“十四五”全民医疗保障规划的通知》（国办发〔2021〕36号）

文件要求稳步建立长期护理保险制度，制定全国统一的长期护理保险失能等级评估标准，建立并完善长期护理保险需求认定、等级评定等标准体系和管理办法，明确长期护理保险基本保障项目。健全长期护理保险经办服务体系。完善管理服务机制，引入社会力量参与长期护理保险经办服务。

4.《中共山东省委 山东省人民政府贯彻落实<中共中央、国务院关于深化医疗保障制度改革的意见>的实施意见》

文中指出要创新长期护理保险制度，全面推行职工长期护理保险，开展居民长期护理保险试点，建立完善不同失能等级和护理模式管理服务标准体系。2021年职工长期护理保险实现全覆盖。2025年居民长期护理保险实现全覆盖。

5.《山东省人民政府办公厅关于印发山东省“十四五”养老服务体系规划的通知》（鲁政办字〔2021〕86号）

文中指出要健全多层次长期护理保障制度，加快构建由长期护理保险、社会救助、社会福利、慈善事业、商业保险组成的多层次长期照护保障体系，满足失能老年人照护服务刚性需求。全面实施职工护理保险制度，完善不同失能等级和护理模式管理服务标准，并逐步将参保范围扩大到城乡居民，2025年年底前，实现城乡居民长期护理保险全覆盖。

健全综合监管机制，明确部门职责，加强协同配合，建立健全以“双随机、一公开”监管为基本手段、以重点监管为补充、以信用监管为基础的跨部门综合监管机制，实现违法线索互联、监管标准互通、处理结果互认。明确监管重点，全面加强对安全质量、从业人员、涉及资金、运营秩序、用地建设等方面的监管力度，加大对各类违法违规行为的惩戒力度。

6.山东省医疗保障局关于印发《山东省长期护理保险模块省级集中工作方案》的通知（2023年9月25号）

为推进全省长期护理保险业务健康平稳发展，在山东省医保业务基础子系统逐步省级集中的基础上，遵循国家版长期护理保险模块技术标准，规范推进各市长期护理保险模块省级集中工作

(一)统一标准。长期护理保险模块省级集中工作，依据国家医疗保障信息平台建设统一规范，遵循国家版长期护理保险模块相关技术标准,省级统筹规划系统部署，统一信息平台和接口，统一数据管理。

(二)统一流程。各市长期护理保险业务经办流程要按照“应统尽统、应优尽优”的原则进行流程调整，减少各市业务流程差异化，实现长期护理保险主要业务流程全省基本统一。

(三)分步实施。根据各市长期护理保险系统建设时间、应用情况、业务模式，以及医保业务基础子系统建设等具体情况,，将全省18个统筹区分三批实施，到2024年底实现全省长期护理保险模块省级集中。第一批包括枣庄、济宁、临沂、德州、滨州、菏泽6个市，2023年底前完成省级集中；第二批包括济南、淄博、东营、烟台、潍坊、日照、泰安、威海、聊城、省直、胜利油田11个统筹区，2024年底前完成省级集中；第三批为青岛市，暂不省级集中，自行按照国家版长期护理保险模块相关标准规范完成本地系统升级工作，并持续做好数据归集工作，完成时间不晚于2024年6月底。待省局组织业务基础子系统省级集中时，同步完成长期护理保险模块省级集中工作。

# 现状与需求分析

## 现状

### 基础环境

威海市医疗保障局长期护理保险子系统将部署在山东省政务云机房，山东省医保局按照山东省大数据局、省电子政务云平台要求，系统部署在省政务云上，上云后医保云平台硬件设施和网络安全平台位于山东省政务云机房。

### 网络系统

山东省医保网络系统包括核心业务区、公共服务区等。目前医保业务纵向网络采用“一政一专”双线路连接到16地市医保局，专线的带宽为200M，通过专线与国家医保局互联，线路带宽为100M。横向网络通过电子政务外网、专线等模式打通了大数据局、民政、公安、银行等网络。采用山东省政务云互联网区提供公共服务。

### 业务应用

全市医疗保障信息平台在结合国家与山东省总体规划的基础上，统筹建设了公共服务类、经办管理类、智能监管类、宏观决策类、应用支撑类共等多个应用子系统。

### 业务数据

现有业务数据主要包括基础信息数据、医保业务数据、异地就医数据、公共服务数据、药品和耗材结算监管数据、医保精准扶贫数据、长期护理业务数据、医疗服务价格业务数据、智能监管审核数据等。

### 软硬件设备

目前，省医保局运行支撑环境内包含：存储设备10台，小型机5台，服务器480余台，网络设备70余台，网络安全设备20余台，机柜20余个等，部署于政务云医保域。

系统软件：数据库软件包括Oracle、MySQL，中间件软件包括Weblogic、Tomcat，操作系统包括AIX7.1、Center OS 7、深度linux、Redhat 7、Windows 2016企业版。

安全防护软件：核心防火墙、DDOS、IPS、防病毒网关、WAF、入侵检测、漏洞扫描、安全审计、数据库审计、杀毒软件。

### 运行维护情况

配置专业的运维团队，对山东省医保信息平台各子系统开展日常维护、故障处理、数据备份、安全维护等各个方面的维护。

### 硬件列表

本次项目建设属于在山东省医疗保障局长期护理保险子系统中完成威海市长护险政策及流程配置接入，且系统部署于省电子政务云平台上，因此本次项目建设的硬件设备基本利旧，无论是应用系统、数据库还是存储等，均不涉及硬件设备的采购。

## 需求分析

### 功能需求分析

长护待遇管理：在长护待遇经办业务办理过程中，经办人员为参保人进行待遇申请、申请变更、申请受理。经办人员为失能评估通过的参保人办理长护待遇登记及登记复核等业务。

失能评估管理：长护经办人员办理失能评估业务中，为参保人制定评估计划、评估计划变更、分配评估人员、录入评估结果、评估结论公示、争议复评、评估结论送达、评估任务中止等业务。

长护费用管理：长护业务经办人员在进行长护费用结算时，为参保人个人待遇进行申报、受理、审核结算，为护理机构申报的费用进行受理、审核结算等。

护理机构及人员管理：长护定点护理机构在业务经办过程中，需要对长护定点机构护理人员进行管理，包括新增、变更维护、审核等，对护理人员信息进行管理。

评估机构及人员管理：用于长护评估机构的新增、变更维护，对评估机构的资质、协议进行管理。

服务项目管理：用于地方护理服务项目的新增、变更维护、机构服务项目匹配审核、维护。

综合管理：长护业务经办人员在日常工作中需要对各类信息进行统计，长护综合查询中可查看一个参保人的多次待遇申请记录、与待遇申请关联的评估信息、待遇享受信息、费用信息等。经办人员对护理机构信息进行综合查询，对参保人医保住院的结算清单进行查询。另外需要按照国家要求上报的数据进行报表开发。

长护监管：对长期护理保险的基金进行监管和日常稽核，需要：实时视频，护理人员开始服务后，在地图中展示服务中的人员信息。经办人员可点击发起实时视频请求，通过实时视频监管服务情况；智能监控，设置监控规则，对申请、评估、护理、培训等环节的业务数据进行智能的筛查和审核；数据监控、建立山东省医疗保障局长期护理保险子系统全景视窗，通过统计报表及图形化技术手段，对关键业务指标、数据质量情况以及数据运行情况等统计数据进行监控及展示，对长护险系统运行、失能评估、护理服务、待遇支付等业务情况进行全方位掌控；智慧巡检，由经办机构生成巡检任务，指定巡检内容，指派巡检人员巡检长护险相关业务的办理情况，录入现场巡检情况、处理意见及处理结果。

移动应用：失能人员应用，可实现失能人员登录、失能申请、申请记录查询、评定结果、护理计划查询、护理记录查询、服务评价等功能；业务员/评估员应用，可实现今日评估、评估任务、评估记录、通知公告等功能；护理人员应用，可实现护理人员登录、今日护理、护理计划、护理记录、通知公告等功能。

### 性能需求分析

性能需求是医疗保障信息系统为配合其功能需求而需具备的特性，包括响应时间、吞吐量和精度三方面。性能需求的满足程度要受到系统架构、实现方式、网络和主机处理能力、系统安全要求等多种因素的综合影响。

由于近几年的技术发展，系统性能对业务经办产生了直接的影响，本系统需要大量进行数据的采集、清洗、转换、加载等数据整合工作，系统面向全市参保群众，数据量巨大，为了保证业务处理能力，需要提升整体业务系统性能。

### 安全需求分析

严格按照业务部门划分使用权限操作，具有完备的数据录入、修改、访问、使用、保密、维护的权限管理机制，采取一定的安全保护技术措施，建立系统权限、数据权限、角色权限三级安全体系结构，即根据业务工作需要，准确地划分网络信息系统的涉密等级、范围和人员，设置各部门的不同系统操作权限，在进入网络信息系统时，任何部门人员都必须进行登录注册，必须准确申报账号和密码。规定不同权限人员访问系统信息的合法范围，以控制不同权限人员只能操作和浏览一定的内容。

# 项目建设内容

按照国家医保局和山东省医保局的要求，依据我市长期护理保险制度政策，建设全面支撑我市长期护理保险参保、待遇申请、失能评定、护理服务提供、服务评价、费用结算于一体的全流程业务管理系统，满足我市长期护理保险业务经办服务需要。

完成与威海市医保局和山东省医保局相关系统对接，对接核心系统获取参保人基本信息、参保信息、单位信息、三大目录基本信息、自付比例、限价以及参保人的就诊结算数据。与省共享交换子系统对接，完成相关系统对接接口的申请及注册。

同时按照国家版长期护理保险模块的数据标准（包括命名标准、码值标准、数据结构标准等）及质量要求，整理本地长期护理保险历史业务数据，并导入威海市长护保险信息系统中，对导入的数据准确性及完整性进行验证，经系统测试后，完成系统正式上线。

后续为系统提供日常应用维护，负责日常业务经办过程中遇到系统问题的诊断及处理，对系统已实现的功能运行故障、BUG等问题进行修复维护，对系统中业务经办错误导致的错误数据及历史错误数据的修正，从而确保威海市长期护理保险子系统的稳定运行，为业务经办提供保障。

# 项目设计方案

## 设计目标

结合医保信息化特点，以“数据汇聚、整合为主线，提供及时、高质量的共享数据”为核心设计理念，将分散的数据资源进行汇集、整合，以“医保主数据”为核心的全局一体化数据建设管理思路，统一全局信息系统内各自独立管理的、分散的服务对象数据，确保服务对象在全局的唯一性识别以及服务对象数据的正确性和共享性。

## 设计原则

数据资源设计遵循以下原则：

1.实用性原则：以实用为第一准则，切实满足管理和业务需求；

2.安全性原则：设计采用有效的软件安全保护，防止非法入侵等攻击，保证子系统数据的安全；

3.先进性原则：设计采用先进软件技术，并考虑适度超前，为今后需求变化留有余地；

4.可靠性原则：技术成熟，保证子系统稳定长期运行；

5.可扩充性原则：采用先进开发手段，组件化的开发模式，以保证可扩充性；

6.标准化与开放性原则：系统设计符合标准化建设和开放的原则。

## 系统总体架构及技术路线

对系统总体架构进行层级结构划分，如下图所示：

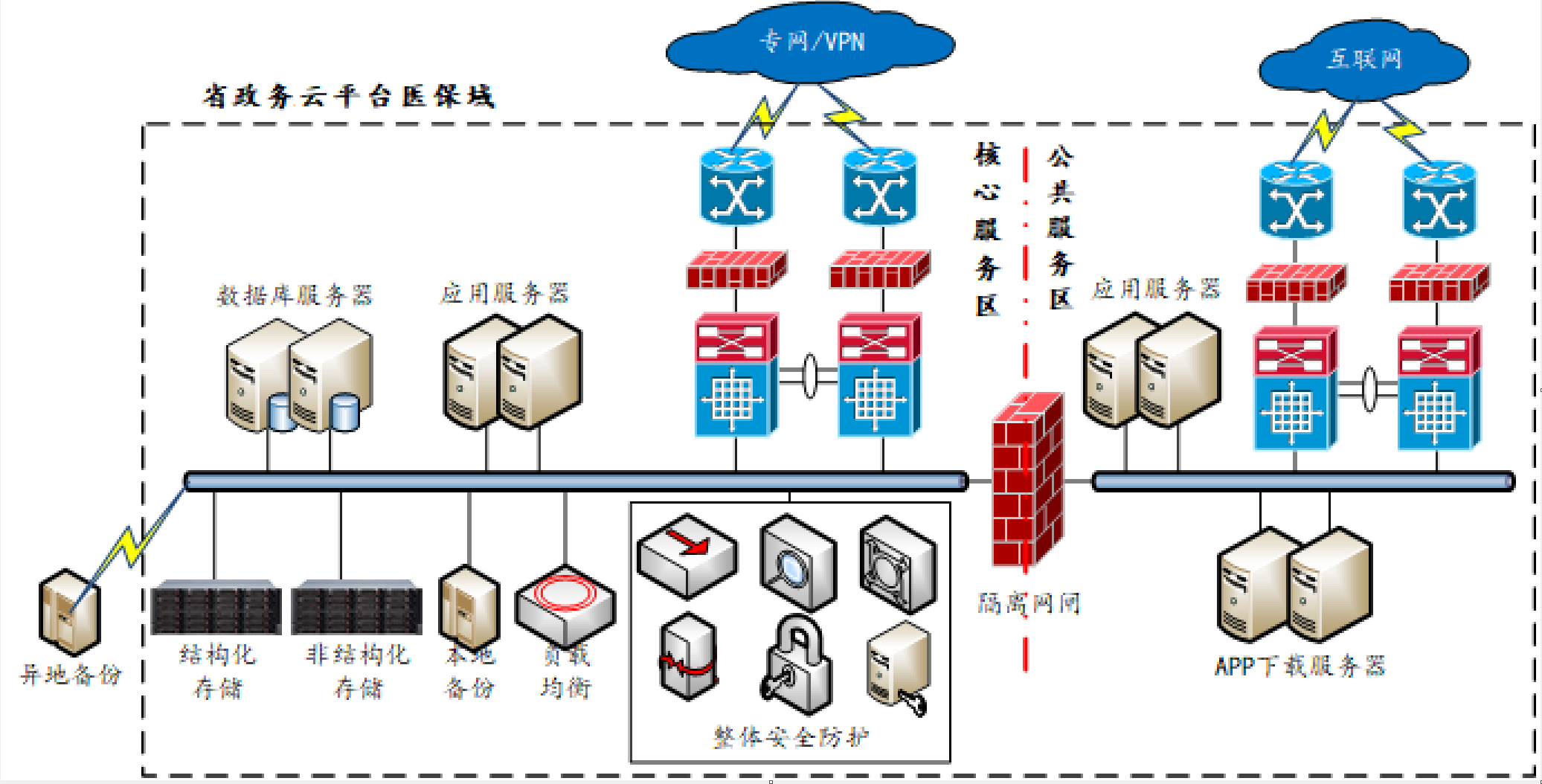


本次长护险子系统接入服务主要为了向医保业务经办管理人员、商保公司、护理机构及护理人员、失能人员提供包括待遇管理、护理服务、护理机构管理、费用结算、综合管理、商保公司管理、移动监管等多方面的功能服务。

项目建设将遵循信息化建设相关标准，信息安全及运维体系充分考虑安全对系统的重要性，采取必要的安全保护和信息保密措施，实现应用和数据等方面对非法侵入、非法攻击和网络病毒时具有很强的防范能力，通过合理的系统运维方式使整个系统正常、高效的运转。

## 系统部署架构

本次项目计划部署在政务云平台医保域的核心业务区和公共服务区。其中移动监管、智慧巡检等子系统部署在公共服务区，其他系统部署在核心业务区，两个网络区域需利用网闸或防火墙进行网络隔离，本次项目所需计算资源、网络资源、存储资源、安全资源均由政务云提供。行政服务区内分别部署业务系统数据库服务器、应用系统服务器等计算资源和结构化存储、非结构化存储、本地备份等存储资源，以及云平台整体安全防护平台和负载均衡，系统通过专网或VPN接入的方式对外提供服务。另外还需政务云提供异地备份服务，对平台业务数据进行异地备份。公共服务区部署应用服务器和移动端下载服务器等相关资源，供移动监管等子系统对外提供服务。具体部署情况如下：



## 应用系统设计

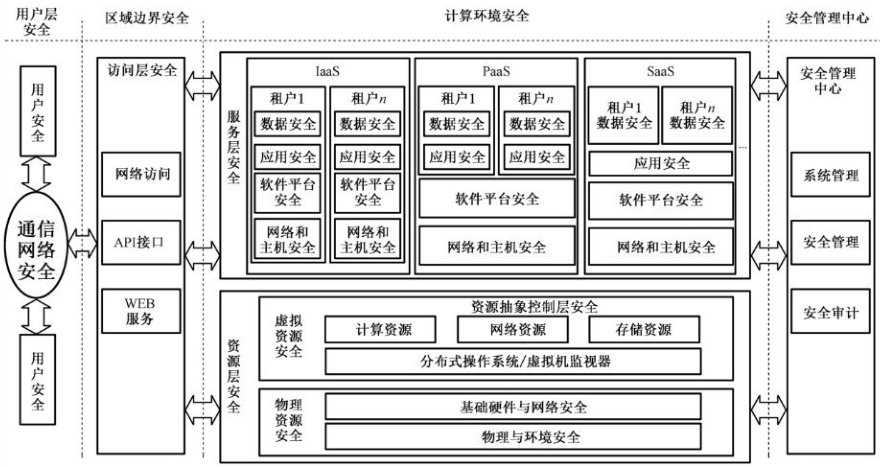
本次项目信息系统的建设采用了云计算技术，应用系统资源由政务云提供。政务云对应用服务器进行了资源池部署，可根据业务应用情况快速地搭建核心业务系统，并且可以灵活地根据业务负载情况弹性调整应用资源的大小，减轻运维压力，可以更好的节省时间和节约资金。

## 网络系统设计

本次项目业务系统部署在政务云环境中，系统网络同样由政务云搭建。医保专网区通过医保专网或VPN接入，对外向护理机构、护理人员等提供访问。

## 安全系统设计

本次项目长期护理保险子系统的安全系统建设依托于政务云安全环境，由政务云提供信息系统的整体安全防护服务。建议政务云参照信息安全技术网络安全等级保护基本要求，结合云计算功能分层框架和云计算安全特点，构建云计算安全设计防护技术架构，包括访问层、服务层、资源层、硬件设施层和管理层。其中一个中心指安全管理中心，三重防护包括安全计算环境、安全区域边界和安全通信网络。



系统通过安全的通信网络直接访问、API接口访问和WEB服务访问等方式安全地访问政务云提供的安全计算环境，安全计算环境包括资源层安全和服务层安全。服务层是对政务云所提供的服务的实现，包含实现服务所需的软件组件，根据服务模式不同，承担的安全责任不同。服务层安全设计需要明确政务云控制的资源范围内的安全设计技术要求，并且政务云可以通过提供安全接口和安全服务为云租户提供安全技术和安全防护能力。云计算环境的系统管理、安全管理和安全审计由安全管理中心统一管控。

## 终端系统及接口设计

### 接口方式

#### Web service方式

Web service方式接口实现数据和信息的实时调用，适应于交互数据量较小的情况。针对Web Service的数据处理模块，提供符合IEC标准的CIS组件接口规范，从其它系统或者应用对象获取数据模型。Web Service提供的接口要依据数据模型进行定义，确保与数据源传输接口的统一。

#### 消息方式

基于消息的接口方式采用基于消息交换机制实现数据交换，对于应用系统来讲，消息交换具备“存储转发”能力，因此消息方式具有“发射不管”的特点。基于消息的交换用于实现基于消息的系统间异步数据交换，采取消息发布/订阅和请求/响应模式，实现可靠（不重复、不丢失）、安全和高效的数据交换。消息交换机制上采用MQ方式，技术上采用JMS，并把接口API封装成服务方式，API分发送和接收两个方法。

#### 文件方式

文件导入方式适合批量导出导入形式的数据交换，通过格式文件导入的方式，将数据导入到信息系统，适应于交互数据量较小的情况。针对文件方式传递的数据处理，要依据通信规约中建立的模型以及模型中的元素来创建xml文件以及文件中的节点，保证和数据源传输接口的统一。

#### 中间库方式

中间库方式适应于交互数据量较大的情况。针对中间库形式的数据处理，是把数据通过数据库访问接口，写入中间库，其接口专用，速度快。要根据建立的对象模型形成中间库，提供统一数据传输接口。

### 关联系统及对接内容

#### 医保业务经办管理子系统

对接医保业务经办管理子系统，实现个人账户余额结算个人负担部分金额。经办机构查询当前已完成结算审核流程的结算申请，可对数据进行扣费和余额查询。扣费为通过医保核心相关服务查询当前人员医保账户余额，如果大于本次所需的费用，可进行扣费，再次调用医保核心相关服务扣除本次所需费用；否则提示余额不足，余额不足的可返还护理机构由护理机构对自费部分追缴。余额查询则查询当前失能人员医保账户余额。

#### 医保信息共享交换子系统

获取失能人员火化信息，在制定护理服务计划、护理服务执行的时候判断当前人员生存状况，验证失能人员是否符合护理服务的条件。避免人员死亡后继续发生护理行为，保障长护基金安全。

#### 数据资源管理子系统

查询的失能人员历史医保结算清单信息，辅助评估人员获得更加准确的信息用于现场评估；查询的失能人员历史医保结算清单信息，辅助护理机构推荐失能人员护理项目选择。

#### 定点专护机构信息系统接口

为了实现本次长护险相关功能服务的接入，在外部将对接本省多家定点专护机构信息系统，获取医疗护理全费数据，用于长护险医疗专护结算判断依据。

## 其他系统设计

### 数据资源流程设计

长期护理保险子系统与已建系统对接，从医保业务经办管理子系统中获取参保人基础信息、就诊信息；从数据资源中心获取失能人员就医的医保结算清单数据；从医保信息共享交换子系统获取失能人员火化信息。

### 数据资源规划设计

长期护理保险子系统所涉及的数据主要包括：长护待遇信息、参保人信息、医保个人账户消费信息、长护监管信息、护理培训信息、失能人员火化信息等结构化数据以及相关图片等非结构化数据。

## 本项目产生的数据资源目录及与市信息资源共享交换平台对接要求

本项目要求承建方严格按照《威海市政务信息资源共享管理办法》等政策文件的要求，主动与威海市信息资源共享交换平台对接，按照市信息资源共享交换平台提供的统一技术规范和接口，在项目验收前实现该项目使用和产生的所有信息资源库表数据梳理好信息资源目录并将数据实时归集到市信息资源共享交换平台。如承建方不能按要求完成对接，建设方不予进行验收。包括但不限于以下目录：（信息资源目录列表）

### 项目产生的信息资源目录列表

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 威海市长期护理保险子系统接入服务项目产生的政务信息资源清单 | | | | | | | | | |
| 序号 | 建设的政务信息系统名称 | 系统产生的信息资源名称 | 系统产生的信息资源概述 | 信息资源包含的信息项名称 | 信息资源的地域范围（省级/全省/全国等） | 信息资源对应的政务服务事项名称（非必填） | 信息资源对应的政务服务事项编码（非必填） | 信息资源的共享类型（无条件共享/有条件共享/不予共享） | 信息资源的开放类型（无条件开放/有条件开放/不予开放） |
| 1 | 威海市医疗保障局长期护理保险子系统接入服务项目 | 长护待遇信息 | 失能人员在护理机构享受长护待遇的情况 | 身份证 | 威海市 |  |  | 不予共享 | 不予开放 |
| 姓名 |
| 性别 |
| 年龄 |
| 区划 |
| 护理类型 |
| 评估等级 |
| 开始日期 |
| 结束日期 |
| 结算日期 |
| 费用总额 |
| 报销基数 |
| 个人负担 |

## 信创适配方案

本项目可应用政务云平台提供的国产化操作系统、数据库、中间件等信创产品，应用软件采用java语言开发，符合信息化建设要求。

在信创云平台服务器端、办公PC端和相关外接设备端都需要做好安全可靠环境保障，且提供了相关应用系统按照安全可靠环境适配进行对接接入的基础上，可对相关应用系统进行国产化操作系统、数据库、中间件、浏览器的兼容适配，以及安全可靠环境下服务接口、数据交换等兼容适配改造。

应用系统的运行存在有一部分中间件的支撑，运行环境更换后，也需对此部分中间件迁移制定对应策略。

应用系统软件由现有非国产化商用环境向信创环境迁移时，涉及到多种软硬件平台、编程语言和实现模式等多个方面，存在CPU指令集兼容性、操作系统兼容性、插件兼容性、数据库迁移等诸多问题，而且软硬件各版本之间也需要考虑兼容性，因此，需要针对应用本身和运行环境的多个方面进行具体分析，确定迁移内容和方法。

# 项目组织管理

## 项目组织机构

本项目管理和实施机构为威海市医疗保障局。

由医保局组织成立由项目实施机构、运行维护机构、承建厂商组成的建设管理机构，包括：项目领导小组、项目管理办公室、需求调研组、软件开发组、质量管理组、项目实施组。

各组责任处室（单位）和人员各执其责，相互协作，确保各项工作落实到位。

项目实施的工作包括：

1.编写项目可行性研究报告，组织项目方案论证。

2.研究、制定本项目实施管理规范并监督执行。

3.项目技术和管理标准和规范的制定，项目建设的调研、分析。

4.工程技术方案、工程设计书、设备采购标书等工程技术文件的编写审核，确定各系统的功能和技术指标。

5.制订工程实施方案和进度计划，组织工程实施、质量管理。

6.拟定项目验收办法，编制验收计划，确定验收范围，进行验收测试，组织专家验收，编写验收报告和工程验收移交。

7.负责项目信息安全目标的实现，管理项目安全系统的建设，进行源代码缺陷分析和安全性检测，完成安全保障体系测试、验收工作。

8.负责管理项目资金，根据有关规定审核项目资金支付使用。

## 项目进度安排

本项目预计建设周期15个工作日。具体日期按照招标采购后，合同签订日期为准。

## 安全管理制度

### 安全管理体系

安全管理制度是本项目整体信息安全体系结构的核心部分，负责安全体系的协调和管理工作，以实现系统的整体安全。安全管理在很大程度上涉及到人员管理和资源调配等方面的内容，因而也是整个安全架构中技术手段和管理手段结合较紧密的一个部分。本系统整体安全架构的安全管理部分的主要内容包括：安全管理体系的建立、安全管理策略的制定。

安全管理体制建设的主要内容是建立本系统内部的安全管理机构，在主管领导的直接管理下开展工作，通过技术人员与管理人员的密切协作逐步建立本系统内部的信息安全防范责任体系，将安全防范的责任逐级落实到每个具体操作人员的日常工作中。安全管理机构的具体职责包括：

（1）根据实际情况，组织全系统安全策略的制定；并随着本系统自身安全需求的变化及安全技术的发展，不断对安全策略进行修正与调整。

（2）根据系统的安全级别及安全风险确定所需的安全保护等级与措施。

（3）制定关键设备及资源的使用授权规则。

（4）制定与安全相关的操作规程。

（5）制定完备的系统维护制度。

（6）制定系统应急处理计划。

（7）对操作人员进行安全教育及安全操作培训。

### 安全策略架构制定

在安全需求调研的基础上，需要进一步提出一个机构内部的信息安全管理架构，对需要采取的技术和管理手段加以说明。该安全策略架构主要面向机构内部的安全管理人员，因此需要采用专业术语和规范的表述方法，力求表达得精确和一致。

安全策略架构的制定过程实际上是一个对安全需求说明中的组织机构内部安全需求进行大致分解的过程，即决定是由安全子系统（技术手段）或其工作环境（主要是管理方面的非技术手段）来满足特定的安全需求。

安全策略架构的技术手段部分需要将安全需求说明中的全部安全目标用适当的安全功能及其保证要求（或安全功能强度）进行说明，并给出必要的约束条件。而管理手段方面主要包括安全责任的落实、配套资源的配备和安全教育培训等方面。

## 人员培训

对医保业务经办人员、护理机构业务经办人员、系统管理人员进行系统操作培训。组织线下集中培训，线上培训根据具体情况适时开展。

### 培训方式

本次项目的培训采用集中授课式培训和线上培训两种培训方式。在项目实施完毕，以理论结合实际的形式对系统管理人员以及相关的业务经办人员进行全方位的培训，由承建方资深培训讲师主讲，主要的培训方式包括：

1）线上课堂培训：根据本项目需求确定培训的要求与培训体系，制定一整套的培训教材，组织相关业务部门进行集中的线上课堂培训。

2）现场培训：除了组织课堂上理论培训外，将另行安排承建方一线实施工程师到现场亲自示范指导业务系统的操作培训，提高业务人员的经办水平。

### 技术文档提交

技术专业关系到本项目的长期稳定运行，需要项目实施单位应提供如下技术文档或资料：

* 技术实现路线、项目管理方法论等；
* 全面的技术培训教材；
* 项目详细设计技术说明书。

### 培训层次

培训层次分为培训对象层次和培训内容层次：

1）培训对象层次

根据系统使用的角色不同，进行不同的层次培训，形成有差异化并倾向专业的培训。比如：系统管理人员培训；一线业务经办人员的培训；日常维护人员培训；其他合适的培训（如对有交叉业务的部门进行协同培训，以便业务办理能更好的协同办公）。

通过提供系统的培训，让系统各个环节的人更加专业化运用本系统，最大限度发挥其价值。

2）培训内容层次

* 统一培训

对各类培训对象统一适用的培训内容，如系统操作、系统管理方法论等。

* 专题培训

除了统一的培训方案外，根据系统具体运用中出现的问题，举行专题化培训，比如针对类业务经办培训。

* 阶段培训

系统运行过程会出现维护更新情况，对于较大的更新情况，针对性组织培训，以便业务部门更好的使用更新后的系统。

### 培训课程

培训课程的制定，针对不同的实际需求，采用基于角色的培训方式，最终目标是达到有益于系统长期安全、稳定的使用和运行。

### 培训计划

根据项目实际需求，无论是业务操作流程，还是详细系统操作，制定周密的培训计划，具体计划根据实际情况制定

## 保障措施

### 技术保障

本项目建设涉及技术复杂，技术领域广，所以要采用成熟、先进的技术，不能把项目建设当作“试验田”。在项目的实施上，要严格限定条件，注重选择项目的系统集成商、应用开发商和工程监理机构，避免技术风险的存在。为了确保项目的万无一失，科学应对本项目关键问题的处理，建立健全系统的应急技术支持响应机制，有效预防、及时控制和最大限度地消除各类关键问题的危害和影响，分析项目建设中可能存在风险因素，提供了一套相对应的应急技术保障方案。

（1）技术支持流程

①对系统突发事件进行分类

根据业务系统突发事件的发生原因、性质和机理，业务系统突发事件主要分为以下三类:

A.攻击类事件：指系统因计算机病毒感染、非法入侵等导致业务中断、系统宕机、系统瘫痪等情况。

B.故障类事件：指系统因计算机软硬件故障、停电、人为误操作等导致业务中断、系统宕机、系统瘫痪等情况。

C.灾害类事件：指因爆炸、火灾、雷击、地震、台风等外力因素导致系统损毁，造成业务中断、系统宕机、系统瘫痪等情况。

②按照突发事件的性质、严重程度、可控性和影响范围，将其分为一般故障、严重故障、重大故障、特级故障四级。

A.一般故障

系统中单个系统故障，但未影响业务系统运行，也未造成社会影响或经济损失的突发事件。

B.严重故障

系统中单个节点故障导致业务中断，可能造成较大业务影响或较大经济损失的突发事件。

C.重大故障

系统中多个分节点或骨干节点故障引起的多个业务系统长时间中断，可能造成重大社会影响和巨大经济损失的突发事件。

D.特级故障

特指发生不可预见的灾难性事故，如火灾、水灾和地震等。

③根据事件类别启动应急预案

根据以上定义的故障分级，当系统事件的要素满足启动应急预案要求时，进入相应的应急启动流程。

A.应急处理工作小组从业务人员或值班人员的故障申告、系统监控报告的故障告警中得知系统异常事件后，应在第一时间解决系统故障。

B.应急处理工作小组针对系统事件做出初步的分析判断。若是电源接触不好、物理连线松动或者能在最短时间内可自行解决的系统问题，及时按照有关操作规程进行故障处理，并报领导小组备案；否则，应急处理工作小组将故障大致定性为设备故障、线路故障、软件故障等故障之一，及时告知领导小组和受影响的相关部门，并采取措施避免事件影响范围的扩大。

C.应急处理工作小组向领导小组报告，在领导小组的授权后启动相应的应急预案。针对灾难事件和影响重要业务运行的重大事件，还要及时向上级机关进行报告。

D.应急处理工作小组根据故障类型及时与外部支持人员取得联系。其中，设备故障的，可与集成商联系；软件故障的，可与系统集成商联系，由系统集成商进行远程技术支持；线路故障的，可与电信运营商联系，三方密切协作力求通信线路在短时间内恢复正常。

E.应急处理工作小组在上级机构或外部支持人员的配合下，充分利用应急预案的资源准备，采取有力措施进行故障处理，及时恢复系统的正常工作状态。

F.应急处理工作小组通知业务部门系统恢复正常，并向领导小组报告故障处理的基本情况。重大事件形成文字资料，以书面形式向上级报告。

G.总结整个处理过程中出现的问题，并及时改进应急预案。

（2）技术支持响应时间

当出现紧急情况时，提供7×24小时服务响应，维护工程师在接到报障后2个小时内处理应用系统出现的故障，及时作出故障原因报告并提出有效措施加以解决。

（3）技术支持响应内容

①黑客攻击处置措施

A.当有关值班人员发现业务系统或网站内容被纂改，或通过入侵监测系统发现有黑客正在进行攻击时，应立即向系统管理技术人员通报情况。

B.系统管理技术人员应在三十分钟内响应，并首先应将被攻击的服务器等设备从系统中隔离出来，保护现场，并同时向应急处理工作小组领导通报情况。

C.系统管理技术人员负责被攻击或破坏系统的恢复与重建工作。

D.系统管理技术人员会同相关支持人员追查非法信息来源。

E.系统管理技术人员组织相关支持人员会商后，向应急处理工作小组组长汇报有关情况。

F.应急处理工作小组组长如认为情况严重，应立即向应急处理领导小组组长汇报。

G.应急处理领导小组组长组织应急处理领导小组召开会议，如认为事态严重，则立即向公安部门或上级机关报警。

②病毒处置措施

A.当发现有计算机被感染上病毒后，应立即向系统管理技术人员报告，将该机从系统上隔离开来。

B.系统管理技术人员在接到通知后，应在三十分钟内响应。

C.对该设备的硬盘进行数据备份。用反病毒软件对该机进行杀毒处理，同时通过病毒检测软件对其他机器进行病毒扫描和清除工作。

D.如果现行反病毒软件无法清除该病毒，应立即向应急处理工作小组组长报告，并迅速联系有关产品商研究解决。

E.应急处理工作小组经会商，认为情况严重的，应立即向应急处理领导小组组长汇报。

F.应急处理领导小组经会商后，认为情况极为严重的，应立即向公安部门或上级机关报告。

G.如果感染病毒的设备是中心服务器系统，经领导小组同意，应立即告知各相关部门做好相应的清查工作。

③软件系统遭破坏性攻击的紧急处置措施

重要的业务系统必须存有备份，与业务系统相对应的数据必须有多日的备份，并将它们保存在安全处。

A.一旦系统遭到破坏性攻击，应立即向系统管理技术人员、业务系统技术人员报告，并将该系统停止运行。

B.系统管理技术人员检查日志等资料，确定攻击来源。

C.由业务系统技术人员向应急处理工作小组组长汇报。

D.应急处理工作小组组长认为情况严重的，应立即向应急处理领导小组汇报。

E.应急处理领导小组认为情况极为严重的，应立即向公安部门或上级机关报告。

④数据库安全处置措施

A.主要数据库应按双机热备设置，并至少要准备两个以上数据库备份，平时一个备份放在机房，另一个备份放在另一个安全的场所。

B.一旦数据库崩溃，应立即启动备用系统，并向应急处理工作小组组长报告。

C.在备用系统运行期间，业务系统技术人员应对主机系统进行维修。

D.如果两套系统均崩溃，业务系统技术人员应立即向应急处理工作小组组长报告，应急处理工作小组如认为情况严重，应立即向应急处理领导小组组长汇报。同时通知相关科室部门暂缓使用业务系统和上传上报数据。

E.系统修复启动后，将第一个数据库备份取出，按照要求将其恢复到主机系统中。

F.如因第一个备份损坏，导致数据库无法恢复，则应取出第二套数据库加以恢复。

G.如果两个备份均无法恢复，应立即向应急处理工作小组组长汇报，并向有关厂商请求紧急支援。

⑤广域网外部线路中断紧急处置措施

A.广域网主、备用线路中断一条后，网络管理员应立即启动备用线路接续工作，同时向应急处理工作小组组长报告。

B.网络管理员应尽快判断故障节点，查明故障原因。

C.如属我方管辖范围，由网络管理员立即予以修复。

D.如属运营商管辖范围，立即与运营商维护部门联系，要求恢复。

E.如果主、备用线路同时中断，网络管理员应在判断故障节点，查明故障原因后，尽快研究恢复措施，并立即向应急处理工作小组组长汇报。

F.经应急处理领导小组同意后，应通知相关部门相关原因，并暂缓使用业务系统和上传上报数据。

⑥局域网中断紧急处置措施

A.局域网中断后，网络管理员应立即判断故障节点，查明故障原因，并向应急处理工作小组组长汇报。

B.如属线路故障，应重新安装线路。

E.如属路由器、交换机等系统设备故障，应立即通知供应商进行保修。

F.如属路由器、交换机配置文件破坏，应迅速按照要求重新配置，并调试通畅。

G.如有必要，应向应急处理领导小组汇报。

⑦设备安全紧急处置措施

服务器、存储设备等关键设备损坏后，值班人员应立即向系统管理技术人员报告。

A.系统管理技术人员立即查明原因。

B.如果能够自行恢复，应立即用备件替换受损部件。

C.如属不能自行恢复的，立即与设备提供商联系，请求派维护人员前来维修。

D.如果设备一时不能修复，应向处理工作小组组长汇报，并告之相关部门，暂缓使用受影响的业务系统。

⑧人员疏散、机房灭火预案

A.一旦机房发生火灾，应遵循下列原则：首先保人员安全；其次保关键设备、数据安全；三是保一般设备安全。

B.人员疏散的程序是：机房值班人员立即按响火警警报，并通过119电话向公安消防请求支援，所有人员戴上防毒面具，所有不参与灭火的人员按照预定的路线，迅速从机房中有序撤出。

C.人员灭火的程序是：首先切断所有电源，启动自动气体灭火装置，灭火值班人员戴好防毒面具，从指定位置取出气体灭火器进行灭火。

⑨供电中断后的设备运行预案

A.外电中断后，机房值班人员应立即检查是否启用了备用电源。

B.机房值班人员应立即查明原因，并向信应急处理工作小组组长报告。

C.如因内部线路故障，请办公室联系相关单位迅速恢复。

D.如果是供电局的原因，应立即与供电局联系，请供电局迅速恢复供电。

E.如果供电局告知需长时间停电，应作如下安排。

停电30分钟以内，由UPS供电；

停电30分钟—1小时，关掉非关键设备，确保关键服务器、核心系统设备供电；

停电1小时以上，关闭所有设备。

⑩关键人员不在岗的紧急处置措施

A.对于关键岗位平时应做好人员储备，确保一项工作由两人能够操作。

B.一旦发生关键人员不在岗的情况，首先应向应急处理工作小组组长汇报情况。

C.经处理工作小组组长批准后，由备用人员上岗操作。

D.如果备用人员无法上岗，请求上级单位或外部支持技术人员支援。

（4）应急技术保障措施

①应急演练

为提高系统突发事件应急响应水平，信息技术部门和相关部门应定期或不定期组织应急预案演练；检验应急预案各环节之间的通信、协调、指挥等是否符合快速、高效的要求。通过演习，进一步明确应急响应各岗位责任，对预案中存在的问题和不足及时补充、完善。

②人员培训

为确保本应急预案有效运行，应定期或不定期地举办不同层次、不同类型的技术讲座或研讨会，以便不同岗位的应急人员能全面熟悉并熟练掌握突发事件的应急处理知识和技能。

③硬件资源保障

为了在系统设备发生故障时能够尽量降低业务系统的受影响程度，须为相应的核心业务系统提供必要的备份设备与线缆等硬件资源，并且配备与现有设备兼容的设备，确保相似或兼容的设备可以在应急情况下调配使用。这些备份设备需预先采购并保存在专门位置。

④文档资料准备

包括系统工程文档、维护手册、操作手册、设备配置参数、拓扑图以及IP地址规范及分布情况等。

⑤技术支持保障

建立预警与应急处理的技术平台，进一步提高系统突发事件的发现和分析能力，从技术上逐步实现发现、预警、处理、通报等多个环节和不同的业务系统、系统以及相关部门之间应急处理的联动机制。

⑥公众信息交流

在应急预案修订、演练的前后，应利用各种信息渠道进行宣传，并不定期的利用各种活动，宣传系统等突发事件的应急处理规程及其预防措施等应急常识。

### 人才保障

项目的建设和实施涉及到信息系统的规划、标准规范的制定、系统的需求分析、建设、维护和应用推广等工作，建设工作技术性强、复杂度高，因此，项目的顺利实施，需要项目管理人员、网络技术人员、系统管理人员、需求分析人员、信息安全人员等各种信息技术人才，威海市医疗保障局会需要全面组织实施人才战略，建立完善培养、引进、管理、使用信息技术人才的工作机制，不断加强人才队伍建设，为实施本工程提供强大的人力保障和技术支持。威海市医疗保障局将建立专家咨询机制，邀请高层次、高水平专家作为技术支撑，参与建设顶层设计、方案制定、标准研究、评估论证等工作，确保建设质量。

### 制度及监理保障

信息化建设是一个复杂的系统工程，牵涉面较广，涉及部门和人员较多，需要一定的政策支持，才能有力地保障工程的顺利实施。在项目建设期间，应依据国务院和国家医保局的政策法规，结合威海市医疗保障局的职能与现状出台地方性法规、政府规章，形成更为完善的法规体系，为全面信息化建设提供法制保障。

### 检测保障

任何一个项目都存在质量风险的可能，为保证项目保质保量、按时进行，项目实施过程必须要有QA全程参与项目对项目实施过程进行全程跟踪，确保项目质量及产出物质量，或者通过第三方资深机构的介入实现对项目的实施质量和效果进行实时监控，确保工程质量。

### 测试保障

软件测试是项目建设过程中保证项目质量必不可少的环节，省医保局组织专业的测试人员组成测试小组，测试发现系统可能存在的各种错误和缺陷，避免带来风险。

### 日常运行维护保障

本项目日常运行维护从以下方面展开：设备维护、网络维护、安全系统维护、应用系统维护等。

（1）设备维护

设备维护对系统建设是很有必要的。好的维护方案和精心的维护，能够延长设备的使用寿命、减少设备故障，从而降低设备的维修成本。设备维护主要从以下几个方面考虑：检查设备环境的温湿度，注意加强降温与除潮、定期检查后台服务器的运行情况、定期对环境进行清洁卫生，去除杂物、定期检查各电源、线路、网线等的连接情况、对设备所在环境的安全保护，如区域保护和灾难保护等。

（2）网络维护

网络维护是网络管理中具体的实施和应用，离不开网络测试。建议网络维护采用自维的方式，由指定专人维护。维护措施注意以下几点：线缆的验证测试、网络部件的认证测试、光缆连接端面的检测、定期检查网线等的连接情况等。

（3）安全系统维护

由于资源部署在电子政务公共服务云平台，建议由信息网络中心指定专人维护。主要从应用系统安全防范、设备冗余备份、操作系统安全防范、检查防火墙、加强入侵检测、扫描系统使用、做好病毒防护、严格控制内部人员对网络共享资源的使用、数据库安全备份、增强安全防范意识等。

（4）应用系统维护

应用系统维护阶段的关键任务是，通过各种必要的维护活动使系统持久地满足日常业务经办需要。主要包括改正性维护、适应性维护、完善性维护、预防性维护。

包括对所有应用系统和支撑软件进行维护，工作内容主要是定期对所开发或购买的软件产品升级，以适应对已发现问题的修正及对新硬件平台的支持。同时，还应对新的软件版本进行必要测试，以保证各信息子系统在实际应用环境中的正常使用。另外，应积极组织人员，及时调整系统功能或增加新的功能，以满足业务管理和信息服务的需要。

### 组织保障

本次项目建设工作的发展大计。建议成立由威海市医疗保障局领导挂帅的工程领导小组，明确信息化建设的指导思想、总体目标、主要任务，统一威海市医疗保障局各级领导和全体工作人员的思想，认清形势，明确任务，调动一切积极因素，把科学的决策变为全体干部和工作人员的自觉行动，为全面实施本工程构筑可靠的思想基础。

项目将成立专门的工程执行和协调机构，并对规划的目标任务逐项分解落实，纳入工作目标责任体系，严格控制项目范围，立足当前，着眼长远，抓住重点，兼顾一般，有计划有步骤地稳步推进本工程的实施。

### 管理保障

制定科学的工程项目管理制度，保障工程实施的成功。通过规范、明确和落实项目建设各方人员的质量控制职责，在本项目建设过程中实施全面的质量管理计划，规定各种必要的质量保证措施，以保证项目的建设达到总体规划的目标，取得显著的实施效果。

本工程需要涉及到多个系统的配合，主要涉及省、市、县（区）三级。项目建设的范围很广，因此，整个项目的建设过程中需要协调好各方面的关系，保证项目的顺利实施。

### 进度保障

本项目建设项目尽管确定工期，在这过程中，难免出现不可预料的因素，控制项目进度、确保整个实施过程能够按照预定的时间表进行，对项目的成败至关重要。为保证项目按计划顺利实施，指定相关人员全程跟踪项目的实施情况，并把项目实施情况作为电子政务相关会议的主要议题，从人力、财力上给予大力支持。

### 售后服务

（1）服务内容

为保障本项目系统的稳定运行，为本项目需提供优质的软件维护升级服务，软件维护升级服务内容包括日常维护、应急性维护、适应性维护、完善性维护、整体优化服务、定期巡检服务、事故分析服务、数据梳理及优化服务等服务，保证系统的正常运行。具体的技术服务内容如下：

①日常维护

日常维护主要是针对系统操作人员在日常业务办理中，因为操作错误所引起的系统错误进行维护；以及对系统在开发过程中因各种原因遗留的bug进行修正，日常维护的内容包括：

A.日常操作操作维护；

B.日常数据错误维护；

C.应用系统3级缺陷修复；

D.日常操作培训。

②应急性维护

当系统出现系统整体性能急速下降，严重影响系统的正常运行，导致部分或全部系统不能正常办理时，进行应急性服务，在最短时间内，恢复系统正常状态。

③适应性维护

适应性维护是针对软件系统为适应外部环境的变化进行的系统修改活动，例如：作为行业的应用系统，政策调整不可避免，当系统已不能通过政策参数的调来适应政策调整要求的时候，进行应用系统的适应性维护。

为保证应用系统版本的一致性，此类完善性维护，由维护人员接受请求后，将应用系统的适应性需求提交给产品维护组进行统一的产品完善后，再部署到服务器上。产品维护组配备了一批技术力量强，熟悉本产品、经验丰富的工程师，对本产品进行统一的维护、测试，即保证了产品版本的一致性，也保证了产品设计的整体性，和应用系统的高性能，为系统的长期稳定运行打下良好基础。

④完善性维护

在应用系统运行过程中，由于多种原因，需要增加对应用系统功能，或对已有的功能进行改善。为满足此类需求，对应用系统进行完善性维护。

为保证应用系统版本的一致性，此类完善性维护，由维护人员接受请求后，将应用系统的完善需求进行统一的产品完善后，再部署到服务器上。产品维护组配备了一批技术力量强，熟悉本产品、经验丰富的工程师，对本产品进行统一的维护、测试，即保证了产品版本的一致性，也保证了产品设计的整体性，和应用系统的高性能，为系统的长期稳定运行打下良好基础。

⑤整体优化

系统经过一段时间的运行，随着业务的扩展，数据量的增加，系统性能有所下降在所难免。此时，需要对系统进行整体的性能优化，以保证系统高性能地稳定运行。

⑥定期巡检

为建立巡检档案，详细记录服务情况，对每次服务进行追踪；根据业务需求定制巡检计划，按计划定期为系统进行综合性的检查，以便及时发现问题，防患于未然。

⑦事故分析

在每一次故障排除或常规检查之后，都将做详细的记载，并做好存档；对每一次故障均做出详细故障原因分析报告，并提供系统维护资料和数据，及时给出适当建议。

（2）响应时间

自本项目正式投入运行和在服务期内，系统出现故障时，提供7×24小时服务响应，维护工程师在接到报障后2个小时内处理应用系统出现的故障，及时作出故障原因报告并提出有效措施加以解决。

### **服务绩效评估标准及评估方式**

#### 基本计分事项

①人员考勤

本项分值共10分。不定期抽查运维单位出勤情况，人数少于合同规定人数的每次扣除1分；运维负责人请假未通知甲方的，每次扣除2分；运维单位更换运维负责人未通知甲方的，每次扣除3分。

②日常巡检

本项分值共10分。运维单位应按照巡检计划完成巡检工作，不定期检查巡检情况，发现一次未巡检的扣除1分。

③运维完成率

本项分值共30分。80%≤运维完成率＜90%，扣除5分；70%≤运维完成率＜80%，扣除10分；60%≤运维完成率＜70%，扣除15分；50%≤运维完成率＜60%，扣除20分；运维完成率＜50%，扣除30分。

运维完成率 = 按时完成数量/需求提报数量\*100%

④问题重复率

本项分值5分。10%＜问题重复率≤20%，扣除1分；20%＜问题重复率≤30%，扣除3分；问题重复率＞30%，扣除5分。

问题重复率 = 90天内出现重复问题数量/问题总量\*100%

⑤数据修改

本项分值10分。需要后台开库调整数据，由运维工程师填报数据库调整申请单，经信息科相关负责人签字同意后，在指定堡垒机上执行，未走流程擅自开库的行为发现一次扣2分。

⑥版本发布

本项分值20分。版本程序发布未在需求论证约定的时间点上线的扣除2分；程序上线后发现1个bug，扣除1分；功能上线不完整需进行补充优化的，发现一处，扣除1分。

⑦投诉

本项分值共10分。发生有效投诉事件，每次扣除2分，情节严重、造成恶劣影响的，本项考核分数清零。

⑧违反行为规范

本项分值共5分。遵守医保局的各项规章制度，精神面貌饱满，穿着得体，谈吐文明，举止庄重。发现一次不遵守的扣除1分。

#### 其他计分事项

①信息泄露

发生数据安全事件（数据泄露），每次扣除20分；造成严重后果及恶劣影响的，追究维护单位违约责任。

②安全事故

发生安全事故，每次扣除20分；造成严重后果及恶劣影响的，追究维护单位违约责任。

#### 服务等级判定

|  |  |  |
| --- | --- | --- |
| 等级 | 整体评价 | 分数要求 |
| 优秀 | 很好地履行合同，现场运维力量充足，对运维事件响应及时，完全满足甲方运维需求，得到甲方好评 | 85≤分数≤100 |
| 良好 | 较好的履行合同，现场运维力量能满足运维需求，对运维事件响应及时，能满足甲方运维需求，得到甲方认可 | 75≤分数＜85 |
| 达标 | 基本能够履行合同，现场运维力量基本满足运维需求，对运维事件响应及时，勉强能满足甲方运维需求，甲方对运维服务评价一般 | 65≤分数＜75 |
| 不达标 | 不能很好地履行合同，现场运维力量不足，对誉为时间多次响应不及时，不能满足甲方运维需求，甲方对运维服务评价不合格或很差 | 分数＜60 |