6 基于平台的应用与业务协同

基于平台的应用与业务协同是医院信息平台的主要作用之一，其设计与实现和传统的独立的临床或管理系统的设计与实现有较大的差别。本章就基于平台的应用与业务协同进行分析，以供相关厂商在具体实现时参考。

6.1 基于平台的应用

本章节主要描述基于医院信息平台的应用，各应用基于平台的业务协同将在6.2 章节举例说明。

6.1.1 医疗一卡通

医疗一卡通系统，就是用户用同一张 IC 卡（或其他标识卡），实现多种不同管理、消费功能，例如挂号、收费、就餐、门禁、消费等，使得用户可以只携带一张卡片就完成多种用途，实现一卡通用。

医疗一卡通根据用户和使用的性质的不同，可以分为患者一卡通和员工一卡通两种，考虑到员工同时使用两张卡带来的不便，条件允许的情况下可以将员工一卡通和患者一卡通合二为一，这样可以大大方便员工的使用，也可以避免重复投资和建设。员工和患者一卡通合并需要注意一些事项，例如原来不同的发卡部门现在需要互相协调，严格的安全管理防止越权访问等等。

以下就患者一卡通和员工一卡通分别展开论述。

6.1.1.1 患者一卡通

患者一卡通系统目前在各医院的使用情况差异较大，在使用方式上主要有一卡多用和多卡兼用两种情况。在使用用途上有身份识别、小额电子钱包和通用借记卡三种。

大多数医院将一卡通系统作为患者身份识别使用，患者可持卡在院内各信息系统、监控管理系统间作患者身份证明。部分城市还要求医院读卡设备兼容社会保障卡、市民卡、诊疗卡、健康卡等区域内统一发放的第三方身份证明卡（多功

能卡）。

部分医院还将一卡通系统（存储卡或射频卡）当作电子借记卡，在院内充当消费结算工具。这种情况下医院会应用院内储值卡的方式，近年来医院与银行等金融机构合作或签署相关互认协议实现相关结算的模式也有应用。

患者一卡通系统根据不同用户的具体情况，主要用于满足患者、患者亲属以及其它访客的日常需要。卡片的发行对象为所有患者、患者亲属及其它访客，主要功能为身份识别和电子借记卡。

卡片可以是非接触式 IC 卡，也可以是其它类型的标识卡。

6.1.1.1.1 需求分析

患者一卡通主要有以下业务需求：

(1) 身份认证

持卡人在医院内活动，出入各种场所，使用各项设施，进行身份认证与信息管理，主要包括：

- 个人基本信息管理，患者身份标识；
- 医疗信息查询管理，功能如查询卡，主要用于自助触摸屏查询；
- 其他。

(2) 个人诊疗预付金帐户

此时卡除用作用户身份识别，还可以用于建立患者预付金账户（押金账户），在医院门诊、住院就诊时使用，可支持与医疗收费和身份识别相关的所有业务。卡作为持卡人在院内就诊的电子钱包（或账户）和身份认证载体，持卡人可以通过刷卡确认身份、缴纳挂号费、门诊缴费、住院结算等。

(3) 电子借记卡

持卡人在医院内进行非现金交易，与院方形成各种支付关系，通过电子钱包或电子账户进行结算，主要包括：

- 饭堂消费，功能如就餐卡；
- 定餐消费，功能如订餐卡，主要针对行动不方便的患者；
- 停车场付费；
- 院内其他代收代付。

6.1.1.1.2 主要功能

(1) 发卡业务

发卡业务主要对系统中用户卡、临时卡、操作员卡所有应用从发行到回收整个生命流程进行统一管理，它包括预发卡（印刷、分配卡号等预处理）、办卡、充值、挂失、解挂、作废、退卡、补卡等功能。

发卡时可手工录入患者基本信息，也支持二代身份证的扫描，直接获取患者信息。新患者产生新的患者 ID，对于姓名、性别、出生日期等组合条件完全匹配的患者自动提示，如果确认为同一人则不再生成新的患者 ID，避免患者标识的不唯一性。通过一卡通系统将患者在医院的多个身份识别号码（门诊卡号、医保卡号、门诊病历号、住院病历号、身份证号等）绑定在一个唯一的全局系统患者 ID 上。

发卡业务主要业务流程为：

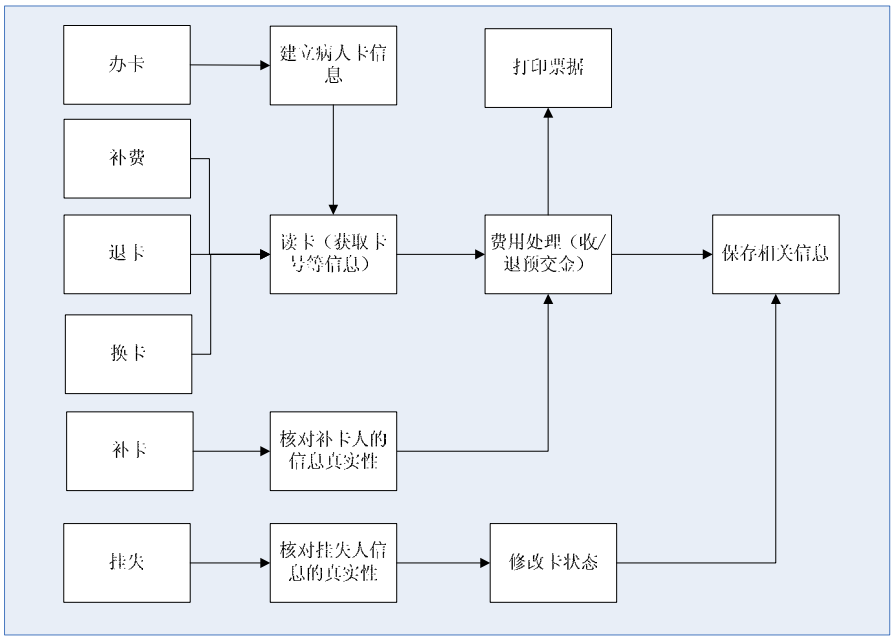


图 6-1 发卡业务主要业务流程图

(2) 消费管理

卡的电子钱包（或账户）功能可以取代现金交易，可以实现车辆停放计费、饭堂就餐消费以及其它院内缴费项目的刷卡消费，增加医院资金管理的安全性以及工作流程的方便性。医院内各个消费点的消费数据通过前置通讯服务器上传到

中心资料服务器进行统一处理，每个消费终端都可以独立地进行消费扣费操作，也可以转换成进行实时通讯的消费系统。

(3) 资金管理

资金管理主要用于对卡内电子钱包（或账户）进行现金充值，包括个人充值和团体充值，用于院内的消费、缴费等。还可以进行“取款”等特殊操作。

资金管理还需提供包括数据更正、数据平衡、数据备份、数据整理、财务结算、自动转账、资料汇总、统计分析、消费查询等功能，并对一卡通系统涉及的所有消费数据进行统一结算和划账。

(4) 查询管理

持卡人通过自助触摸屏查询自己的个人信息、缴费记录、用卡记录等情况。如此，既使患者能够方便地查询自己充值、消费的记录，增加信息透明度，又由于患者能够自助获得这些信息，一定程度上也减轻了医务人员的工作负担。

(5) 系统管理

系统管理包含资源管理、密钥管理、系统维护等子模块。

- 资源管理

资源管理子模块是系统中用户资料、权限管理和设备管理的资源总控，分为三部分：

人员资料管理：包括系统涉及的所有用户，包括用户（患者、患者亲属、其它访客等）、操作员、系统管理员等所有相关人员的文字信息以及照片。

设备数据管理：包括系统中涉及的所有设备，包括消费设备、圈存设备、前置通讯设备和读卡设备等的相关管理信息。

权限管理：针对不同级别和不同部门的管理人员和技术人员赋予不同类型的权限，并配以相应的登陆密码，使得每个人的管理权利和责任都区分明确，操作有据可查。

- 密钥管理

密钥管理子模块管理系统中的根密钥、机具设备密钥、用户卡密钥的生成、发放、更新、存储、应用和销毁工作。

- 系统维护

系统维护子模块提供系统初始化、系统参数设置、机具密码设置、卡密码设

置、操作日志、数据库设置等功能，完成对全系统的维护工作。

6.1.1.1.3 系统支撑环境

患者一卡通系统的应用需要医院内各相关应用系统的支撑与接口实现，其与院内其他系统的关系如图所示：

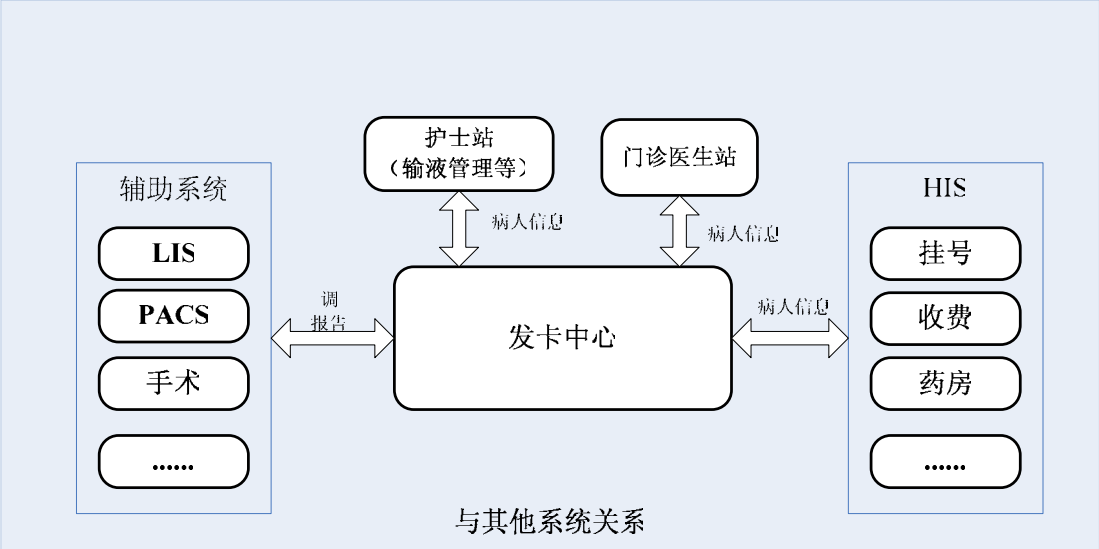


图 6-2 患者一卡通系统与其他系统关系图

各应用系统对患者一卡通的支持，传统模式是点对点的，由各个应用系统基于患者一卡通系统提供的接口分别进行改造。这种模式使得各应用系统与患者一卡通系统的耦合度很高，且部分功能（如患者资料登记）多处提供，没有统一规划，建议基于医院信息平台制定患者一卡通标准接口规范和统一业务流程，实现全院各相关应用系统的整合。

6.1.1.2 员工一卡通

员工一卡通系统主要完成医院的内部事务管理，系统集中了身份认证、门禁控制、就餐及购物消费等。员工凭一张员工卡，不仅可以作为工作证出入各办公场所，还可到食堂就餐或到超市购物。员工一卡通系统在提高了医院的内部管理水平及工作效率的同时，为员工创造了一种轻松、高效、安全的工作环境。

部分医院还将一卡通系统（存储卡或射频卡）当作电子借记卡，在院内充当消费结算工具。这种情况下医院会应用院内储值卡的方式，近年来医院与银行等金融机构合作或签署相关互认协议实现相关结算的模式也有应用。

医疗一卡通管理系统根据不同用户的具体情况，主要用于满足医院员工在医院内的日常事务处理，主要功能为身份识别和电子借记卡。

卡片可以是非接触式 IC 卡，也可以是其它类型的标识卡。

6.1.1.2.1 需求分析

员工一卡通主要有以下业务需求：

(1) 身份认证

员工在医院内活动，出入各种场所，使用各项设施，进行身份认证与信息管理，主要包括：

- 个人基本信息管理，功能如员工证
- 员工信息查询管理
- 其他

(2) 行政管理

员工卡可以是持卡人的电子门匙，用于开启医院内的各通道门禁，应用于主要通道、重要办公室、隔离病房和隔离区域、限制进入的检测室、内有贵重设备的实验室和机房、药房、招待所、设备间和仓库等。通过在卡上或门禁控制器上存储持卡人进出各通道门的权限和有效时段信息，可以实现严密而灵活的通道管理，有效而礼貌地防止非授权人员的进出。管理人员可以根据各通道门的安全级别自由地设置持卡人（或访客）进出各门的权限、有效时段以及刷卡认证、密码认证、卡+密码等多种开门方式。通过下载门禁控制器记录的进出记录，可以作为进出统计或事故核查的依据。

员工卡还可以对医院考勤工作进行统一的管理，包括人事考勤和后勤人员考勤。系统对固定节假日、考勤部门、考勤人员、考勤规则等要素进行统筹规划，员工只需要在到达和离开医院办公大楼的时候进行刷卡操作，系统即可根据打卡记录自动分辨员工的正常、迟到、早退、缺席等情况。同时在系统中登记员工的请假、外勤、加班等情况，最后将所有的数据汇总成报表以供人事部门进行评定工作。系统还可以针对特殊部门（如保卫处）设定复杂的“多时段”、“三班倒”等考勤规则。

(3) 电子借记卡

员工在医院内进行非现金交易，与院方形成各种支付关系，通过电子钱包进行结算，主要包括：

- 饭堂消费，功能如就餐卡
- 购物消费，功能类似电子借记卡
- 院内其他代收代付

6.1.1.2.2 主要功能

(1) 发卡业务

发卡业务主要对系统中用户卡、临时卡、操作员卡所有应用从发行到回收整个生命流程进行统一管理，它包括预发卡（印刷、分配卡号等预处理）、办卡、充值、挂失、解挂、作废、退卡、补卡等功能。

发卡业务的主要业务流程为：

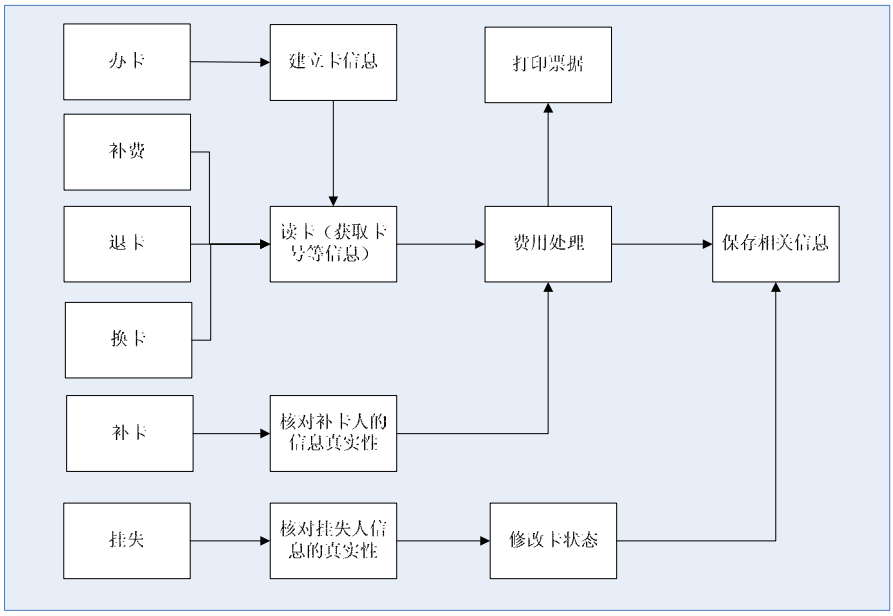


图 6-3 发卡业务主要业务流程图

(2) 消费管理

员工卡的电子钱包（或账户）功能可以取代现金交易，可以实现车辆停放计费、饭堂就餐消费以及其它院内缴费项目的刷卡消费，增加医院资金管理的安全性以及工作流程的方便性。医院内各个消费点的消费数据通过前置通讯服务器上传到中心资料服务器进行统一处理，每个消费终端都可以独立地进行消费扣费操

作，也可以转换成进行实时通讯的消费系统。

(3) 资金管理

资金管理主要用于对员工卡的电子钱包（或账户）进行现金充值，包括个人充值和团体充值，用于院内的消费、缴费等。还可以进行“取款”等特殊操作。

资金管理还需提供包括数据更正、数据平衡、数据备份、数据整理、财务结算、自动转账、资料汇总、统计分析、消费查询等功能，并对一卡通系统涉及的所有消费数据进行统一结算和划账。

(4) 查询管理

持卡人通过自助触摸屏查询自己的个人信息、考勤记录、缴费记录、用卡记录等情况。如此，既使员工能够方便地查询自己各种相关信息，增加信息透明度，又由于员工能够自助获得这些信息，一定程度上也减轻了管理人员的工作负担。

(5) 系统管理

系统管理包含资源管理、密钥管理、系统维护等子模块。

资源管理子模块是系统中用户资料、权限管理和设备管理的资源总控，分为三部分：

- 人员资料管理

包括系统涉及的所有用户，包括用户、操作员、系统管理员等所有相关人员的文字信息以及照片。

- 设备数据管理

包括系统中涉及的所有设备，包括消费设备、圈存设备、前置通讯设备和读卡设备等的相关管理信息。

- 权限管理

针对不同级别和不同部门的管理人员和技术人员赋予不同类型的权限，并配以相应的登陆密码，使得每个人的管理权利和责任都区分明确，操作有据可查。

密钥管理子模块管理系统中的根密钥、机具设备密钥、用户卡密钥的生成、发放、更新、存储、应用和销毁工作。

系统维护子模块提供系统初始化、系统参数设置、机具密码设置、卡密码设置、操作日志、数据库设置等功能，完成对全系统的维护工作。

6.1.1.2.3 系统支撑环境

员工一卡通系统的应用需要医院内各相关应用系统的支撑与接口实现，其与院内其他系统的关系如图所示：

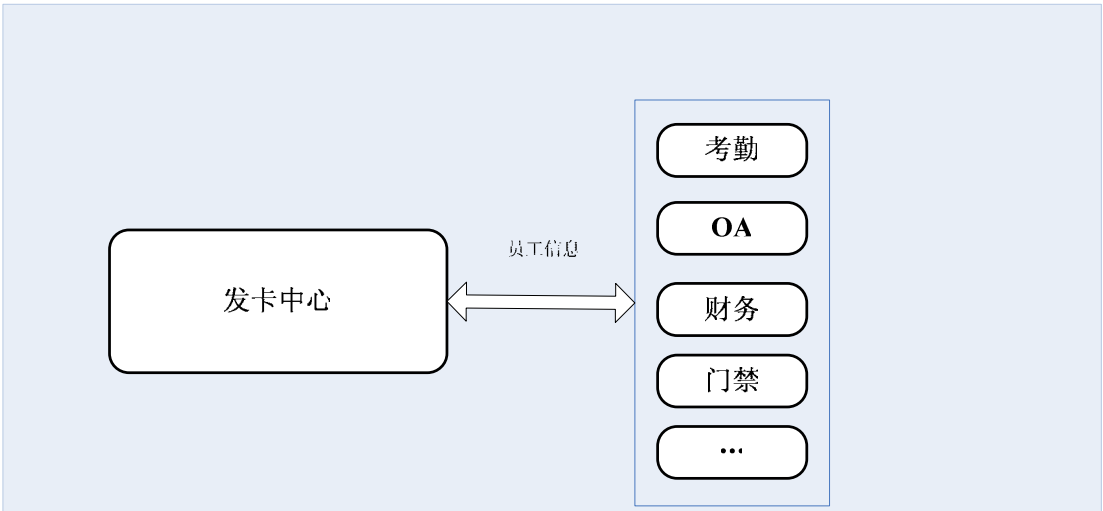


图 6-4 员工一卡通系统与其他系统关系图

各应用系统对员工一卡通的支持，传统模式是点对点的，由各个应用系统基于员工一卡通系统提供的接口分别进行改造，这种模式使得各应用系统与员工一卡通系统的耦合度较高，且部分功能（如员工资料登记）多处提供，没有统一规划，建议基于医院信息平台制定员工一卡通标准接口规范和统一业务流程，实现全院各相关应用系统的整合。

6.1.2 智能电子病历编辑器

电子病历编辑器是采集、录入并生成 EMR 文档的基本工具；是处理电子病历文书的核心组件；是形成结构化电子病历的关键工具。基于电子病历的医院信息平台中，电子病历编辑器承担着将所有业务系统完成集成以后的信息进行整合并按照 EMR 文档构造与存储要求进行存储与管理的职能。

电子病历编辑器包括所有生成 EMR 文档的电子文档编辑工具，包括病历书写、报告书写及其他动态记录文档的编辑器。

6.1.2.1 需求分析

电子病历编辑器要求完成信息集成后的 EMR 文档的生成，要求遵照卫生部、国家中医药管理局关于《病历书写基本规范（试行）》和《中医、中西医结合病历书写基本规范（试行）》、《电子病历基本规范（试行）》等相关要求。

6.1.2.1.1 支持结构化和自然语言混合的书写模式

支持卫生部病历书写规范中列出的所有病历文书类型，包括病历、病程、申请单、知情文件、其它记录、护理文书、图文诊疗报告等。这些病历文书类型各异，内容既有结构化的也有自然语言描述的，因此要求电子病历编辑器支持结构化和自然语言混合的书写模式。

6.1.2.1.2 支持表格、图形、上下角标的处理

表格在表达意思上的直观和准确性，在病历的专科检查和制式病历中具有广泛的应用，表格在版面排版的特殊作用，决定了编辑器要很好支持表格功能（如合并、拆分单元格等）。病历草图的标注在表达意思上有时比文字叙述更直观、明确，病历中经常用到。上下角标在产科病历中体现很充分。

6.1.2.1.3 支持多媒体形式的内容嵌入

实际临床业务发生时，各种临床信息系统都可能产生各类不同的基于多媒体形式表达的数据，如音频、视频、特定格式的电子文档（如 PDF）等。这些基于多媒体形式的数据也是临床信息的重要组成部分，电子病历编辑器必须支持将其作为电子病历或者 EMR 文档的一部分进行保存，无论是采用指针形式还是直接存储的形式。

6.1.2.1.4 能够适应内容结构变化发展的要求

由于医学技术的发展，会不断地有新的内容结构增加到病历中。而由于认识和技术手段的进步，原有的结构也会发生改变。电子病历的描述模型要能适应这种结构上的变化，能够支持新的结构类型并能保持历史结构。内容与结构在本质

上是可分离的，在表现时内容又必须与结构结合才能准确表达意思。由于病历是一种长期存储的资源，病历的内容及病历的结构不仅在书写时用到，而且在日后的查看中也需要用到，同时新旧模板的更替使系统要能准确地调用与内容对应的结构。

6.1.2.1.5 方便进行临床科研数据抽取

电子病历编辑器在制作模板时能够设置病历科研所需的数据项，保证这些数据能够始终存在，同时按照科研的要求设置必填项、按格式录入和对输入的数据能做必要的正确性检查，确保能正常抽取临床科研数据，满足科研需求。

6.1.2.1.6 痕迹保留

根据临床三级检诊的要求，病历书写要求进行痕迹保留，在电子病历书写的环境下形式上也应实现相应功能。而对非电子病历编辑器录入的其他来源数据也建议以数据来源为准，进行数据来源的修改痕迹保留。

6.1.2.1.7 多种展现形式

需要满足电子病历的多种展现形式，包括编辑模式、浏览模式，同时还需支持脱离电子病历系统环境独立浏览模式，为最终实现“数字病案室”、“区域医疗病案集中归档”、“区域居民健康档案”等奠定必要的信息转移基础。

支持多种病历打印输出功能，如整洁打印、续打、局部选择打印等功能。

6.1.2.1.8 智能化需求

电子病历编辑器除实现各种病历文书的基本编辑、查看、打印功能外，还需要基于医院信息平台集成临床知识库、相关医疗监管业务规则、相关业务流程控制等，以实现临床路径、病历质控、智能提醒、知识库应用等智能化功能，为医务人员提供全面、知识化、智能化的电子病历编辑工具。

6.1.2.2 主要功能

表 6-1 电子病历编辑器主要功能

功能	功能点	备注	等级	相关子系统
创建医疗记录	提供创建各类医疗记录的功能，支持卫生部病历书写规范中列出的所有病历记录类型。	病历记录含门诊病历记录，属文档型医疗记录	必需	医生工作站 护士工作站
	提供对创建的医疗记录指定医疗记录类型、标题、创建者并自动记录创建时间的功能。创建时间应至少精确到分钟。		必需	医生工作站 护士工作站
	提供补记医疗记录的功能，允许所补记记录内容所对应的时间不同于医疗记录的录入时间。	记录内容对应的发生时间不同于医疗记录本身的创建时间。如查房记录的查房时间不同于查房记录的创建时间。	必需	医生工作站 护士工作站
编辑录入	提供各类医疗记录录入编辑功能，支持卫生部病历书写规范中列出的所有病历文书类型。		必需	医生工作站 护士工作站
	提供根据医疗记录类型、内容要求和电子病历系统中的已有数据，自动生成医疗记录部分内容的功能	如在入院记录中根据数据库中的数据自动生成患者信息，在首次病程记录中根据入院记录中的主诉自动生成主诉内容	推荐	医生工作站 护士工作站
	提供医疗记录自由文本录入功能		必需	医生工作站 护士工作站
	提供在医疗记录中嵌入图片并对图片进行编辑的功能		推荐	医生工作站 护士工作站
	提供在医疗记录中嵌入表格并对表格进行编辑的功能		推荐	医生工作站 护士工作站
	提供在医疗记录中复制、粘贴患者其它医疗记录指定内容的功能		必需	医生工作站 护士工作站
	提供禁止复制、粘贴非患者自己的医		推荐	医生工作站

功能	功能点	备注	等级	相关子系统
	疗记录内容的功能			护士工作站
	提供在医疗记录中插入来自于电子病历数据中患者的基本信息的功能	基于平台	推荐	医生工作站 护士工作站
	提供在医疗记录中插入来自于电子病历数据中检查检验报告的功能	基于平台	推荐	医生工作站 护士工作站
	提供在医疗记录中插入来自于电子病历数据中医嘱信息的功能	基于平台	推荐	医生工作站 护士工作站
	提供在医疗记录中插入来自于电子病历数据中生命体征信息的功能	基于平台	推荐	医生工作站 护士工作站
	提供常用术语词库辅助录入功能	基于平台 常用术语包括：疾病名称、药物名称、手术名称、地名等	推荐	医生工作站 护士工作站
	提供在医疗记录中嵌入多媒体数据的功能	多媒体数据包括扫描仪、数码相机、摄像机、录音机采集的数据，如：文字、语音、音频、视频、摄影形式等	推荐	医生工作站 护士工作站
	提供模板辅助录入功能，可以按照疾病、医疗记录类型选择所需模板		必需	医生工作站 护士工作站
	提供整个医疗记录级别模板和内容片断级模板支持功能		必需	医生工作站 护士工作站
	提供结构化（可交互）模板辅助录入功能		推荐	医生工作站 护士工作站
	提供在医疗记录中保留结构化模板形成的结构功能	结构化模板可以只起到辅助录入作用，在形成的医疗记录中不保留结构；也可以在辅助录入的同事在形成的医疗记录中保留结构	推荐	医生工作站 护士工作站
	提供在医疗记录中插入来自于系统或外部的疾病知识资料库相关知识		可选	医生工作站 护士工作站

功能	功能点	备注	等级	相关子系统
	文本的功能			
	提供包含呈现样式的医疗记录录入编辑和保存功能	保留样式是指样式信息随着病历内容长期保存并能被软件解读和再现	推荐	医生工作站 护士工作站
	提供多种编辑方式，例如所见即所得的医疗记录录入编辑功能		推荐	医生工作站 护士工作站
	提供医疗机构定制医疗记录默认样式的功能	样式包括纸张尺寸、字体大小、版面设置等	推荐	医生工作站 护士工作站
	提供暂时保存未完成医疗记录（草稿）的功能		必需	医生工作站 护士工作站
	提供在医疗记录录入编辑过程中自动保存编辑内容并在系统出现异常中断的情况下恢复正在编辑文档的功能		推荐	医生工作站 护士工作站
	提供能够查看暂时保存的未完成医疗记录功能	授权的其他用户查看未完成医疗记录	必需	医生工作站 护士工作站
	提供防止对正在编辑的医疗记录另行打开编辑的功能	一个用户打开多个录入会话或者多个有权限用户同时打开多个录入会话	必需	医生工作站 护士工作站
	提供医疗记录确认完成和记录确认时间功能		必需	医生工作站 护士工作站
	提供医疗记录双签名功能，当医疗记录由不具备相应医疗资质的人员录入时，由该录入者和具备医疗记录资格的人员共同签名以示医疗记录完成	不具备病历记录资格的录入者包括实习生、进修生等，这些使用者可以录入医疗记录，但不能独立确认完成医疗记录	必需	医生工作站 护士工作站
修改	提供医疗记录的修改功能	修改包含删除	必需	医生工作站 护士工作站

功能	功能点	备注	等级	相关子系统
	提供自动保留医疗记录修改痕迹功能，对确认完成的医疗记录修改时，自动记录修改内容、修改人、修改时间	创建者自己未确认完成的医疗记录的修改不需要保留修改痕迹	必需	医生工作站 护士工作站
	提供医疗记录禁止修改的设置功能	按照一定的规则可自动对符合条件的病历设置为不能修改，如设置病历归档后不能再行修改	推荐	医生工作站 护士工作站
	提供对医疗记录修改权限管理功能，允许上级医务人员修改下级医务人员创建的医疗记录		必需	医生工作站 护士工作站
模板定义	提供用户自定义医疗记录模板的功能		必需	医生工作站 护士工作站
	提供对医疗记录模板的使用范围进行分级管理的功能，医疗记录模板使用范围包括：创建者个人、科室范围、全院范围		必需	医生工作站 护士工作站
	提供创建模板权限管理功能，能够对用户可以创建的模板使用范围进行授权	创建模板的权限从低到高依次为：创建个人模板、创建科室模板、创建全院模板	必需	医生工作站 护士工作站
	提供创建结构化（可交互）模板功能，可交互模板至少包含单选项、多选项、填空、不可修改文本等元素		推荐	医生工作站 护士工作站
	提供模板中定义自动宏替换功能，宏替换项可以是在医疗记录中经常出现的患者姓名、性别、主诉等内容		可选	医生工作站 护士工作站
	提供结构化（可交互）模板中，限定元素在录入时为必须点击项或必须填写项的功能	必须点击项和必须填写项是为了防止记录内容遗漏	可选	医生工作站 护士工作站
	提供结构化（可交互）模板中元素录入值合理性校验和元素录入值之间相关性校验的功能	如体温的合理值校验，性别与女性相关症状校验	推荐	医生工作站 护士工作站

功能	功能点	备注	等级	相关子系统
	提供结构化（可交互）模板中元素值的自动计算功能		可选	医生工作站 护士工作站
	提供模板中定义智能化控制功能，对用户的选择和输入项目进行合理性校验和约束	如阳性体征与阴性体征不能同时选择	可选	医生工作站 护士工作站
打印	提供病历记录按照最后版本（不含修改痕迹）打印功能		必需	医生工作站 护士工作站
	提供病历记录中的全部或部分医疗记录连续排版打印功能	连续排版是指医疗记录之间不新分页	必需	医生工作站 护士工作站
	提供打印指定医疗记录的功能		推荐	医生工作站 护士工作站
	提供打印指定页码病历记录的功能		必需	医生工作站 护士工作站
	提供医疗记录接续打印功能，按照医疗记录在整个病历记录中的排版位置进行打印		推荐	医生工作站 护士工作站
	提供病历记录按纸张装订双面印刷版式打印		必需	医生工作站 护士工作站
	提供病历记录打印预览功能		推荐	医生工作站 护士工作站
质量控制	提供按照时限要求对住院病历记录完成情况进行自动检查并对未按时完成的病历记录进行提示的功能	基于平台	推荐	医生工作站 病案质量检查系统
	提供住院病历各类医疗记录的完成时限定义功能	基于平台	推荐	病案质量检查系统
	提供在院患者病历质量人工审查所需的病历选取、病历阅览和缺陷记录功能		必需	病案质量检查系统
	提供对人工审查的病历标记审查时间、审查者的功能		必需	病案质量检查系统
	提供病历质量检查人员定义缺陷项目的功能		必需	病案质量检查系统
	提供将病历质量检查人员记录的缺陷病历及缺陷内容通知医生的功能	可在医生登录工作站时，提示其记录的病历存在缺陷	必需	医生工作站
	提供病历质量检查人员对缺陷病历的纠正情况追踪检查的功能		推荐	病案质量检查系统
	提供终末病历质量检查评分功能		推荐	病案质量检查系统

功能	功能点	备注	等级	相关子系统
	提供患者生命体征观察结果记录功能，生命体征观察项目包括：体温、脉搏、血压、呼吸、入出量等		必需	护士工作站
	提供护士自行增加生命体征观察项目的功能		必需	护士工作站
	提供符合卫生管理部门要求的患者体温单（生命体征单）的显示和打印输出功能		必需	医生工作站 护士工作站

6.1.2.3 系统支撑环境

电子病历编辑器对系统环境要求不应过于苛刻，主流 PC 或终端计算设备应当能支持电子病历编辑器的运行，包括可能的支持临床业务信息录入的便携或嵌入式设备。

6.1.3 计算机化医嘱录入

计算机化医嘱录入（Computerized Physician Order Entry，CPOE）是医生为了诊治其所负责的患者（尤其是住院患者），对医疗指令进行电子录入、处理及跟踪的过程。这些医嘱内容及当前状态通过医院信息平台发布到全院各相关科室的应用系统，负责执行医嘱的医务人员或相关科室（如药房、检验科、放射科、功能科、手术室等）可随时查询医嘱内容及当前状态，为诊疗活动提供支持。CPOE 需要基于医院信息平台的患者电子病历、临床知识库、相关医疗监管业务规则、相关业务流程的支持，使医生在录入医嘱的时候能够根据统一的业务规则和监管规则处理。例如基于药品知识库，可以及时了解药品的药理属性、药品剂量、药物不良反应、毒副作用、药物间的相互作用、过敏反应等。

CPOE 不仅仅是医生通过计算机录入医嘱，同时通过在医嘱录入过程中的用药检查、用药控制、联机提醒和警示，减少医嘱完成的延误，减少与书写或转抄有关的错误，减少不规范、不合理或错误的医嘱，减少医疗差错，保证医疗安全，提高工作效率，提高医疗质量。通过对医嘱生命周期的全程跟踪和监控，实现对医嘱的闭环管理。

6.1.3.1 需求分析

医嘱是医生根据病情为患者拟定的有关各种检验、检查、手术、治疗、用药、护理、膳食等具体的诊疗方案，由医务人员共同执行。根据医嘱的属性可对医嘱进行不同的分类。

按照医嘱时间属性可分为长期医嘱、临时医嘱和备用医嘱：

- ✓ 长期医嘱：有效时间在 24 小时以上的医嘱，超过医师注明的停止时间后即失效。
- ✓ 临时医嘱：有效时间在 24 小时以内的医嘱，在指定时间内执行。
- ✓ 备用医嘱：又叫“预测医嘱”，依病情需要，分长期备用医嘱和临时备用医嘱。长期备用医嘱，有效时间在 24 小时以上，超过医师注明停止时间后方为失效。临时备用医嘱，仅在规定的时间内有效，一般 12 小时以内，过期尚未执行则自动失效。

按照医嘱的类别属性可分为护理医嘱、饮食医嘱、治疗医嘱、处置医嘱、药品医嘱、检验医嘱、检查医嘱、手术医嘱、输血医嘱等。按照医嘱的状态属性可分为新开状态、提交状态、审核状态、执行状态、完成状态。

对于医嘱管理主要包括医嘱下达、传递、执行以及检验、检查申请及报告的管理，重点是支持住院及门（急）诊的各类医嘱，保障医嘱实施的正确性，并记录医嘱实施过程的关键时间点。医嘱管理详细要求参见卫生部《电子病历系统功能规范（试行）》。

6.1.3.1.1 符合临床诊疗规范的医嘱录入

医嘱贯穿于患者从入院到出院的整个诊疗过程，是发药、检验、检查、治疗、手术等临床业务活动的依据，是电子病历的重要组成部分；同时，临床业务中所有费用的发生都是来源于医嘱的下达和执行，医嘱是费用和病历的纽带和桥梁。

在医院信息化建设发展初期，由于基本没有医生工作站应用系统，主要是在护士工作站中提供医嘱录入及处理功能，医生仍然在纸质医嘱单上书写医嘱，由护士将纸质医嘱录入电脑转换成计算机化医嘱。但是这些医嘱基本上是以费用处理为目的的，部分兼顾发药与执行单的需要，在医嘱的设计上只考虑了计费、

发药与执行单的方便性，大多忽略了医嘱在临床上的标准和规范，医嘱项目大多为收费项目，往往遗漏了那些不产生费用的医嘱，其医嘱大多是不完整的，不规范的，尤其是检验、检查、手术等医嘱，用以计费为主要目的的医嘱项目来表达，缺乏临床诊疗中关键属性的描述，无法反映完整的医嘱信息。由于信息系统不能提供完善的医嘱录入及处理流程，医生在医嘱已录入电脑的同时仍需要保留纸张医嘱单。

随着医院信息化建设逐步向临床信息系统推进，符合临床诊疗规范的计算机化医嘱录入就显得尤为重要，CPOE 是 EMR 的核心构件，它建立在医护工作站基础上，是面向医疗的，能够承担传统纸质医嘱的全部功能，通过 CPOE 可以完全取消纸质医嘱。同时基于医院信息平台上的患者电子病历、临床知识库、相关医疗监管业务规则、相关业务流程控制等，使得 CPOE 更为智能。例如通过平台上药品知识库的支持，如药品的使用剂量、毒副作用、配伍禁忌等，通过对医嘱内容的自动逻辑检查，减少医疗过程中的差错，提高临床医生的工作效率与质量。

符合临床诊疗规范的计算机化医嘱录入系统，使得在临床信息化的条件下，医生仍然可以按照临床诊疗规范下达医嘱，保持诊疗思维的连贯性，在提高临床信息化水平的同时不影响医生的诊疗习惯。同时通过医嘱与临床诊断、治疗结果基于医院信息平台的整合与关联，还可为临床决策、科研教学提供依据，辅助医生提升医疗服务水平，真正体现信息化为临床服务而不是相反。

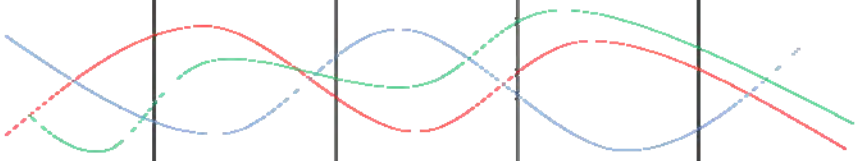
6.1.3.1.2 基于医嘱的临床图表

基于医嘱的临床图表（Clinical Chart）是指按照医嘱的时间顺序将医嘱按照护理、饮食、药品、处置、检验、检查、手术等进行分类，使用图表化的方式对医嘱全生命周期进行展示。在临床图表中可以使用曲线的方式展示患者生命体征情况，通过临床图表可以非常直观的了解患者在全诊疗过程中的医嘱信息及医嘱执行状态。以医嘱为主线贯穿整个医疗业务过程，可以非常清晰地反映患者的治疗过程，是临床医生了解患者情况、监控患者病情的工具。

临床图表以二维图表的形式对医嘱进行全方位的展示，X 轴表示时间顺序，Y 轴表示医嘱分类，中间表格为生命体征曲线图及医嘱信息和医嘱状态，对于检验、检查类的医嘱还能显示检验、检查结果的摘要信息。基于医嘱的临床图表展

示模式可参考下表：

表 6-2 临床图表

类别 \ 日期		1月1日	1月2日	1月3日	1月4日	1月5日
生命体征	体温 脉搏 呼吸					
护理		外科护理常规 二级护理		术后护理常规 一级护理		
饮食		普食				
药品						
检验		生化全套				
检查		腹部B超				
手术			阑尾切除术			
输血						
其它						今日出院

临床图表可以展示丰富的医嘱及相关信息，在临床图表的设计上应满足以下要求：

- ✓ 临床图表中 X 轴每页显示的时间间隔及数量可根据需要进行配置，可按指定的时间间隔向前或向后滚动，当日期变换时自动更新图表中的数据及图形。
- ✓ 临床图表中的医嘱分类项目可进行灵活定制，可显示全部医嘱项目或医生所关心的项目。
- ✓ 临床图表上部为生命体征曲线图，可根据需要查看详细的体征数据。
- ✓ 临床图表下部为该时间医嘱信息，可根据需要查看详细的医嘱信息。
- ✓ 对于医嘱项目可根据需要显示或查看更详细的信息，如皮试结果、检验、检查报告等信息。

6.1.3.1.3 医嘱闭环管理

医嘱的闭环管理是指从医生下达医嘱开始，护士确认医嘱，医嘱信息相继传递到各个执行部门（如药房、检验科、放射科、功能科、手术室等），药房进行摆药、发药、护士执行相关的药物及治疗医嘱，患者接受检验、检查、手术等，并返回相关的检验、检查结果，直到完成医嘱的全部过程进行管理。

通过医嘱的闭环管理，从医生录入医嘱开始，就可对医嘱的各种情况进行提示，可对护士执行医嘱的状态的进行监测和过程的提示，通过对医嘱的精确查询可以了解医嘱全过程的执行情况，建立完善的医嘱追述系统（Order Track System）,实现患者在诊疗全过程中的“可视化”监测和管理，确保在正确的时间对正确的患者使用正确剂量的药物，进而达到整体治疗目标。

在整个医嘱的生命周期中可以通过使用腕带、条码、射频等技术，采用 PDA、药房自动摆药机等先进设备在医嘱流程的各个环节中进行医嘱的执行及医嘱状态的确认，以提高效率、杜绝差错。

6.1.3.2 主要功能

医嘱录入系统包括的功能应该满足各类医嘱的录入要求和录入规范，由于药品、检验、检查、手术、输血、会诊、转科、出院等医嘱在录入时的要求是不相同的，因此对这类医嘱应该提供单独的录入界面，满足不同录入项的要求，录入完成后应提供自动转换为医嘱格式的功能。在医嘱执行的过程中应该提供医嘱提醒、医嘱复核、医嘱打印、医嘱卡片、医嘱执行、医嘱计费及医嘱查询等功能，详细的医嘱录入系统功能见下表：

表 6-3 医嘱录入系统功能列表

类别	功能	功能说明
医嘱录入	医嘱录入	包括医嘱的录入、修改、删除、作废、停嘱、重整等功能。 可录入药品、检验、检查、手术、输血、会诊、转科、出院等各类医嘱。 可通过调用成套医嘱快速录入。 药品医嘱录入过程中可进行合理用药的审核
医嘱提醒	医嘱提醒	对于新开、新停等所有变动医嘱提供及时提醒的功能，使护士及时了解和掌握医嘱变动情况，以便及时执行。
医嘱复核	医嘱复核	护士对医生提交的医嘱进行复核，对于有问题的医嘱退回给医生，医生修改后重新提交。提供按患者复核及批量复核功能。
医嘱打印	长期医嘱单打印 临时医嘱单打印	分为长期医嘱、临时医嘱的打印，需要提供医嘱续打、补打和重打功能。
医嘱执行	医嘱计划单	根据医嘱生成医嘱执行计划单
	医嘱执行卡	根据执行计划打印医嘱执行卡片，如口服卡、注射卡、输液卡等
	医嘱执行	根据医嘱执行计划执行医嘱、记录医嘱执行的信息，可通过PDA、平板电脑、移动推车在床边进行医嘱的执行
医嘱计费	医嘱计费	根据医嘱与费用的对应关系在医嘱执行后进行计费
医嘱查询	医嘱信息查询	医嘱信息及医嘱状态的查询功能。
	临床信息查询	查看各类检验、检查报告单等临床信息数据。
临床图表	医嘱临床图表	提供医嘱临床图表功能，按照时间分类展示医嘱
医嘱维护	医嘱字典维护	对医嘱字典进行维护，医嘱字典包括饮食医嘱、药物医嘱、检验医嘱、检查医嘱等
	成套医嘱维护	成套方案包括常规医嘱组套（入院常规、术前常规、术后常规）和针对患者诊断相匹配的治疗方案。
	医嘱权限维护	医嘱权限包括开医嘱的权限（处方权、开单权）和用药权限（精神药权限、毒性药权限、麻醉药权限、抗生药权限、贵重药权限等）

6.1.3.3 系统支撑环境

由于医嘱贯穿了患者整个诊疗过程，涉及到用药、检验、检查、手术等各种医疗环节以及各种费用的记账，所以在实施 CPOE 前必须已建设了 HIS、LIS、RIS/PACS、手术麻醉、EMR 等系统，并且这些系统已进行了良好集成，实现了互联互通和信息共享。

6.1.4 管理辅助决策

管理辅助决策是一种典型的基于平台的应用，基于平台积累的大量数据为医院管理提供辅助决策。通过医院管理辅助决策系统，让医院管理阶层从各个维度随时了解医院运营情况，衡量医院对于目标的达成程度，并及早发现过程中可能发生的问题，以便及早补救已经发生的问题，并防止可能发生的潜在问题。为医院管理者的决策提供科学依据，从而使医院在竞争中立于不败之地。

6.1.4.1 需求分析

医院管理辅助决策的内容极其广泛，贯穿医院经营活动的始终，是整个医院管理的核心。经营决策的正确与否，关系到医院能否健康发展，甚至关系到医院的生死存亡。决策者由于无法及时访问高质量、全面、可靠、个性化的运营和财务信息，因而在制定关键决策时常常感到压力巨大。如何将来自医院的多个数据源的数据（历史数据和近期数据）整合到一起，并将数据转化为关键洞察力来支持战略决策制定、推动持续的业务流程改进和促进整个医院协调一致，是医院发展方向上的战略性问题。

医院管理辅助决策的数据来源于不同的信息管理系统，有临床诊疗、医疗管理及后台运营管理等，数据以不同的格式保存。从总体看，数据是无组织的，需要对数据进行数据清理，继而对预处理过的数据进行转换，再按某分析主题进行组织和展示。可以获取任意时间的任意即时数据，即实时分析处理数据，使用者可以随时了解到医院当时的各种情况，同时系统能从不同角度对数据进行分析，并快速高效的获得结果，有助于全面了解隐藏于数据中的有用信息，方便领导决策。

6.1.4.2 主要功能

6.1.4.2.1 主题分析

表 6-4 门诊业务主题分析

主题	子主题	主要分析维度	作用	数据来源
门诊工作情况	门诊收入情况	时间、科室、医生、收费项目、药品类型、挂号类型、病种、患者来源区域、患者年龄段、患者类型、日期	医院门诊工作情况多方位展示、以利于工作安排合理化、进行经济分析预测	HIS
	门诊收费情况			
	门诊处方情况			
	门诊工作情况	接诊状态、时间、科室、挂号类型、病种、患者来源区域、患者年龄段、医生、收费项目、药品类型、患者类型		
	门诊医生出诊情况	医生、挂号类型、时间、科室		
	门诊药品情况	药品名称、药品类型、生产厂家、销售金额、时间		
门诊挂号情况分析	门诊挂号人次	挂号类型、挂号类别、时间、挂号状态、科室、医生、患者年龄段、患者类型		
	门诊挂号时间段			
	门诊挂号类别分析			
	门诊挂号诊别分析			
	门诊挂号退号构成			
门诊就诊情况分析	门诊人次费用分析	时间、科室、医生、收费项目、药品类型、挂号类型、病种、患者来源区域、患者年龄段、患者类型		
	门诊工作效率分析			
	门诊票据打印情况			

表 6-5 住院业务主题分析

主题	子主题	主要分析维度	作用	数据来源
住院工作情况	住院工作情况	时间、科室、医生、病种、患者类型	医生住院工作情况多方位展示，以利于住院工作安排合理化	HIS
	住院患者转科情况			
	住院患者转区情况			
	住院患者科转区比例			
	出院患者治愈率情况			
	住院诊断分析			
	在院人数分析			
住院患者分析	住院患者来源分析	时间、科室、医生、病种、患者类型、费用类别	合理化病床安排，提高病区服务质量	
	住院患者费别构成分析			
住院收入分析	住院收入分析	收费项目、时间、科室、医生、病种、费别、患者来源、患者类型	为决策提供参考	
	住院患者退费构成比			
	住院收入业务构成分析			
住院医嘱分析	住院医嘱量分析	医嘱开立科室、医嘱执行科室、医嘱类型、收费项目、医生、时间、病种、费别、患者来源、患者类型	为医生工作效率考核作依据	
	住院医嘱构成分析			
	住院医嘱 80/20 分析			
住院药品分析	住院药品分析	药品品名、药品类型、生产厂家、销售金额、时间、科室、医生、	控制药比	
住院疾病分析	疾病攀升率分析	病种、收费项目、时间、医生、病种、费别、患者来源、患者类型、患者年龄	通过历史疾病发病情况分析出疾病发病规律，合理安排工作	
	疾病发病率分析			
	病种趋势分析			
	病种年龄构成比分析			
	在院患者疾病占比分析			

表 6-6 手术业务主题分析

主题	子主题	主要分析维度	作用	数据来源
门诊手术	门诊手术例数分析	时间、科室、医生、病种、患者类型、收费项目、手术项目、患者年龄段、手术时长、手术执行科室、手术申请科室	为决策提供参考	HIS、手术系统、麻醉系统
	门诊手术攀升情况			
	门诊手术占比分析			
	门诊手术执行效率分析			
	门诊手术收入分析			
住院手术	住院手术例数分析	时间、科室、医生、病种、患者类型、收费项目、手术项目、患者年龄段、手术时间段、手术执行科室、手术申请科室		
	住院手术攀升情况			
	住院手术占比分析			
	住院手术执行效率分析			
	住院手术收入分析			

表 6-7 成本核算主题分析

主题	子主题	主要分析维度	作用	数据来源
成本分类分析	固定成本	时间、科室、人员、设备	通过对成本进行数值监控，使管理层能做到实时监控重要之处及抓住主要因素、降低成本费用	财务系统、HIS系统、统计病案管理系统、人力资源系统等
	变动成本	时间、科室		
	资产与负债分析	时间、科室		
效益投入产出分析	业务收入情况	时间、科室、费别、门诊或住院	通过分析科室的各种指标。找出科室的投入产出规律，从而克服投资的盲目性	
	费用支出情况	时间、科室、费别、门诊或住院		
	成本效益的投入产出	时间、科室		
	科室内部成本运行规律	时间、科室		
材料收支分析	材料申领情况分析	时间、科室、材料分类、库房名称、收发类别	分析各个科室的材料申请、消息消耗情况，了解材料耗费去向，节省开支，减少浪费，从而实现医院服务经营的最优运转	
	材料消耗情况分析			
	科室材料成本分析	时间、科室、材料分类		
运营综合分析	本利量分析	时间、科室、会计科目	利用本利量数学模型代替主观预测，科学化地预测科室的保本工作和保本收入，为运营管理决策提供数据支持	

表 6-8 医保分析主题分析

主题	子主题	主要分析维度	作用	数据来源
全院专题	在院医保综合监控	医保类型、医保代码、时间、在院状态	对医院医保各项指标进行实时监控，及时掌握医院医保情况，做出正确的决策	HIS 系统、医保 医院端
	全院医保费用概览	时间、费用类别		
科室专题分析	医保费用-科室概览	时间、科室、费用类别	按照科室分析，在确保医疗质量的基础上控制医保患者的费用	
	医保金额-科室（趋势）	时间、科室、住院状态、转科状态、医保类型、医保代码		
	医保金额-科室（构成）			
	医保金额-科室（八二）			
	医保金额区域占比分析	时间、科室、住院状态、转科状态、医保类型、患者来源		
医生专题分析	科室超标-医生排名	时间、科室、医生、医保类型、医保代码	对医生的工作量进行排名、趋势分析、构成分析八二法则分析、同比和环比分析，用以对医生绩效考核	
	医保金额-医生（趋势）	时间、科室、医生、住院状态、转科状态、医保类型、医保代码		
	医保金额-医生（构成）			
诊断专题分析	医保金额-诊断（趋势）	诊断名称、时间、科室、住院状态、转科状态、医保类型、医保代码	对诊断进行趋势分析、构成分析、八二法则分析、同比及环比分析，可以提高医疗质量	
	医保金额-诊断（构成）			
	医保金额-诊断（八二）			
患者专题	医保金额-患者	时间、科室、年龄段、住院状态、转科状态、医保类型、医保代码	根据患者的年龄段、性别就诊科室分析出医保主要受惠人群	
	医保金额-类型占比分析	时间、科室、年龄段、住院状态、转科状态、医保类型、医保代码		
	医保费用科室-性别分析	时间、科室、性别、住院状态、医保代码		
	医保费用患者性别分析	时间、科室、医保类型、医保代码、年龄段、性别、人群分类		

主题	子主题	主要分析维度	作用	数据来源
PCI 支架专题	出院PCI支架金额分析（趋势）	诊断名称、时间、科室、住院状态、转科状态、医保类型、医保代码		
	出院PCI支架金额分析（同比）			
	出院PCI支架金额分析（患者）			

表 6-9 绩效考核主题分析

主题	子主题	主要分析维度	作用	数据来源
财务收益	业务收入（占比，同比，环比，趋势）	时间、科室、医生	分析医院盈利能力，评估医院运营风险，全面系统地掌握医院经济运行状况，优化配置现有资源	HIS 系统，财务系统，病案系统，人力资源系统，物资系统等
	业务支出（占比，同比，环比，趋势）			
	业务收益（占比，同比，环比，趋势）			
	综合分析（资产负债，本利量，杜邦分析）			
客户市场	患者满意度、投诉次数、病员增长率等	时间、科室、医生	促进建立良好的医患关系	
内部流程	服务效率（门诊人次、病床使用率、平均住院天数等）	时间、科室、医生	改善提升服务效率和质量，提升医院核心竞争力	
	服务质量(诊断符合率、治愈好转率、感染率等)	时间、科室、医生、病种		
学习成长	发展能力（科研考评，教育培训考评等）	时间、科室、医生	激励促进医疗工作者提高业务技能，进而提升医院科研发展水平	

表 6-10 综合运营主题分析

主题	子主题	指标	说明	数据来源
财务收益	经济效益	科室收益率	考核科室收益与成本之比，一方面反映科室的盈利水平	HIS 系统，财务系统，病案系统，人力资源系统，物资系统，问卷调查等
		人均收益	科室人均收益	
		床位收益	反映每床位的收益	
		技术性服务收入增长率	反映技术服务收入增长情况	
		医疗设备投入增长率	反映设备资金投入情况	
	患者负担	门诊人均诊疗费	反映人均门诊费用负担	
		住院人均诊疗费	反映人均住院费用负担	
		药品成本占总成本比例	反映药费比	
客户市场	患者满意度	患者满意率	通过问卷调查得出	
		门诊患者增长率		
		住院患者增长率		
	缺陷管理	患者投诉率		
		医疗赔偿率		
学习成长	科研发展	新技术应用	考核新技术应用情况	
		研究成果产出	考核发表论文、论著、课题等研究成果情况	
	员工成长	职工满意率		
		年人均培训小时数	反映职工接受培训情况	
		中高级职称晋升比率	晋升中高级职称人员占专业人员比率	

表 6-11 人力资源主题分析

主题	子主题	指标		说明	数据来源
医师评价KPI	医师基本素质	专业知识、专业技能、专家等级、学术任职、职务、资质、工作年限、年龄、职称、学历		将医师评价KPI分七个主题筛选出102个指标，并根据不同维度进行组织，包括时间维、专业维、岗位维、职称维、疾病维、病员维、诊治维等。不同的维度组合构成不同的约束条件，从而实现不同角度的分析，对医师绩效执行情况进行监控和分析，为医师未来的发展提供建议。	HIS系统，财务系统，病案系统，人力资源系统，物资系统等
	履职情况	上级部门评价、患者评价、同行评价、科室评价、带教情况、工作态度、出勤、任职目标、职责			
	临床业绩	管理指标	医院感染漏报率、病案书写质量、传染病报告率、医疗纠纷、规章制度执行率、医疗责任事故、医疗技术事故		
		医疗质量	门诊诊断与出院诊断符合率、临床诊断与病理诊断符合率、术前诊断与术后诊断符合率、同一疾病七日内再住院例数、Ⅰ类切口甲级愈合率、Ⅰ类切口感染率、抢救成功率、放射诊断与术后诊断符合率、三日确诊率、院内感染、并发症		
		工作效率	平均住院日、术前平均住院日、日均占床数、床位使用率、床位周转次数		
		疗效	治愈人数、治愈好转率、好转人数、病死率、无效人数、死亡人数		
		工作量	门诊量、急诊量、院外会诊次数、收治量、手术量、院内会诊次数、医疗工作时间		
		危重病人	抢救次数、一级护理人数、ICU/CUU人次、特护人数、疑难病人量、危重病人量		
	科研能力	研究生培养、实习生培养、新技术开展、论文发表、科研奖励、教材编写、科研成果、专利、出版专著、科研经费、课题数量			
	学习成长	授课时教、学术讲座、进度报告、继续教育、学术活动、国内进修、出国进修			
	卫生经济	总收入、百元成本费、总利润、门诊人均费用、住院人均费用、床均收益、日均效益、检查费、药品费、手术费、检查费、其他费用、治疗费			
	医德医风	合理检查、合理用药、收受红包、收受回扣、科室满意度、患者满意度、尊重患者、文明礼貌、仪表仪态			

6.1.4.2.2 展现方式

1）多维分析

联机分析处理（Online Analytical Processing，OLAP）分析是商业智能系统的主要数据展现和分析手段，用户通过浏览器与 OLAP 服务器联结，可以快速、一致、交互地访问各种可能的信息视图，洞察数据深处，掌握隐于其中的规律。OLAP 分析可以帮助医院中的决策人员、业务分析人员、数据分析人员完成各种 OLAP 需求，如：在不同层次之间计算和建模；从不同角度切割数据集合进行分析；从宏观到微观，对数据进行深入分析；从微观到宏观，对数据进行汇总分析；查询底层细节数据；对不同数据集合进行基于多个角度的比较。

2）固定报表

固定报表主要面向决策和管理人员，通过固定报表可以快速了解医院当前的运营情况，并可及时地捕捉异常信息，是决策支持系统中基本的也是重要的表现形式。

3）灵活查询

灵活查询提供简单易用的数据查询环境，方便、准确、完整地向各层面人员提供多层次的综合性信息。

4）综合分析仪表盘（Dashboard）

为便于医院管理层更加直观的通过系统进行分析，选定多个主题进行综合展示，就是通常所指的仪表盘（Dashboard），Dashboard 的基本构成是由一个核心的结果指标图和一系列影响该结果指标的图表构成。能够帮助管理层人员关注医院核心业务指标，同时能够对于影响该业务指标的因素进行综合分析。为了保证直观性和全局性,Dashboard 展现形式都采用可组合的小型块状分析图表构成。一般相关图表统一采用相同的时间跨度，不需要输入查询条件。

当需要对某个图表进行详细分析时，系统提供链接方式使用户可以直接进入该图表的分析界面。

5）绩效看板

绩效看板是现代医院用于激发和促进员工提高工作绩效的常用管理手段。一种类型是将每个业务组织甚至个人的主要运营绩效、排名通过看板的形式公布

出来，促进员工之间互相学习、互相促进、良性竞争。绩效看板的采用能够加大数据仓库系统的应用广度。

6）指标预警

指标预警用于帮助管理人员在分析过程中，快速发现业务中存在的严重问题，以便及时采取改进措施，避免问题的扩展，和造成更大危害。可以很灵活的由客户设定预警阀值，不需要独立开发预警报表。

7)导航框架

支持树型结构的图表导航，可用外部框架与前端展现工具进行集成，集成后的框架与工具的用户之间需进行映射，支持单点登录，域用户登录等，且能完整的应用前端展现工具中配置的权限，或者基于前端展现工具进行开发，为用户提供友好的导航界面。

8)地图定制

支持地图的定制，并可实现地图间、地图图块与相关图表的链接联动，地图中相关指标的预警等功能。

9)门户

商业智能系统应该提供门户整合的功能，能够与主流的门户系统进行内容的整合，包括单点登陆、权限控制、内容集成。

6.1.4.3 系统支撑环境

对于医院管理辅助决策支持系统的软硬件系统配置需求，本方案根据医院的规模，提出了中低端、高端两种配置方案（可以根据实际情况进行配置方案的组合，但需要明确方案的适用范围和条件）。在医院信息系统建设中，应根据医院的规模、效益等实际条件，本着经济、实用、高效的原则，选择合适的配置方案。

表 6-12 两种配置方案的定义及适用条件

方案名称	规模及技术规格	适用条件
中低端方案	■ 中小规模 ■ 提供报表、图表等多种统计、分析功能 ■ 采用 B/S 架构	■ 二级及以下医院 ■ 业务量不大 ■ 系统建设投入适当
高端方案	■ 大规模 ■ 提供报表、图表、数据挖掘等多种统计、分析、挖掘功能 ■ 采用 B/S 架构	■ 三级医院 ■ 业务量很大 ■ 系统建设投入较大

6.1.4.3.1 硬件架构

6.1.4.3.1.1 硬件架构概述

医院管理辅助决策支持系统硬件架构由以下组件构成：

硬件服务器：从功能上划分可以分为数据库服务器、应用服务器、Web 服务器、备份服务器等。在满足实际业务、计算能力、可靠性和系统安全等需求的前提下，一台物理服务器可以同时运行多个不同服务器功能。例如，应用服务器和 Web 服务器可能运行在同一物理服务器。服务器应采取开放式的架构，具有较好的可伸缩性、可靠性和经济性，经过广泛用户群验证，人员培训成本较低。

存储设备：磁盘阵列、磁带库等。

终端设备：台式机、笔记本、手持终端以及其他专用终端设备等。

网络设备：包括交换机、路由器、防火墙、VPN 以及无线网络设备等。

6.1.4.3.1.2 典型配置方案

1) 网络拓扑图

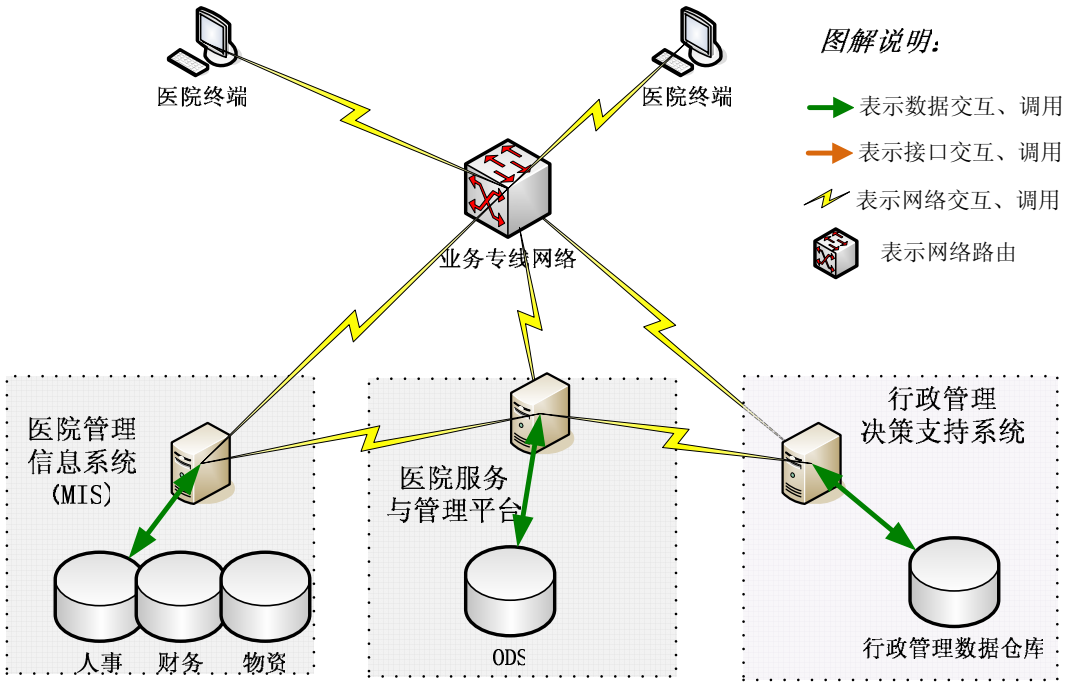


图 6-5 医院管理辅助决策支持系统网络拓扑图

2) 系统组件及构成

下表中分别列出了建设医院管理辅助决策支持系统的组件需求，在系统建设过程中，根据医院的规模、经济能力等实际情况，选择最佳的配置方案。

表 6-13 医院管理辅助决策支持系统硬件配置方案

ID	系统组件	配置及性能要求		数量	说明
		中低端配置	高端配置		
1	硬件服务器	■ 类型:X86 服务器(或同级服务器) ■ 处理器：2C（4 核） ■ 内存：8G ■ 存储：320G 以上	■ 类型：多路 X86 服务器（或同级服务器） ■ 处理器：4 路（8 核） ■ 内存： 8G ■ 存储：320G 以上	2	应用服务器和数据库服务器各一台
2	磁盘阵列	无	■ 容量： ■ 支持分区、快照、克		根据实际业务量估计存

	系统		隆等基本功能 ■ 支持在线扩容，无须停机		储容量
3	交换机、路由器	企业级路由式核心交换机	企业级路由式核心交换机		视实际网络情况而定
4	终端	■ 类型：PC ■ 内存：1GB ■ 硬盘：160GB	■ 类型：PC ■ 内存：1GB ■ 硬盘：160GB		
5	防火墙	企业级硬件防火墙	企业级硬件防火墙		

6.1.4.3.2 软件架构

6.1.4.3.2.1 软件系统架构

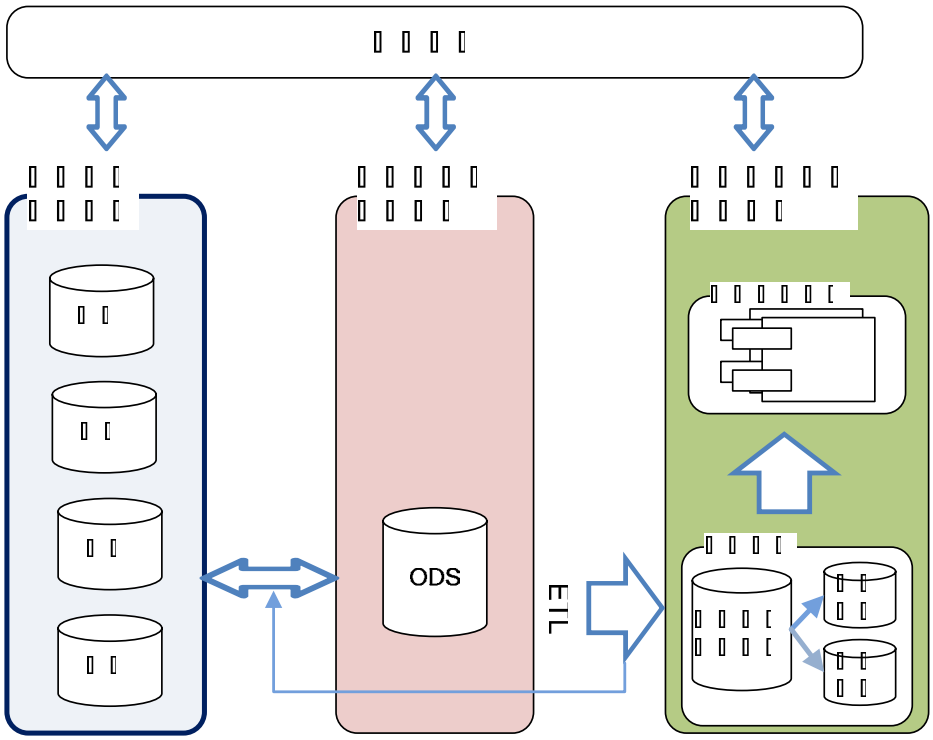


图 6-6 医院管理辅助决策支持系统软件架构图

6.1.4.3.2.2 软件系统配置

医院管理辅助决策支持系统，主要对医院的人事、财务、物资等方面的管理进行决策支持。除数据库和应用中间件以外，医院管理辅助决策支持系统可能还将采用 BI(Business Intelligence)软件，而 BI 软件的价格较为昂贵。因此，在做选型的时候需要充分考虑业务需求及实际情况，做到经济、实用。

6.1.4.4 案例分析

1）分析目的

直觉告诉医院决策者，降低全院平均住院日可以增加收治病人数，提高收益率。但业务科室的工作量增加，来自内部员工的反对声不绝于耳。管理层如何统一全院的思想认识成为迫切的问题，通过来自医院信息平台的数据，以及基于数据的预测分析，破解了这一难题。

2）决策过程

✧ 分析数据准备：

医院信息平台中的数据抽取、挖掘组件每天将医院日常费用信息、诊疗信息、设备使用信息等提取到主题数据仓库，可在需要分析的时候直接使用，不干扰业务系统正常运行。

✧ 决策分析：

医院管理决策系统通过对主题数据仓库的数据进行多维分析，最终以报表、仪表盘等形式将结果展现给决策者。分析过程如下：

首先，对病人入院后每日的诊疗活动和发生费用进行统计，通过住院工作分析、住院收入分析、诊疗活动费用趋势图比较发现，住院过程存在明显的“二八法则”，即在住院较前的 20%的时间里完成 80%的诊疗活动，较后 80%的时间里完成了 20%的诊疗活动；

其次，对内科系统和外科系统各专业进行具体的分析，通过住院时间、手术时间分析发现需做手术的外科专业受制约的因素主要是术前时间过长。内科专业受制约的主要因素依次是检查检验等待时间、停药/出院指征的掌握和转科等待时间，并对各科的平均住院日进行合理、可行的预测；

第三，对大型诊断检查（CT、MR、彩超 等）的申请日期和检查日期进行统计分析，找出影响术前时间过长的原因，并采取推行临床路径管理、引导临床科

室向康复科室转送康复期病人、技术诊断科室弹性上班、延长检查检验工作时间等一系列管理措施。

3）分析结果

通过以上分析，可以得出结论，病人住院费用大部分产生于入院前期，如能有效降低病人检查检验、手术的等待时间，缩短后续治疗、观察的时间，最终降低病人平均住院日，提高床位周转率，将能显著提高医院整体收入水平。

在决策过程中，统一认识是关键，没有详尽的数据是很难有说服力的，由于有了管理决策系统，能够将直观、具体的分析结果展现在大家面前，最终使大家从内心支持这一决策，提高了决策执行力。

另外，决策分析的作用还体现在跟进措施方面，发现了制约降低平均住院日的原因，并加以解决。

6.1.5 临床辅助决策

临床辅助决策是一种典型的基于平台的应用，基于平台积累的大量的数据为临床业务提供辅助决策。临床辅助决策支持是指能够提供给临床工作者、患者以临床知识或统计信息，并选择适当的时机，智能地过滤并表示这些信息，以提供更好的健康干预过程、更佳的患者个体护理服务，最终实现更高的人群健康目标。

基于临床指南的临床辅助决策支持系统（Clinical Decision Support System, CDSS）能够有效的提高医疗质量和效率、减少医疗差错、降低医疗费用。临床辅助决策支持系统建立在数据仓库及知识管理平台的基础上，通过与临床路径、合理用药、专家知识库等系统结合，为临床诊疗提供标准化的诊疗过程且能对其实行持续检测和定期评价。

总的来说建设临床辅助决策支持系统的目标是：以临床诊疗指南为依据，海量的临床知识库为基础，围绕医疗质量、效率、效益、医疗安全提供数据挖掘与综合统计分析服务。

6.1.5.1 需求分析

6.1.5.1.1 临床辅助决策支持分析

临床辅助决策支持分析系统能为临床决策者提供多层次、多维度、多变量的数据挖掘服务。具体来说主要包括如下服务：

1）临床用药分析：通过及时跟踪并获取临床用药情况，然后对药品医嘱用药适宜性进行审核，判断用药与临床诊断的相符性；针对剂量、用法的审核；剂型与给药途径的审核；是否有重复给药现象，是否有潜在临床意义的药物相互作用和配伍禁忌。

2）治疗效果分析：通过分析知识库数据，比较不同治疗方案对相同疾病的治疗效果和经济效果，对期望成本、成本-效果和治愈成本进行决策树分析，从而为临床制定合理用药方案和新药的研究、上市、使用提供科学依据。

3）临床知识挖掘：能够从文本源中提取知识进行文本发掘并能够依据人与信息之间的关系描述知识形成知识地图。

4）临床预警提示：针对临床上容易出现不合理处置、用药的情况提供预警功能,当医生进行药疗开处方时若出现上述情况,系统则会给出警告并要求医生改正,或确因治疗需要则要求进一步确认。

5）临床路径管理过程与效果监测：根据临床路径系统实时获取路径中治疗效果情况、路径变异情况，对治疗过程和路径变异进行分析最后根据分析结果调整变异症状知识库、路径改造，同时提供变异预警、单病种疗效与超限价影响因素分析等功能。

以下为院内临床辅助决策分析用例图：

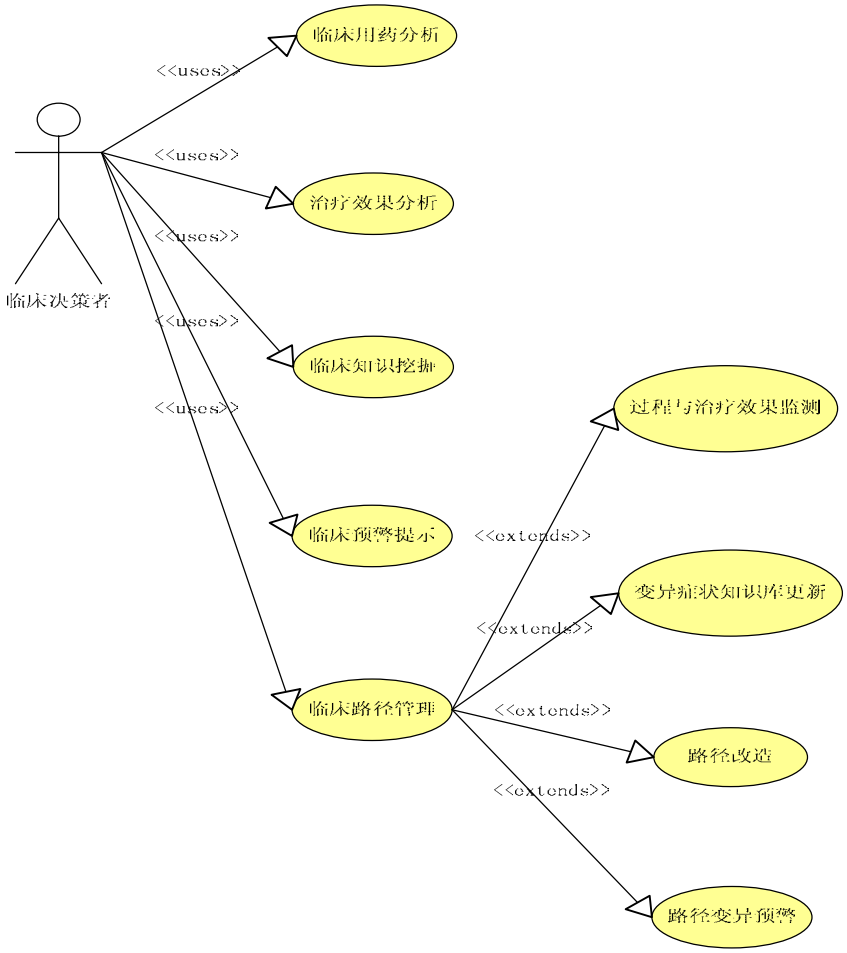


图 6-7 临床辅助决策支持分析用例图

6.1.5.1.2 基于临床辅助决策的应用系统

1） 合理用药系统

合理用药系统是以临床用药数据库为基础所构建的药物信息决策支持平台，主要作为临床辅助系统的一部分，为临床诊治及临床药学工作提供及时的信息支持。

- ✓ 合理用药系统可以对药物医嘱中可能存在的药物-药物相互作用、注射液体外配伍、重复用药、过敏药物、禁忌症、副作用、用法用量和特殊人群用药等潜在不合理用药问题进行及时性监测，将监测信息提示给医师或药师，使其更好地考虑用药方案、防范用药风险，达到合理用药的目的。 同时还需要提供审查模式的用户自定义功能。

- ✓ 支持药物相互作用审查、药物过敏史审查、注射剂配伍审查、老年人用药审查、儿童用药审查、妊娠期用药审查、哺乳期用药、禁忌症审查、不良反应审查、重复用药审查、药物剂量审查、给药途径审查、药物信息查询功能、药物临床信息参考、药品说明书、患者用药教育、中华人民共和国药典、检验值查询、医药学常用计算公式 、医药法规;
- ✓ 系统支持的查询：药物-药物相互作用、药物-食物相互作用、国内注射剂配伍 、国外注射剂配伍 、禁忌症 、副作用 、老年人用药、儿童用药、妊娠期用药、哺乳期用药等。

2） 临床路径系统

目前对临床路径（Clinical Pathways，CP）比较公认的定义是由医院各种背景的专家，根据某种疾病或某种手术方法，制定一种大家同意认可的治疗模式，让病人由住院到出院都依此模式来接受治疗，并依据治疗结果来分析评估及总结每个病人的差异，以避免下一个病人住院时发生同样的失误。医院通过此种方式可以控制医疗成本，提高医疗质量。临床路径以缩短平均住院日、合理支付医疗费用为特征，按照病种设计最佳的医疗和护理方案并根据病情合理安排住院时间和费用。不仅可以规范诊疗过程，减少一些不必要、不合理的诊疗行为，而且还可以规范诊疗行为，并辅助为临床诊疗方案做决策。

- **临床路径系统用例图：**

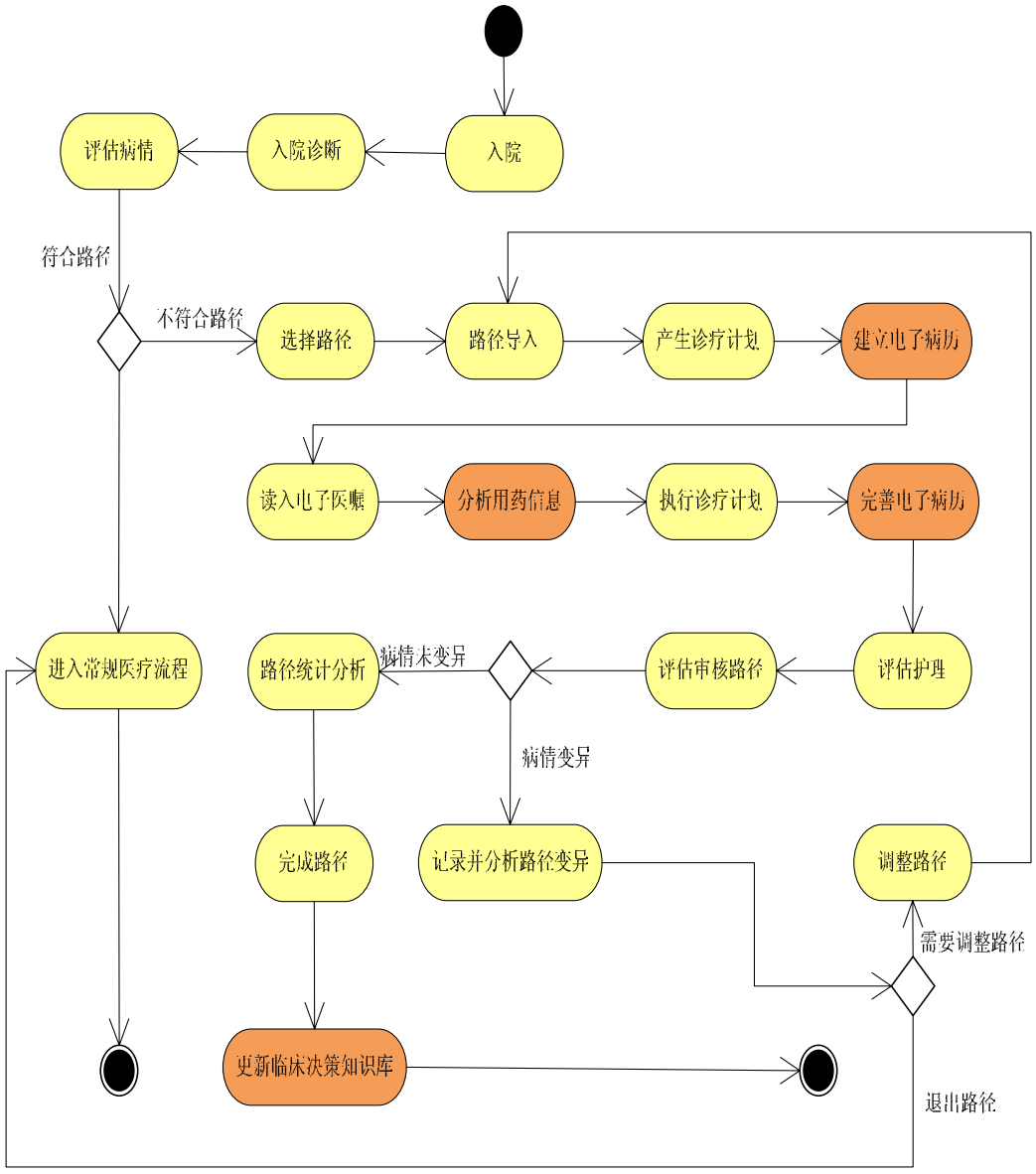


图 6-8 临床路径系统用例图

- **临床路径系统活动图**

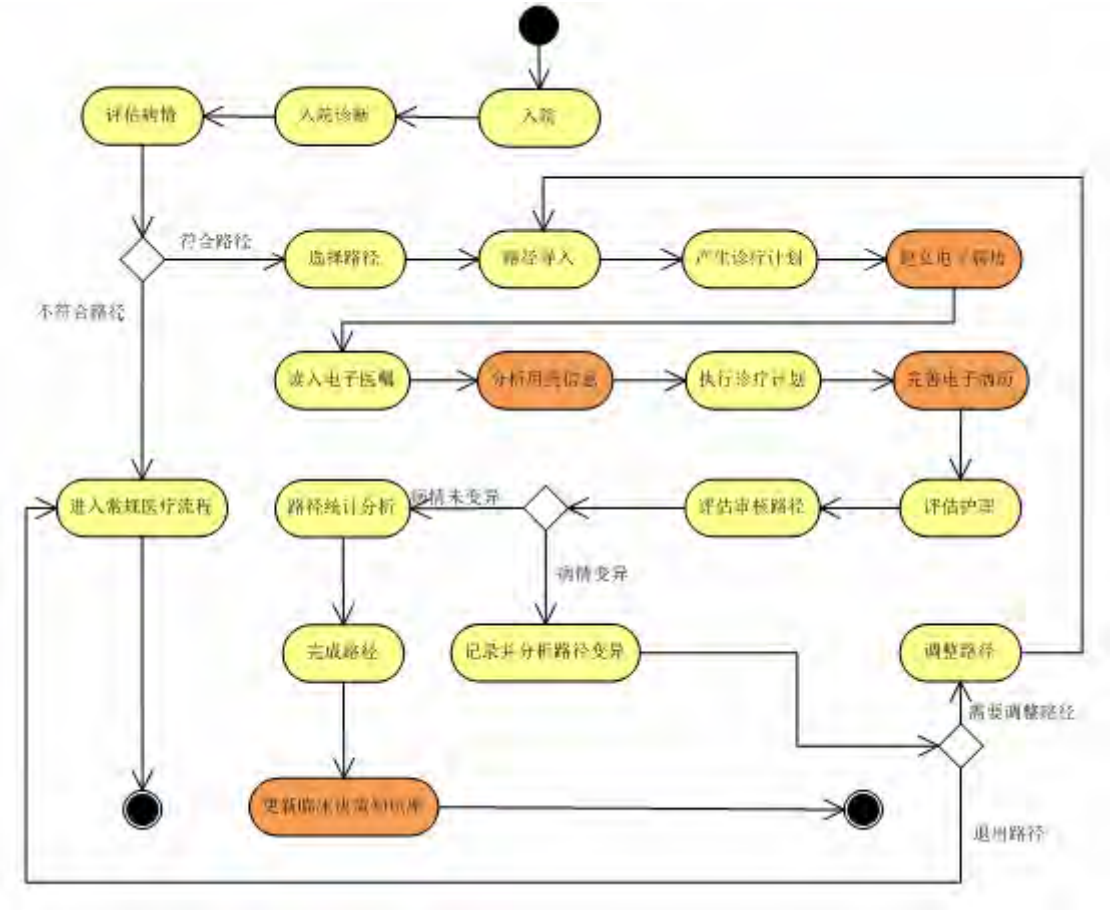


图 6-9 临床路径系统活动图

3） 基于知识管理的临床支持系统

医学信息在促进医学科技事业发展、帮助医学科研工作者发现新规律、提高临床医疗质量、加强卫生事业管理等方面发挥着重要的作用。伴随计算机技术、网络技术、生物医学信息学的飞速发展，各种类型的生物医学资源在新型信息环境下迅速增长，其内容繁多、分布广泛、动态变化，质量良莠不齐。面对医学信息资源来源的多样性、组织的动态性与无序性，需要对医学信息资源进行系统组织与分析，以方便临床实践人员、医学领域的研究人员合理高效地利用信息，为临床服务提供信息支撑。

构建临床医学知识库系统的目的在于为医务工作者提供更加个性化的知识产品，提供以知识节点为对象的知识服务，扩大医学图书馆知识服务的范围。通过临床知识库，帮助临床医生快速获取疾病治疗、疾病诊断、疾病检查中的各种知识。

基于知识管理的临床支持系统主要包括以下内容：

- **知识组织**

对知识客体进行收集、整理、分类、过滤、加工、提供。对知识单元本身进行描述和标引以及揭示知识节点之间的逻辑联系。建立疾病库、药品库、检查库和疾病诊治相关的知识库。

- **标准化**

医学知识库需要对疾病名称、药物名称、检查名称、疾病体系、药物体系、检查体系建立规范与标准。

- **临床预警及提示**

通过事件监视机制，主动地给医生提出决策建议，强制性阻止一些严重后果的发生，例如用药配伍禁忌和药物疾病禁忌等。

- **辅助诊疗**

通过将患者基本信息、症状，输入给知识库系统，知识库系统能够经过算法计算，推送出可能的结果。并给出病患可以进行的检查、给出相关药物治疗的初步方案。

6.1.5.2 主要功能

6.1.5.2.1 临床路径管理

- **路径执行**

A. 系统嵌入医师工作站，实现对住院患者的管理。
B. 系统可以自动或人工对患者是否进入路径进行判断。
C. 对每种进入路径的病种定义步骤与临床套嘱，包括药物、检查、化验、治疗以及护理等医嘱。
D. 医护人员可以按照每个步骤规定的套嘱开立医嘱，为患者治疗。
E. 支持对出院患者进行差异化分析。
F. 支持诊疗程序的规范化和变异分析，调节路径的某些环节的治疗方案。
G. 支持患者版路径，帮助患者及家属了解医护详细过程与时间安排。支持打印功能。

- **路径配置**

根据各种疾病进行临床路径的选择与设置。

- **相关数据统计**

费用及住院天数统计、评估情况统计、完成率统计、路径变异统计、单病种质量管理与控制以及国家规定的相关指标统计。

6.1.5.2.2 合理用药系统

- **药品相互作用审查**

提示两种药物给一个患者时可能出现的药理学效应，这些相互作用可能导致毒性增强、药效降低等，使药物的实际使用效果发生改变，或导致不良反应。

- **药物过敏预警**

主要对药品的禁忌症、副作用、老年人用药、儿童用药、妊娠期、特殊药物剂量的审查和预警。

- **合理用药监控**

提供药师在药品调配时对患者处方或医嘱进行合理用药自动和人工审查功能，将发现的问题进行记录并反馈给责任医师的功能。

- **用药研究**

用药研究模块是提供给医生研究药品资料的入口，在该模块中医生可以查询和组合审查药品知识库中全部几万种药品，也可将当前下达的用药医嘱导入用药研究中与另外的药品组合测试，在用药研究平台中所有信息都不会被保存，也不会影响医生工作站正常的医嘱。

6.1.5.2.3 基于知识库的临床支持系统

- **疾病数据库**

提供各类专科系统疾病信息，包括：疾病名、英文名、缩写、别名、ICD 疾病代码、概述、流行病学、病因、发病机制、临床表现、并发症、实验室检查、其他辅助检查、诊断、鉴别诊断、治疗、预防、预后及循证医学证据等项目。

- **药品数据库**

提供药品信息，包括药名、英文名、别名、剂型、药理作用、药动学、适应证、禁忌证、注意事项、不良反应、用法用量、药物相互作用、专家点评等项目。

- **辅助检查数据库**

提供各类检查项目信息，每一种检查项目涉及名称、缩写、正常值、临床意义等内容。

- **循证医学数据库**

主要包括：临床实践指南、系统评价和临床科学研究，其中临床科学研究包括：随机对照试验、对照临床试验、非随机对照临床试验、病例对照研究、队列研究、病例报告、病例分析及横断面研究等研究证据。以统一的数据规范存储成全文数据库。

- **医学资料参照库**

提供具有代表性权威临床研究论文、医学期刊和临床医学学会的全文文献。提供各科权威临床医学教科书全文。针对特定主题做导览式查询，并提供相关图书、期刊文献、药物信息、临床指引、卫教信息等参考列表。

- **临床辅助诊断**

主要提供辅助诊断治疗，根据病人的症状，通过分析决策引擎，推断出患者的疾病，并提供合适的治疗方案，供医生参考。在医生确诊并开出处方或处置以后，对疾病、处方以及处置进行分析，与知识库中的规则进行比对，确认处方、处置的安全可靠性，如果有异常，则发出警报，对医生提醒，从而提升医疗服务质量，减少或避免医疗事故的发生。

6.1.5.3 系统支撑环境

对于临床辅助决策支持系统的软硬件系统配置需求，本方案根据医院的规模，提出了中低端、高端两种配置方案（可以根据实际情况进行配置方案的组合，但需要明确方案的适用范围和条件）。在医院信息系统建设中，应根据医院的规模、效益等实际条件，本着经济、实用、高效的原则，选择适当的配置方案。

表 6-14 两种配置方案的定义及适用条件

方案名称	规模及技术规格	适用条件
中低端方案	■ 中小规模 ■ 提供报表、图表等多种统计、分析功能 ■ 采用 B/S 架构	■ 二级及以下医院 ■ 业务量不大 ■ 系统建设投入适当
高端方案	■ 大规模 ■ 提供报表、图表、数据挖掘等多种统计、分析、挖掘功能 ■ 采用 B/S 架构	■ 三级医院 ■ 业务量很大 ■ 系统建设投入较大

6.1.5.3.1 硬件架构

6.1.5.3.1.1 硬件架构概述

临床辅助决策支持系统硬件架构由以下组件构成：

硬件服务器：从功能上划分可以分为数据库服务器、应用服务器、Web 服务器、备份服务器等。在满足当地实际业务、计算能力、可靠性和系统安全等需求的前提下，一台物理服务器可以同时运行多个不同服务器功能。例如，应用服务器和 Web 服务器可能运行在同一物理服务器。服务器应采取开放式的架构，具有较好的可伸缩性、可靠性和经济性，经过广泛用户群验证，人员培训成本较低。

存储设备：磁盘阵列、磁带库等。

终端设备：台式机、笔记本、手持终端以及其他专用终端设备等。

网络设备：包括交换机、路由器、防火墙、VPN 以及无线网络设备等。

6.1.5.3.1.2 典型配置方案

1) 网络拓扑图

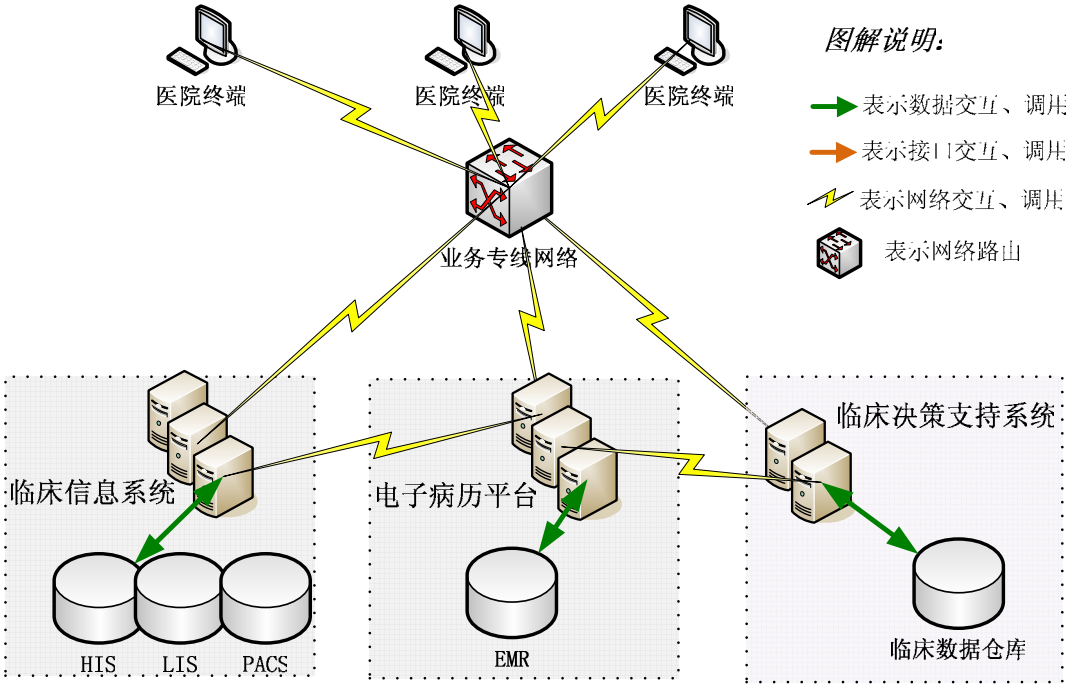


图 6-10 临床辅助决策支持系统网络拓扑图

临床辅助决策支持系统采用 B/S 架构部署，通过医院信息平台，将电子病历信息抽取到临床数据仓库中，建立决策分析主题，使用 BI 工具对这些主题进行展现。用户通过医院终端，可以访问临床辅助决策支持系统。

2) 系统组件及构成

下表中分别列出了建设临床辅助决策支持系统的组件需求，在系统建设过程中，根据医院的规模、经济能力等实际情况，选择最佳的配置方案。

表 6-15 临床辅助决策支持系统硬件配置方案

ID	系统组件	配置及性能要求		数量	说明
		中低端配置	高端配置		
1	硬件服务器	■ 类型：X86服务器（或同级服务器） ■ 处理器：2C（4核） ■ 内存：8G ■ 存储：320G以上	■ 类型：多路 X86 服务器（或同级服务器） ■ 处理器：4路（8核） ■ 内存： 8G ■ 存储：320G以上	2	应用服务器和数据库服务器各一台
2	磁盘阵列系统	无	■ 容量：		根据实际业

			■ 持分区、快照、克隆等基本功能 支持在线扩容，无须停机		务量估计存储容量
3	交换机、路由器	企业级路由式核心交换机	企业级路由式核心交换机		视实际网络情况而定
4	终端	■ 类型：PC ■ 内存：1GB ■ 硬盘：160GB	■ 类型：PC ■ 内存：1GB ■ 硬盘：160GB		
5	防火墙	企业级硬件防火墙	企业级硬件防火墙		

6.1.5.3.2 软件架构

6.1.5.3.2.1 软件系统架构

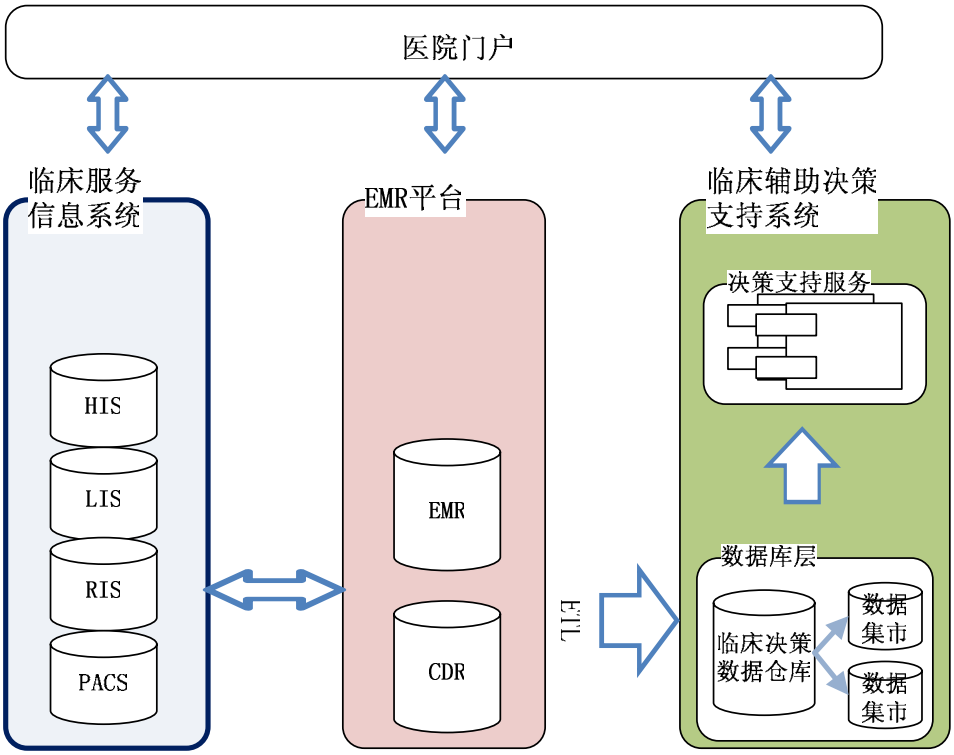


图 6-11 临床辅助决策支持系统软件架构图

6.1.5.3.2.2 软件系统配置

临床辅助决策支持系统，是一个准实时系统，涉及到大量病历信息，因此在选择软件时应充分考虑系统的高效、灵活、安全等多方面的性能。

由于临床辅助决策支持系统使用到 BI 软件，投入会比较大，在做选型的时候需要充分考虑业务需求及实际情况，做到经济、实用。

6.1.5.4 案例分析

1）分析目的

利用临床辅助决策支持系统对亚思达阿奇霉素两种不同给药方案治疗小儿肺炎支原体肺炎的成本-效果进行分析比较，找出较优方案。

利用医院信息平台及临床辅助决策支持系统可在平时临床治疗过程中随时完成研究数据积累，缩短了临床研究的周期，并能将分析结果以友好、直观的界面形式展现给临床研究人员，提高了临床研究的效率。

2）决策过程

✧ 基础数据准备

决策分析的数据基础来源于临床活动，医院信息平台通过数据抽取、挖掘技术将用药数据、费用信息等提取到主题数据仓库为之后的决策提供支持。

✧ 病例筛选

选取临床症状、体征、胸片及肺炎支原体抗体检查确诊为支原体肺炎患儿为研究对象，排除对阿奇霉素药物过敏者和严重心、肝、肾及血液系统疾病患儿，总共 64 例入选（均为住院患者）。治疗前患者均未使用过其他抗生素。系统将其随机分为两组：A 组 32 例，男 20 例，女性 12 例，年龄 3 岁~10 岁；B 组 32 例，男性 18 例，女性 16 例，年龄 4 岁~11 岁。

✧ 用药方案筛选

A 组均为采用阿奇霉素注射液（商品名：亚思达，规格：0．25 g/2 ml，批号：051104，价格：23．50 元/支，0.01 g/（kg·d），静脉滴注，总疗程为 10 d 的案例；B 组为先采用阿奇霉素注射液 0.01 g/（kg·d），静脉滴注,7 d 病情好转后则改为出院带药治疗，口服阿奇霉素干混悬剂（商品名：希舒美，规格：0．1 g×6 袋/盒，批号：65864056，价格：48．60 元/盒）,剂量按说明书操作，口服 3 d 的案例。治疗期间均不同时使用其他抗生素，但给予常规治疗（如解痉、平喘、止咳、化痰等）。

✧ 决策分析

通过分析引擎，临床辅助决策系统在界面上以报表或仪表盘展现以下几组比

较结果：

临床疗效比较

两组治疗后，有效病例的干咳、发热、气喘等症状多在 3 d 内明显好转；给药前胸片有明显异常者分别为 25 例和 23 例，治疗后病灶消失者两组各为 23 例（92.0％）和 21 例（87.0％）；两组临床有效率分别为 90.6％和 87.5％，差异无显著性（P>0．05）。

治疗成本比较

成本是指所关注的某一特定方案或药物治疗所消耗的资源的价值，用货币单位表示。由于两组的检查成本相同，故治疗成本只计算所用药品费用和住院费用。

药品成本：患者所用药品的总费用。亚思达 0．25g，每瓶 23.50 元；希舒美 0.1g，每袋 8.10 元，将每日药品成本疗程计算每位患者的药品成本。A 组的平均药品成本为 2450.60 元，B 组平均药品成本为 1560.40 元。

住院成本：住院成本包括床位费、护理费、治疗费等，每日住院成本为 45+40=95.0 元，将每日住院成本按疗程计算每位患者的住院成本，最后根据公式：总成本=药品成本+住院成本，计算每位患者的治疗总成本。两组的总费用平均为：A 组=95×10+2450.60=3 400.60 元；B 组=95×7+1560.40=2225.4 元。

成本-效果分析

成本-效果分析是目前应用最广泛的药物经济学方法，目的在于平衡成本和效果，在二者之间寻找最佳结合点；成本-效果比则将二者有机地联系在一起，采用单位效果所需花费的成本来表示。

系统通过折线图、柱形图、报表形式显示两组方案的成本-效果分析结果，最终可直观发现两组间成本比较 A 组成本明显高于 B 组。

不良反应

两组案例中共出现不良反应 8 例，A 组恶心 2 例，胃肠道不适 3 例；B 组腹泻 1 例，胃肠道不适 2 例。两组间差异无显著性（P>0．05）。

3）分析结果

两组在有效率及不良反应发生率方面差异无显著性（P>0．05），但A组的治疗成本却明显高于B组（P<0．01），且成本-效果A组高于B组。结论：对小儿肺

炎支原体肺炎，采用序贯给药治疗不但安全、有效，而且更加经济、合理。

系统将最终研究结论保存至临床知识库，供医生在临床治疗中参考。

6.1.6 医院门户应用

门户以统一的方式来组织和展现不同来源的信息，为用户提供个性化和客户化的服务，将用户引导到感兴趣的信息上。

医疗门户可根据用户对象的不同划分为医务人员门户、医院管理人员门户和患者公众服务门户。医疗门户既是垂直门户、区域门户，也是团体门户和行业门户，对医疗管理人员门户而言，它又是政府门户。医疗门户兼具以上各类门户的特点。通过结合统一用户和权限管理系统，可以实现单点登陆所有应用系统；提供无门槛的用户自定义功能；增强的全文检索功能；通过统一的门户集成标准，快速集成其他应用系统；在一个界面框架中，自由切换和应用不同系统，以及可将多个应用系统的内容集成在一个模块中。

总而言之，医疗门户就是指在互联网环境下，把各种应用系统、数据资源和互联网资源统一集成到医疗门户之下，根据每种用户使用特点和角色的不同，形成不同的应用界面，并通过对事件和消息的处理传输把用户有机地联系在一起。它不仅仅局限于建立一个医疗网站，提供一些医疗服务信息，更重要的是要求能实现多业务系统的集成、能对用户的各种要求做出快速响应、并且能对整个医疗服务网点进行统一管理。

6.1.6.1 需求分析

医疗门户根据用户的不同而分为医务人员门户、医院管理人员门户和患者公众服务门户。三种门户都需提供医疗信息及医疗新闻的浏览功能，并且要同时满足三种用户根据自身权限在门户上完成一定的医疗行为的操作和信息交流。

根据现阶段医疗门户在国际上的发展趋势，并结合我国的实际情况，门户的需求包括三个层次，第一个层次为浏览的需求，包括浏览医疗信息，医疗主管部门网站及最新医疗管理的规章制度，并可以通过权限控制浏览自己相关的临床资料、诊疗信息和政府信息；第二个层次为满足用户在门户上录入和发布信息的需求，可将该信息发布至相关人员和组织部门；第三个层次为支持用户在门户和网

页上开展医疗实践的功能，包括患者门诊预约、医院管理人员使用决策支持系统等功能。

从技术角度看，注册服务、权限控制、安全性和系统跟踪是三类门户所必需的，在基于医院信息平台的建设模式下，这些内容大多可基于平台来实现（参见第 5 章）。

本章重点介绍医务人员门户和医院管理人员门户。患者公众服务门户见下一节患者公众服务。

6.1.6.1.1 医务人员门户

根据不同医务人员的权限、需求和兴趣，提供简单、迅速、客户化配置的医疗信息的浏览方式，从而将大量不同来源的医疗信息以一种有效的方式提供给不同使用者，包括医务人员所需的所有医疗信息和相关 web 站点的链接；以及更进一步地提供医疗实践的支持，如处方录入、远程会诊、远程教学及科研等，从而实现跨不同医疗系统，为提供统一、便捷、有效的医疗服务而建立起来的医务人员门户，其目标是通过提供医疗信息综合浏览操作平台而达到对病人的高效、快捷、准确的医疗服务，从而最终提高医疗服务的质量。

医务人员门户需提供同用户专业相关的学术信息、规章制度，所负责患者的诊疗信息，以及院内行政工作相关的业务和办公信息。

6.1.6.1.2 管理人员门户

根据医院管理者的需求、提供简单、迅速、客户化配置的信息浏览方式，包括各科室接诊情况、各类疾病费用统计信息等。从而将大量不同来源的医疗信息以一种有效的方式提供给院内卫生管理者。疾病分布、病人统计、费用分析、医保、突发事件、员工绩效的管理，以及所有信息的统计和分析功能。

医院管理者门户主要是能够和院内相关的系统以及区域卫生管理网站连接，如 HIS、医院决策支持系统、医院 OA 系统、CDC、上级管理机构网站等；并能够和其他机构组织的系统相连，如所在区市省三级的卫生管理门户、社会保障部门相连，从而有效的管理院内各种卫生活动并与区域内各个医疗机构形成紧密的卫生业务联动。医院管理者门户的主要需求是能达到浏览相关信息，及时从所属的

各个医疗、管理系统收集数据，发布数据至相关的行政管理部门，并具有数据统计和分析功能。

6.1.6.2 主要功能

门户集成的信息根据不同用户的需求，可以包含各种应用的信息和入口，本章节列出部分常用功能以供参考,其中部分功能直接在门户上完成，部分功能只是提供入口，用户基于单点登录、统一权限管理进入相关功能界面。管理人员同时又是医疗服务人员时，其定制的门户将包含两类门户的功能，方便用户使用。

6.1.6.1.1 医务人员门户

- 电子病历浏览

为医务人员提供患者历次就诊产生的电子病历的浏览功能，同时支持根据权限访问以保护患者隐私。

- 医疗咨询

为医务人员进行医疗咨询提供支持，在为患者服务时医生随时可根据需要方便快捷地浏览患者的电子病历，更好地服务于患者。

- 会诊管理

提供院内外会诊申请、申请审核、接受申请、参加会诊等功能。

- 远程医疗

提供远程医疗申请、申请审核、接受申请、进入远程医疗等功能。

- 转诊/转检

提供院间转诊/转检申请、申请审核、接受申请、结果反馈等功能。

- 协同办公（OA）

满足日常办公需要，包括办公文件的发布与接收、分配与接受工作安排、浏览待办事项、工作提醒等内容。

- 论坛与博客

为医务人员提供论坛与博客服务，方便内部人员的知识与信息的发布、分享与讨论，有需要时还可对外开放给公众通过互联网访问，增进医患互动，拉近医患距离，消除医患隔膜。

- 科研教学支持

为医务人员提供病历研究、知识管理、知识库查询等服务，为临床服务与科研教学等工作提供丰富的信息来源。

- 其他信息浏览

包括医学信息，如最新临床科研进展、相关专业网站链接等；政府信息，如有关医疗法律法规、最新公告和通知、相关机构组织网站链接等。

6.1.6.1.2 管理人员门户

- 协同办公（OA）

满足日常办公需要，包括办公文件的发布与接收、分配与接受工作安排、浏览待办事项、工作提醒等内容。

- 人员管理

提供根据管理权限对所管理工作人员的基本信息查询与管理、排班与考勤信息查询、下属工作计划及进度查询等。

- 医疗服务质量监控

提供医疗服务质量监控信息查询，便于管理人员掌握医疗服务质量状况，及时制定和采取适当的干预措施，提高医院整体医疗服务质量。

- 管理信息统计分析

提供预定义的、定制的各种医院管理信息的统计分析结果，包括临床、运营等各方面的管理信息，为管理人员作出管理决策提供支持。

- 其他信息浏览

包括医学信息，如最新临床科研进展、相关专业网站链接等；政府信息，如有关医疗法律法规、最新公告和通知、相关机构组织网站链接等。

6.1.6.3 系统支撑环境

6.1.6.3.1 硬件架构

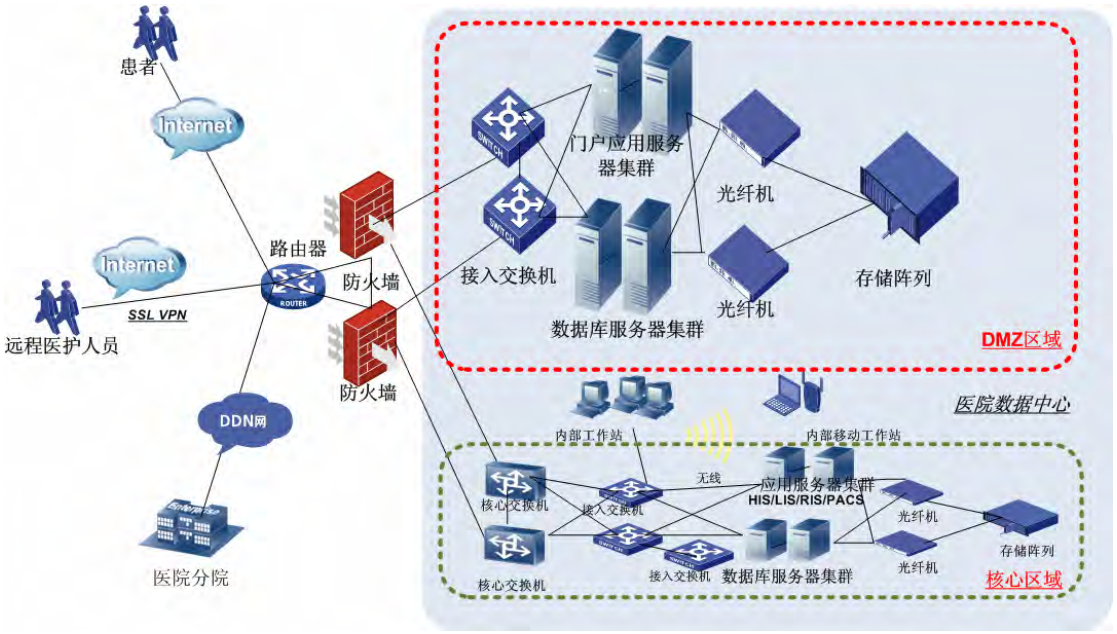


图 6-12 医院门户典型系统支撑环境

医院门户提供对外服务，所以需要单独部署在由防火墙控制的非军事化区内，与医院内部业务进行隔离，患者可通过互联网进行一般信息的浏览，对于内部和远程医务人员则建议采用专线或 VPN 的方式进行信息浏览。

表 6-16 地级市二甲医院配置方案

主要设备	资源类别	关键配置规格说明	数量	用途/关系
X86 服务器（或同级服务器）	应用服务器	CPU：四核 硬盘：146G*2 内存：16G 网卡:1000M*2 4GB FC 主机通道卡*2	2	安装门户产品服务端 并作应用服务器集群
	数据库服务器	CPU： 四核 硬盘：146G*2 内存：16G 网卡:1000M*2 4GB FC 主机通道卡*2	2	安装数据库软件，做数据库集群
数据存储设备	SAN 磁盘阵列	采用两个以上控制器/电源/冗余传输线等保证不出现单	2	安全存储容量=（业务数据存储需求× 1.5[存储开销]）×

		点故障，并采用阵列内复制、快照等技术进行数据保护； IOPS>8000； 缓存>4GB,并可扩展； 使用 15K 高速 SAS 硬盘，并可使用多个磁盘柜进行扩展容量到百 TB 以上； 支持 RAID 0/1/10/5		（ 1 + 0.5[索引开销] ） × 1.2[相关数据管理冗余]
网络设备	网络交换机	交换机：千兆或百兆端口； 在任意时间与应用服务器 ping 包响应时间在 50ms（最低 100ms）以内；在正常使用时间 ping 应用服务器丢包率<1%（最低 3%）每客户端的带宽>40KBits	2	两台避免交换机单点故障
	防火墙	一般网络入侵防护功能，支持 IPSEC/SSL VPN	2	划分 DMZ 安全区域 网络安全防护和支持 VPN 联网 两台避免单点故障

表 6-17 地级市三甲医院配置方案

主要设备	资源类别	关键配置规格说明	数量	用途/关系
X86 服务器（或同级服务器）	应用服务器	CPU：四核 硬盘：146G*2 内存：32G 网卡:1000M*2 4GB FC 主机通道卡*4	4	安装门户产品服务端 并作应用服务器集群
	数据库服务器	CPU：四核 硬盘：146G*2 内存：32G 网卡:1000M*2 4GB FC 主机通道卡*2	4	安装数据库软件，做数据库集群
数据存储设备	SAN 磁盘阵列	采用两个以上控制器/电源/冗余传输线等保证不出现单点故障，并采用阵列内复制、快照等技术进行数据保护； IOPS>8000； 缓存>4GB,并可扩展； 使用 15K 高速 SAS 硬盘，并可使用多个磁盘柜进行扩展容量到百 TB 以上； 支持 RAID 0/1/10/5	2	安全存储容量=（业务数据存储需求× 1.5[存储开销]）×（ 1+0.5[索引开销] ） ×1.2[相关数据管理冗余]

网络设备	网络交换机	交换机：千兆或百兆端口；在任意时间与应用服务器 ping 包响应时间在 50ms（最低 100ms）以内；在正常使用时间 ping 应用服务器丢包率<1%（最低 3%）每客户端的带宽>40KBits	2	两台避免交换机单点故障
	防火墙	一般网络入侵防护功能，支持 IPSEC/SSL VPN	2	划分 DMZ 安全区域 网络安全防护和支持 VPN 联网 两台避免单点故障

6.1.6.3.2 软件架构

图 6-13 门户软件架构

- 最上面的表示层，提供用户界面显示（Portlets）和 Web 服务。
- 服务转换层负责将门户服务提供平台和第三方系统的业务对象进行转配和转换，统一业务对象，为表现层提供统一的展现支持。
- 服务层则提供门户服务，提供平台的核心业务规则、流程处理和领域对象访问，并为服务转换层提供服务。
- 持久化层为服务层提供持久化对象管理，和统一数据访问（数据库、文档）入口。

6.1.6.4 案例分析

6.1.6.4.1 医务人员门户

医生打开网页，通过用户名和密码登陆，进入已配置好的该用户的界面，查看自己的病人的临床资料，查看检验检查结果，检查结果提示轮状病毒感染，给出诊断和治疗建议，查看政府最新的关于轮状病毒感染患儿的报告制度，完成报告，发布报告。

1） 浏览信息

- 浏览医学信息，包括医学和护理学相关专业内容，用户所在领域最新临床和科研进展。需提供相关专业网站的链接。
- 浏览政府信息，包括相关政府部门有关医疗的法律法规，和医务人员临床行为密切相关的最新公告和通知。提供相关机构组织的网页链接，如CDC，所属卫生局，社会保障局及卫生部等。
- 浏览病人信息，包括病人基本信息、过敏及副作用信息、用药、诊断以及有会诊申请的病人的会诊结果等。

2） 发布信息

- 接收挂号，会诊，并将处理结果发布给申请者。
- 非结构化的数据输入：如各种格式的文档、图片文件的导入。
- 直接的病人事件录入：包括诊断和治疗方案录入，支持医疗文件的书写，支持录入的医疗文件的发布。
- 支持进入其他医疗信息系统，RIS/PACS, LIS 等，支持发布影像学诊断信息。

3） 开展医疗实践

- 提供诊断支持功能，医学知识数据库和临床路径等。
- 应答患者咨询请求，开展网上开处方和提供诊疗建议。
- 接收患者的远程监护数据，如心电图、血糖、血压等。
- 同社区服务中心，医疗保险局及其他联网的医疗机构和个人进行业务合作，开展网上医疗费用支付等医疗活动。

6.1.6.4.2 管理人员门户

医院办公室主任输入用户名、密码登陆管理者门户。待办事项窗口提示用户有一个待办事项：季度绩效考核需要给所管辖医务人员进行评定。他首先打开医生工作量统计窗口，浏览各医生本季度的工作量统计分析，并仔细查看不合格人员的工作量明细，之后又通过费用统计界面查看药品费用比例，分析哪些医生在本季度内药品超过了合理比例。最后根据之前的数据，办公室主任为每个所属医务人员进行了恰当的工作评定。工作完成后主任又通过政策规范浏览界面学习了刚更新的卫生部医改精神，对以后的工作方向有了更明确的认识。

6.1.7 患者公众服务

随着医疗体制改革的深入，我国医疗服务逐渐由以医疗机构为中心、以医生为中心向以患者为中心过渡。而在此过程中医院信息化建设发挥了重要的作用。以前挂号时间长、检查时间长、取药时间长、看病时间短的“三长一短”现象长期令病人不满。但是，如今一大批现代化信息手段涌现出来，患者检查、取药、缴费花半天的状况已大为改观。

当前在院内外已经有一大批信息系统在为患者提供便捷的诊疗服务：网上预约挂号、医院呼叫中心（Call Center）解决了病人早起排队挂号之苦，足不出户就能在家预约指定的专科医生；候诊环节改为自动排队、电子叫号，病人再也不用因为焦急的等待而惴惴不安；处方电子化，每项药品以及收费都明明白白的列在一起，可随时通过病人咨询服务系统查询，医生开的处方再也不是“无价天书”；检验检查报告自助打印，检验报告丢失、个人隐私泄露的问题也得到了解决。还有诸如输液自动监控、短信通知缴费、短信空床通知，远程诊疗，网上、电话患者随访等一系列服务，让患者切实对医院看病难、服务差的印象起了改观，也提高了医院运营效率，增强了竞争能力。

6.1.7.1 需求分析

患者公众服务的最终目的是为了给患者提供方便、快捷的医疗服务，缩短患者在医院逗留时间，提高就诊效率，改善就诊心情。其主要需求按空间维度可分为院外需求和院内需求。

1） 院外服务需求

在医院外，患者希望尽可能多的了解与就诊相关的信息，不用去医院也能随时随地完成部分就诊环节，缩短花在医院看病的时间。其主要需求如下：

- 通过网站、电话、短信等手段获取医院的专家信息、接诊时间安排。过去由于信息传递手段的落后，很多患者有病乱投医，不知道去什么医院找什么专家，或者由于不知道专家接诊时间而反复去医院，耽误病人的宝贵时间。
- 就自己的病情进行远程咨询，远程诊疗。由于各地医疗资源分布不平均，很多患者需要到外地就医，由此产生了外出就诊的交通费、住宿费、家属陪护费等大量费用，路途的颠簸也使患者本已脆弱的病体雪上加霜。而许多没有条件或者无法到大医院就诊的患者则耽误了治疗。通过远程医疗，既能充分利用宝贵的专家资源、又降低医疗费用，免除患者长途辗转求医的辛苦，缓解看病难的问题。
- 远程预约挂号。通过远程预约挂号患者不再为挂号而面对交通、排队、熬夜等苦恼了。医疗机构也可避免门诊高峰挂号困难、等候时间长的问题，以方便患者就医，此外，医院通过预约门诊可以起到“削峰填谷”作用，使就诊人员趋于均衡分布，在一定程度上缓解门诊高峰期“人满为患”的现状。
- 远程获取检验检查结果。过去，在医院进行检验、检查、体检的所有结果必须凭单到医院领取，不方便且耗时。如能把检验、检查结果放在医院网站上，患者只需输入卡号和密码就可以在电脑上看到并打印检验、检查结果，既方便了病患，又减轻了医务人员工作负担。
- 人性化的病人关怀。当今，衡量一所医院的竞争优势，已不再仅仅局限于医疗技术和设备配置方面，还要比服务、比特色。而且，越来越多的患者需要快捷、方便地得到医院全方位的服务。如就诊后，医院会通过网络或电话征询满意程度，可以阅读到医院关于疾病预报和疫情通报的短信，方便地得到生活必须的医学常识。每当季节交替，医院会发提示短信提醒注意季节变化，预防感冒等消息。这些服务让病人觉得十分温暖，增加了其对医院的忠诚度。

2） 院内服务需求

目前院内就诊流程繁杂、不合理，且需要让患者自己去适应就诊各个环节，从而给患者带来许多不便，也使医院的某些工作处于混乱状态。

希望通过各类院内患者服务打造智能化、人性化、一站式诊疗服务，进一步

提高医院服务质量。其主要需求如下：

- 提供预约服务。由于有的检查要求检查前空腹或憋尿等特殊准备，而检查在不同的科室进行，不能保证患者的检查流程比较合理。提倡电话、手机短信、网络、现场预约等方式，以便于分流人群、缩短候号、候诊时间。
- 提供候诊区服务功能。患者挂号后大多坐在候诊区域等候，在候诊区通过电子显示屏、触摸服务屏等手段播放医院介绍、形象宣传、专科信息、门诊时间、急诊信息、流行病预防、专家介绍、就诊流程、科室分布图、各科室介绍、科室主要医生介绍等。在患者就诊的整个流程中，只有这个环节最能使患者得以安下心来坐在椅子上等候医生接诊。一方面分散患者注意力、减少候诊焦虑。还可增加患者对医院的了解，进行健康教育，宣扬医院文化，起到投入少、效益大的良好效果。
- 提供良好的导引服务。医院普遍存在的一种现象是患者拿到检查单不知道去哪里作检查，大部分患者需要通过询问才能知道到何处做检查。应通过语音播放、电子地图、自助查询、电子路标、处方备注等手段方便患者寻找科室。
- 提供透明的诊疗费用查询服务。医疗收费长期以来一直是雾里看花，通过设立费用查询服务，患者可以查询到门诊处方费用明细、住院费用明细、并能查询标准药品及服务项目收费价格等，有效提高了医疗服务收费的透明度，增加了患者满意度。
- 提供简便省时的结果查询手段。过去在医院进行检验、检查、体检的所有结果是由各相关科室录入后打印出来送到查询处，查询处人员再按患者姓氏分门别类归置，患者需要到查询处排长队等候领取检验检查报告单，不方便且耗时。通过提供自助查询、自助打印服务，使患者不用再排队等候领取，既方便了病人，更好地保护病人隐私，又减轻了医务工作人员的负担。
- 多种交费手段缩短患者交费时间。一次就诊，多次交费，反复排队，且交费排队时间长一直是医院就诊的一个老大难问题。为缓解这种情况，建议采用自助银行卡交费、手机交费、医院一卡通预存款交费等多种手段，帮助患者轻松实现划价、交费零等候。
- 提高医生、护士反应速度。当前，业内提出了“时间生命线”概念，如患突发性疾病的患者，在最快时间内得到抢救和及时治疗，就能有效提高生存希

望，减少悲剧的发生。通过无线定位、床前呼叫、输液监控等手段有效提高医生、护士反应速度，使其能在患者需要服务的第一时间赶到现场，提高患者满意程度，关键时刻还能挽救患者生命。

6.1.7.2 主要功能

表 6-18 患者公众服务主要功能

服务分类	服务方式	功能
院外服务	医院网上服务（即患者公众门户）	健康信息发布
		医院资料查询（科室、专家、接诊时间）
		检验检查报告查询
		就诊记录查询
		处方查询
		费用查询
		网上咨询
		网上预约挂号
		网上回访
		网上投诉
	医院短信平台	短信预约挂号
		短信交费
		空床通知
		候诊短信提示
		短信咨询
		短信药价查询
		短信检验报告查询
		短信回访
		短信投诉
	医院呼叫中心	电话预约挂号
		电话咨询
		电话回访
		电话投诉
院内服务	病人自助终端	自助挂号
		医院电子地图查询
		医院科室、专家介绍
		处方、费用自助查询
		检验检查报告自助打印
		自助交费
		健康信息查询
	患者提示	电子显示屏提示
		语音提示
		语音叫号

	无线应用	床边紧急呼叫
		医生无线定位
		患者无线追踪
		无线输液监控

6.1.7.3 系统支撑环境

患者公众服务包含院内服务和院外服务，其系统支撑环境与医务人员门户、医院管理人员门户类似，参见 6.1.7.2 章节。

6.1.7.4 案例分析

6.1.7.4.1 医疗机构呼叫中心、短信通知

通过医疗机构的呼叫中心系统（Call Center），可以为患者提供电话相关医疗服务。包括电话咨询、门诊挂号预约、相关业务查询和提示等等。呼叫中心的模式可以是自动语音的，也可以是人工坐席，或者两者混合的模式。

王军最近一直觉得嗓子不舒服，想到医院去看看，但又不愿意早起排队挂号，这天正好听说附近的区医院可以打电话挂号，于是决定试试。他拨通了医院的预约电话，自动语音提示他已经连接到医院呼叫中心系统，按照语音向导提示操作，王军查到第二天耳鼻喉科李大夫的出诊信息，于是他预约了就诊并留下联系方式。几分钟后预约确认短信就发到了他的手机上，回复确认后，王军成功的完成了电话约诊。

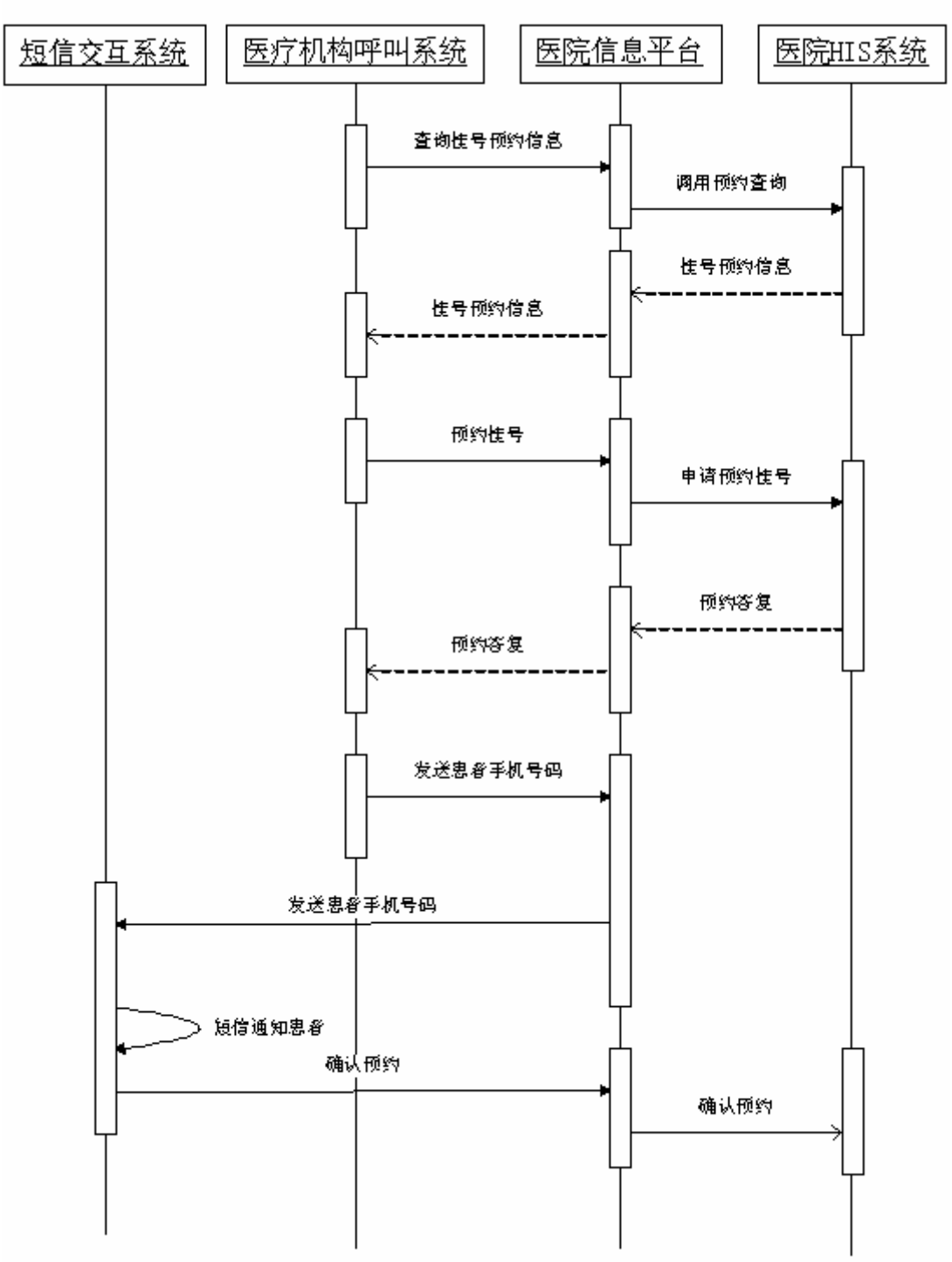


图 6-14 医院呼叫中心业务活动图

6.1.7.4.2 门诊预付费

随着医院信息化越来越普及，运用信息技术可解决患者排队多的难题。门诊预存款服务正是在原有医院信息系统的基础上，通过改变患者的看病流程，解决

了患者在看病过程中多次排队的现象，患者到医院只需在一卡通帐户预存费用，就可以免去就诊排队时间长、排队次数多的苦恼。

预存款式一卡通就诊模式全面取消了传统模式下的挂号、划价、交费等与患者诊疗没有密切关系的辅助环节。患者初次来院就诊，到办卡处办理医疗一卡通，并将就诊过程中可能需要支付的款项提前预存到一卡通账户上，在整个就诊过程中发生的费用支出均从该账户扣减，如果患者已经拥有“一卡通”则直接到分诊台分诊。

当系统呼叫到该患者即可进入诊室就诊，医生经初步诊断后开具电子检验检查申请单、治疗申请、电子处方等，患者可以直接到相应的检验检查科室、治疗科室进行刷卡确认身份、扣减费用、进行检查治疗，不需要到收款处交费。经过检查确诊后，根据治疗需要开具电子处方、治疗申请单，患者持卡到相应药房刷卡取药或到治疗部门刷卡治疗，就诊结束后到办卡处结算、打印收据并将就诊余额退还，完成就诊。

图 6-15 预交金场景示意图

6.1.7.4.3 网上预约挂号、网上病历查询

患者可以通过医疗机构的门户网站，进行预约挂号业务。为患者带来了方便，减少了去医院排队挂号等待的时间。

区医院为了更好的为居民服务，提供了网上自助服务。李军现在只需通过互联网登陆区医院自助服务首页，选择预约挂号，就能提前预约就诊。并且就诊完毕后，还能通过网站查询自己的电子病历信息。

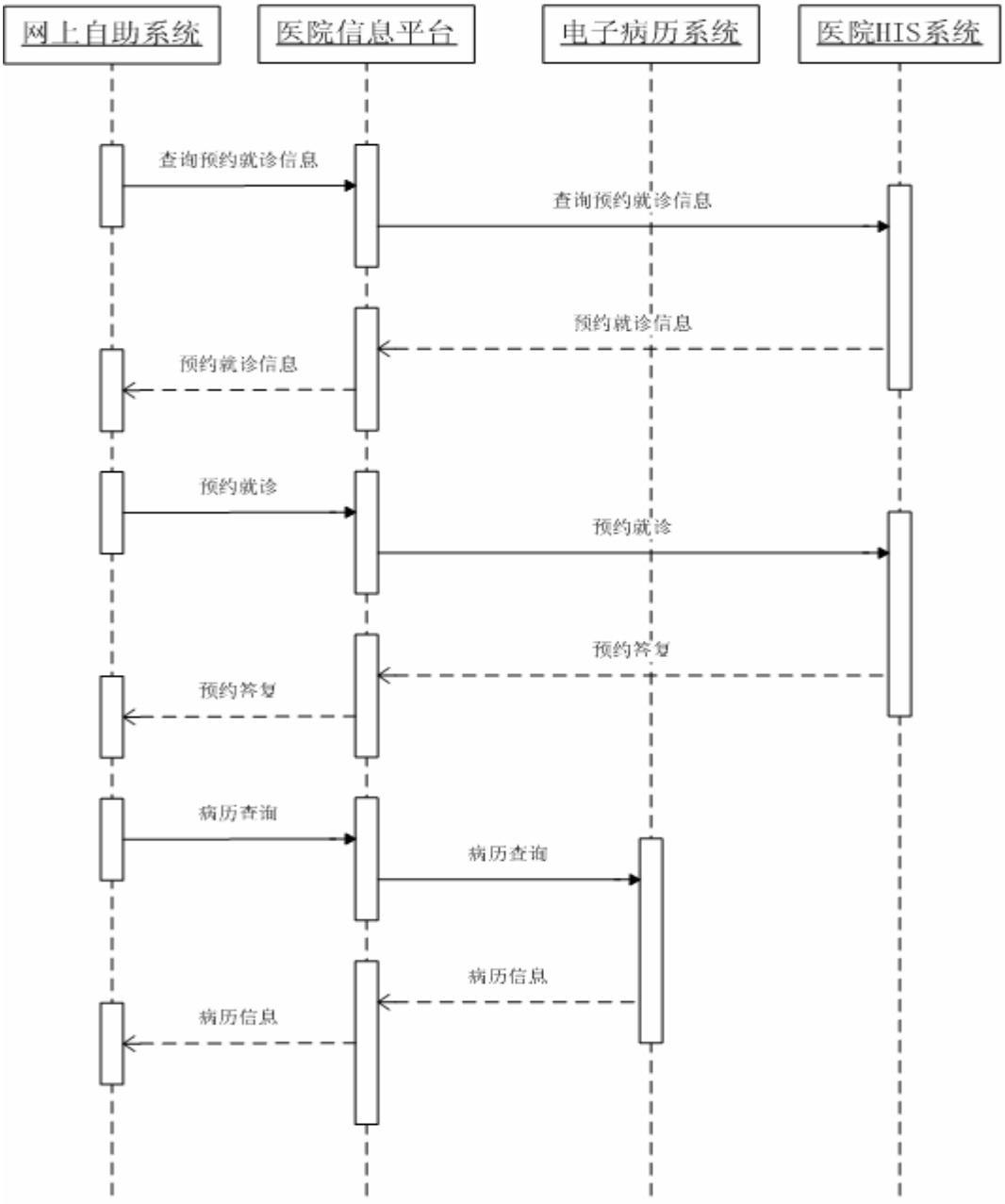


图 6-16 网上预约挂号活动图

6.1.7.4.4 自助查询、自助打印化验单

医疗机构可以提供多种方式实现患者自助查询、自主打印化验单业务。比如通过患者服务门户（包括 Web 门户和 WAP 门户），医疗机构内的自助终端。

过去检验报告放在检验室窗口旁，旁人可随意翻看和提取。这样患者隐私得不到保护，被不认识的人看了也就算了，如果碰巧被熟人翻看到，又不想被对方知道隐私，后果就会比较严重。而且更严重的是，没人看管，检验报告有被人拿走、丢失的可能性。现在区医院新实行的自主打印报告单系统解决了这个问题。李军发现在检验窗口多了一台自助终端，现在取检验报告只需刷一下就诊卡，就能方便、安全的取到自己的检验报告，再也不用担心以前的那些麻烦了。

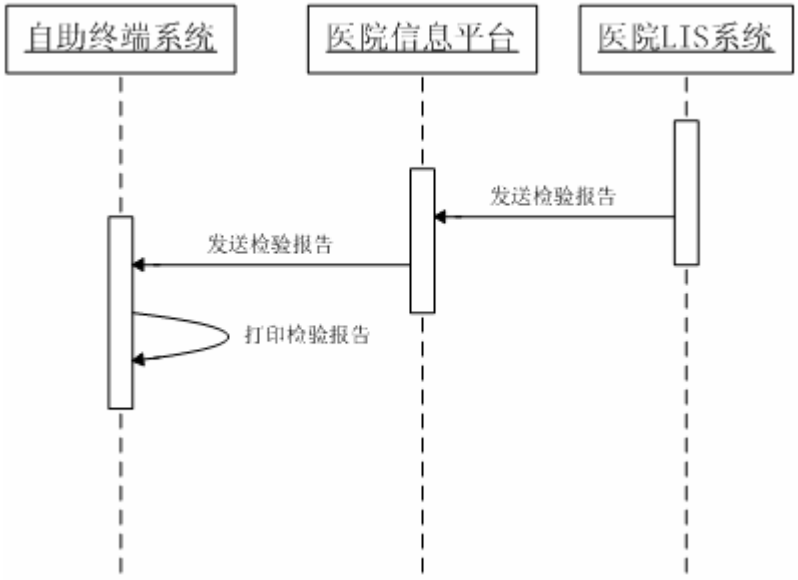


图 6-17 自助查询、自助打印活动图

6.1.7.4.5 住院空床通知

医疗机构业务繁忙时期，住院病床非常紧张，对病床资源的合理调度和充分利用提出挑战。利用医疗机构信息化手段可以实现患者病床排队，有空床时自动对患者进行通知。通知方式可以是手机短信，自动语音，电子邮件或患者门户消息。

李军在最近的体检中被确诊胆结石，医生建议手术治疗，但区医院最近床位紧张。医生告诉他医院可以提供空床通知服务，得到李军同意后，医生帮他在系

统中发出了空床等待申请。一周后李军得到短信通知，医院已经有空床可以住院，回家在网上自助系统再次确认后，李军第二天住进了区医院等待手术治疗。

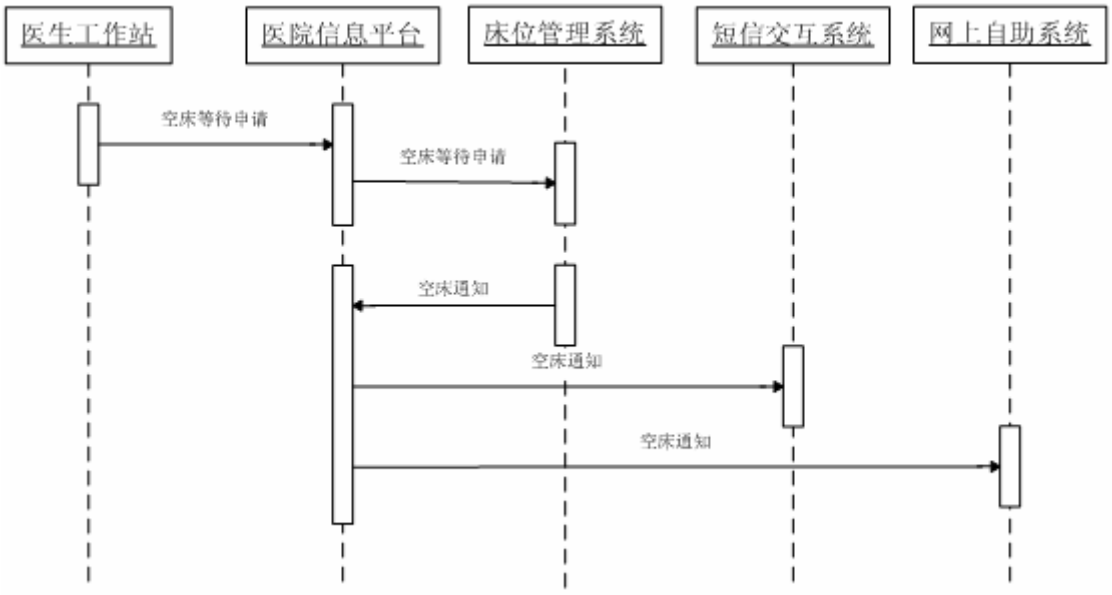


图 6-18 短信空床通知活动图

6.2 基于平台的业务协同

6.2.1 与临床相关的业务协同

通过基于电子病历的医院信息平台建设，使整个临床业务活动能基于医院信息平台更为充分的实现信息的共享与交换。实现各项临床业务活动在信息使用层面上最大程度的业务协同。使实际临床业务工作在充分的信息利用条件下实现提高业务效率、减少临床差错、降低业务成本、提高临床服务满意度。

6.2.1.1 需求分析

电子病历作为所有和临床业务活动相关的业务活动信息与数据的集散地，在基于电子病历的医院信息平台建设中，与电子病历相关的业务协同活动将是最主要也是最活跃的系统协同活动。从患者进入各项医院的服务环节开始，从查房到医嘱产生、到医嘱主动或被动的执行以及医嘱执行后患者的各项主观、客观指标

或数据的产生与记录，通通需要和电子病历产生业务协同行为。大量临床业务活动信息在医院信息平台上进行实时、非实时的共享与交换。各种临床业务活动不断的产生各种电子病历文档被记录与存储，不断地成为电子病历文档的数据源，医院信息平台将各类信息进行汇总，用以支持后续的临床业务活动。这些信息可能来源于手工记录、医疗设备、医疗仪器，或者各种临床信息系统。

6.2.1.1.1 电子病历与业务系统之间的业务协同

电子病历文档作为临床业务中最重要的信息载体，它的信息与数据来源于各个日常不断运转的业务系统之中，反映各项业务系统在患者发生临床业务活动的最终状态。

各种管理系统、临床业务系统、临床医技系统都在为电子病历文档提供着各种信息。而这些系统都在不间断与医院信息平台进行着信息与数据交换，电子病历则通过在平台中的信息共享与交换，按照规范、内容框架与标准来组织 EMR 文档并汇集到 CDR 进行存储。

在医技类临床业务发生时，集成的电子病历信息将成为医技项目执行时的重要信息参考，包括在执行医技项目前患者的基本状况、病情、病史、辅助检查等情况，避免因为信息了解的缺失与不及时导致医疗差错或过失情况的产生。

电子病历应当能够为其他系统提供尽可能完善的汇总临床信息，包括来自其他临床信息系统中的信息与数据，使基于电子病历的医院信息平台发挥最大效用。可以通过电子病历浏览器的方式提供或者通过基于电子病历的医院信息平台智能化分析引擎，将与执行该医技项目相关的临床信息与内容组织起来推送到执行者的终端，帮助其更好的识别需求与风险。

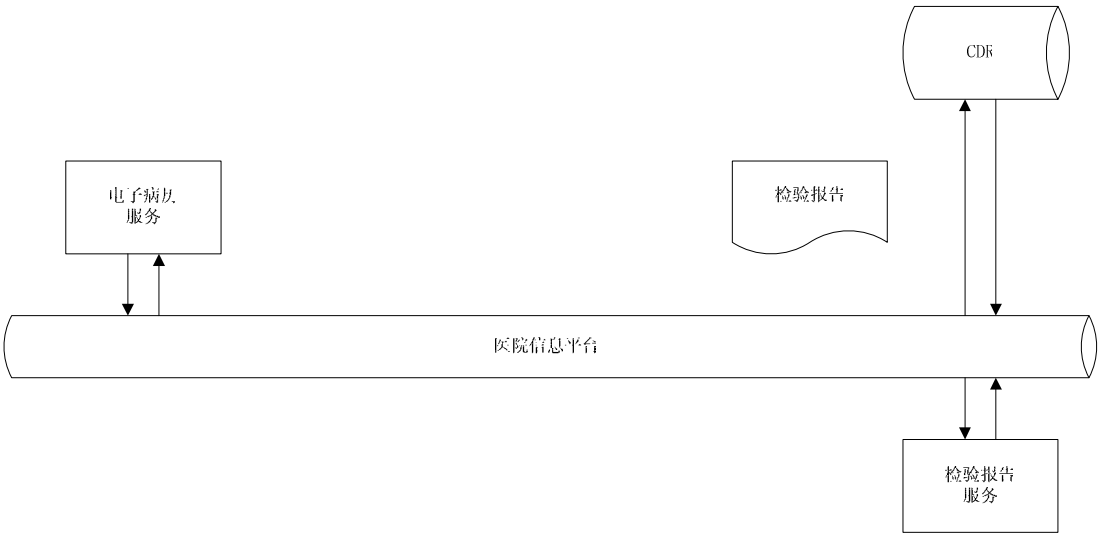


图 6-19 电子病历与业务系统之间的业务协同

6.2.1.1.2 各业务系统之间的业务协同

在不同的业务系统之间，业务协同随着业务的发生而不停地产生。传统实现方式可以通过两个系统之间进行点对点的直接数据与信息交换进行业务协同，但这样的方式无法实现被交换的数据重复利用。

通过借助医院信息平台实现业务协同以及协同的数据与信息交换，这样在业务协同过程中的数据与信息将得到最充分的利用，同时也减少了在各个系统间进行点对点的协同服务开发带来的成本增加，使点对点的业务协同转变为多点系统间的业务协同。

如以下案例所述，数据与信息通过平台被多个协同业务共享，同时各协同业务产生不同的 EMR 文档并存储于 CDR 当中，以便将来发生其他临床业务时进行调用。

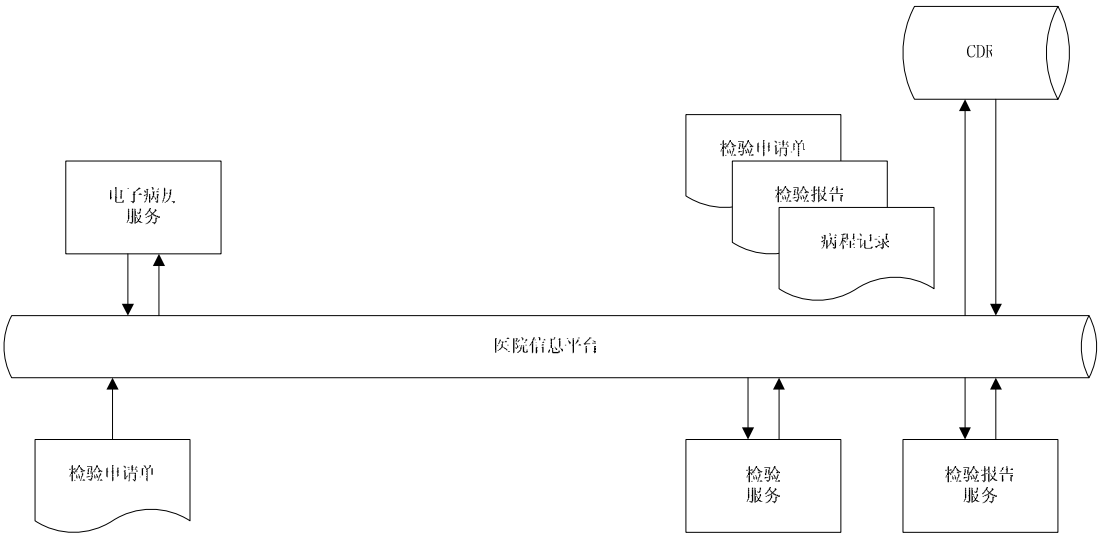


图 6-20 各业务系统之间的业务协同

6.2.1.2 案例：检验信息系统与电子病历业务协同

一名先天性心脏病、房间隔缺损患儿全麻体外循环下房间隔缺损修补术后，术后监护室医生通过系统提交了进行血钾浓度测定的检验申请。通过整合的电子病历系统，一份包含患者诊断的检验申请单被提交到医院信息平台之上。医院信息平台通过识别检验类别和项目，将申请单提交给医嘱服务、住院记账服务；医嘱服务完成对检验标本采集执行确认后，通知住院记账服务完成记账；之后申请单被提交给检验接收服务，检验接收服务将申请单信息接收，并发回回执；检验系统通过检验样本核收完成送检样本与检验申请单的核对与确认后，检验仪器开始对样本进行检测并返回检测结果给检验系统；检验人员将检测结果与检验申请单的信息进行对照并给出检验结果建议。这时检验人员发现检验申请单提供的信息不充分，随即使用检验系统通过医院信息平台发送查看该检验项目患者的电子病历信息，获得该患者的术后病程记录。经评估，检验人员认为此次的血钾浓度高出正常值应考虑术中体外循环时间过长，红细胞破坏导致的血钾浓度过高，建议隔 1 小时候复查血钾浓度。

在整个业务交互过程中，申请单的产生激活了医嘱服务，医嘱服务激活了住院记账服务，记账服务激活了申请单状态确认服务，申请单激活了检验服务，检验服务激活了病情摘要服务，发回检验报告激活了检验报告服务。过程中产生的申请单 EMR 文档、检验报告 EMR 文档、反映本次业务发生情况的病程记录的 EMR 文档都将进入 CDR。为将来可能发生的电子病历调阅服务、患者临床数据

分析、预警等服务完成文档、信息与数据的存储。

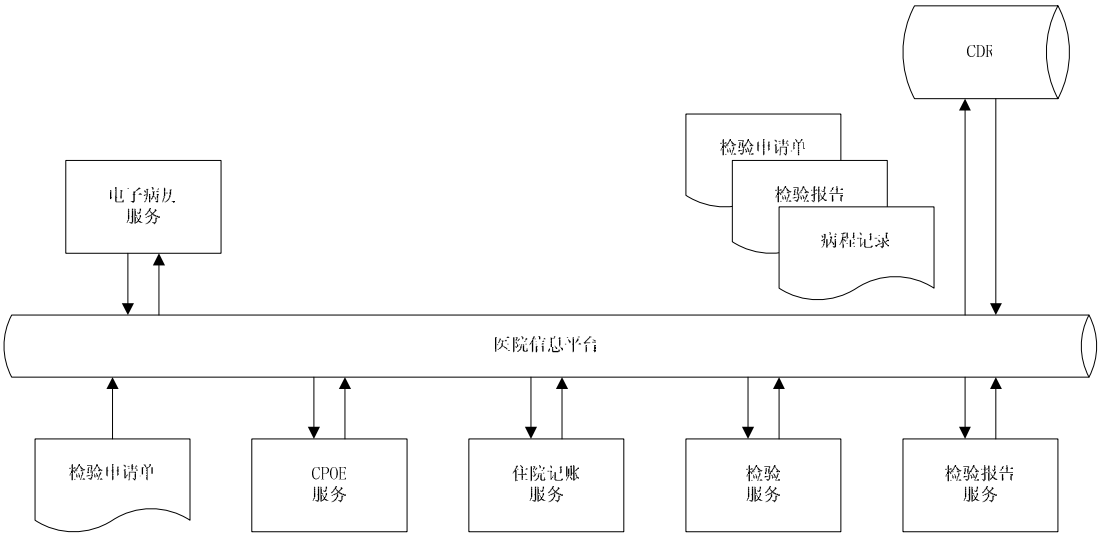


图 6-21 检验信息系统与电子病历业务协同

6.2.2 与医院管理相关的业务协同

为提升医院的管理水平，实现医院精细化管理和运营，逐渐有一些医院将 ERP 的管理思想和管理方法引入到医院的运营管理领域中来，建设 HRP（Hospital Resource Planning）系统。医院 HRP 是指建立在信息技术基础上，以医院的人、财、物资源为管理对象，实现医院运营目标为方向，引入先进的、系统化的管理思想，有效保障医疗质量、降低医院运营成本、提高工作效率、提升管理水平，为医院决策层及员工提供决策运行手段的管理平台。

医院 HRP 主要分为两个层面，一是支持医院正常业务流转的各类运营管理系统，如人力、财务、物流等，二是建立在这些业务系统之上的管理决策系统，本节主要探讨在建设基于电子病历的医院信息平台背景下 HRP 决策支持与平台的交互协同关系。

1) **HRP 运营管理与决策的目的：**

- 建立以财务为核心的医院运营一体化平台，实现财务、物资、资产的有效管理，并实现资金流、业务流、数据流的同步和信息共享；
- 建立医院后台运营管理标准，统一基础信息；
- 制订符合医院的管理流程，全面实现运营管理信息化，将医院与运营管理相关的每个环节，每个方面都纳入管理体系；

- 提升工作效率，有效降低运营成本；
- 通过运营平台，建立事前、事中、事后控制体系，实现医院运营目标；
- 开放的平台，流程、表单、报表可以根据用户需求灵活定义；
- 基于 BI 建立医院职能分析平台，对数据进行深度挖掘分析；

2) HRP 核心价值：

a) 财务管理

✓ 实现财务集团化管理

- 通过医院与分院的账表合并，实现财务集团化管理；
- 制订统一的核算方式、会计科目，实现财务的统一管理；

✓ 实现财务一体化管理

- 财务系统与医院收费系统、物资系统、资产系统、日常报销等各种系统整合，实现财务一体化管理；
- 实现对供应商往来、科研项目经费的准确核算；

✓ 满足日常管理需求，提高工作效率

- 满足财务日常的账务处理要求；
- 自动生成各种凭证，提高工作效率；
- 建立财务报销工作流，实现网上报销审批；

✓ 强化财务监管职能

- 财务可以实时了解医院物资、资产的使用状况，强化财务监管职能；

b) 成本核算

✓ 建立医院核算体系实现全成本核算

- 建立医院全成本核算体系；
- 实现医院的科室全成本核算；

✓ 有效控制成本，准确指导科室经营

- 通过成本分析，准确找到科室的成本控制点，进行成本的有效控制；
- 指导科室的经营管理，找到成本控制方法和提升效益方法；

✓ 为预算管理和绩效考核提供依据

- 成本核算的结果，为编制预算提供详实的数据依据；
- 成本核算的结果，为绩效考核提供数据参考；

c) 预算管理

✓ 灵活的预算编制方式和准确的编制结果

- 根据医院需求，可以选择“自上而下”或“自下而上”的编制方式；
- 基于临床科室业务工作量的预算编制结果，符合医院的实际情况；
- 预算对象落实到每个职能科室和管理科室，实现全院所有科室的预算管理；
- 预算内容包含：收支预算、专项预算等医院所有经济活动；

✓ 建立医院的预算事前控制体系

- 在预算编制环节和预算的实际执行环节进行预算控制，真正发挥预算在医院的事前控制作用；
- 在事前控制体系下，医院“有计划的赚钱，有计划的花钱”，一切尽在院长和领导班子的掌控之中；

✓ 实现预算的有效分析

- 及时分析预算的执行结果，提前预测预算可能出现的问题；
- 对每个科室、每个项目的预算进行分析；

d) 物流管理

✓ 实现医院所有物资的管理

- 普通材料/高值材料/植入材料/代销材料都纳入到物资管理中；
- 材料的信息完整（条码、品名、效期、类别、费别、三证等任何信息）；

✓ 建立完整的管理流程

- 从物资的需求计划、采购、入库、移库、出库、消耗每个环节的管理，实现真正的物流管理；
- 根据不同的材料（普通/代销/高值）针对性的设计管理流程；

✓ 确保材料安全

- 加强“三证”管理、实时检测，确保材料安全；

- 加强对效期、灭菌日期等管理；

✓ 引进先进技术，提高工作效率

- 流程中信息、数据可以自动导入，提高工作效率；
- 引入个体条码管理，实现耗材的全程跟踪；
- 引入品种条码管理，通过无线条码枪实现库房移动盘点；

✓ 供应商管理及分析

- 对供应商付款进行实时、准确的管理；
- 对供应商的供货价格、供货效率进行分析，评出优质供应商；

✓ 二级库/科室库管理

- 实现医院的二级库和科室库的管理，将管理触角伸向医院的任何角落，确保物资的有效管理；
- 财务核算由“以领代销”转变为“实耗实销”；

✓ 与 HIS 系统的有效整合

- 收费材料入库自动核对收费字典，及时提醒更新；
- 收费材料可以分析每个科室的材料收费情况，确保材料用到患者身上；

✓ 消毒供应管理

- 消毒包的条码跟踪管理，对消毒包的收/发/清洗/消毒等每个过程进行跟踪管理；
- 医用包的价格核算和收发管理；

✓ 及时预警，避免事后损失

- 短缺货预警，有效期预警，证件预警等各种预警，避免医院造成事后损失；

3） HRP 与医院信息平台的交互协同

HRP 系统作为医院内信息化建设重要的一环，其正常运行与医院临床业务系统密不可分。通过数据交换，将医院临床业务系统发生的数据传递到医院 HRP 系统中，满足运营管理的需要，实现医院信息流、数据流、物流、资金流的统一，从而实现医院管理、系统的高效协同、统一管理。

6.2.2.1 需求分析

医院管理虽然从管理内容上包括医疗管理和运营管理，但是实际上两方面的管理相互间有着非常密切的联系，可以说是一个完整的体系。医院在经营过程中产生大量与管理相关的数据，运营管理系统需要对这些数据进行收集、整理、处理、利用，医疗管理每时每刻都在影响着医院的运营管理。同样，运营管理也在影响着医疗管理，辅助医疗管理决策。因此，要求医院运营管理系统实时的与平台及医疗管理系统进行数据交互，传递相关信息，辅助管理决策。

医院运营管理与平台交互的数据非常多，总体来分，可以分为三类：

1）财务数据的交互

伴随着医院业务活动的变化，医院的财务数据也在不断发生着变化，因此平台与财务系统有着大量的数据交互。例如：收费系统每时每刻都在收费，收费的信息（包括：收费类别、收费科室、收费金额、患者信息等）必须及时、准确的传递到财务系统中，以便财务系统可以及时反映医院的收费，医院实时掌握收费状况，实现资金流的同步核算。

2）物流数据的交互

医院物流与业务关系最为紧密，医生每开一张处方，都可能会开药品，为医院药品管理系统传递药品信息。开处方的同时，医疗系统需要判断该药在医院是否还有库存，能否正常开出，这一切都离不开医生工作站与药品管理系统的交互。

卫生材料也是如此，医生在下医嘱时，如果系统判断使用材料没有库存，那么应该自动生成该材料的需求计划，方便医院进行订货采购。材料在医疗过程中消耗收费，系统应该自动消减库存，确保材料库存的准确性。

医疗设备的工作量、质量情况及时反馈到固定资产管理系统中，实现固定资产的效益评价。

3）人员信息的交互

医生的出诊情况、排班情况等人员相关信息，及时传递到人力资源管理系统中，确保考勤信息的准确。

医院绩效考核的内容包括了医疗质量、服务效率、患者满意、科研、医疗安全等各类指标的考核。此类考核指标的执行结果产生于医院的诸多系统，包括了临床系统和医疗管理系统。因此，绩效考核系统需要从医院信息平台中将相关数

据提取，进行统计、汇总、计算，形成绩效考核需要的考核数据。

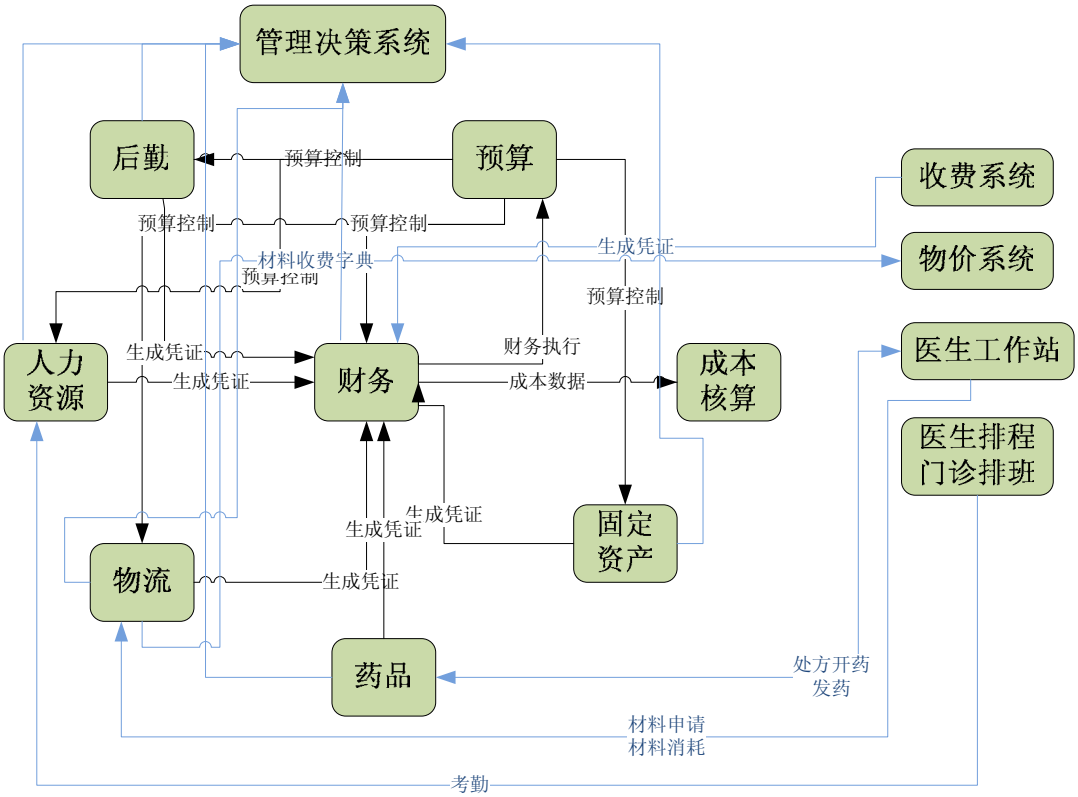


图 6-22 医院运营管理与信息平台交互图

6.2.2.2 功能设计

医院 HRP 系统与医院信息平台的交互主要分为两类：

1） 利用平台进行消息转发，实现实时业务数据交互，避免了原来与所有系统点对点的连接方式，在此过程中主要使用平台提供的以下服务：

表 6-19 HRP 使用平台消息交互功能列表

功能	子功能	功能描述
系统服务	平台注册服务	注册交互平台、系统、接口等相关信息
	交互设置	设置交互的相关参数，包括交互的系统、交互的频率、交互的协议、流程等
消息服务	消息校验	消息交互前的数据校验
	消息转换	消息格式转换
	消息转发	实现数据交互，并将交互结果反馈给相关系统

	消息日志	记录数据交互的日志

2) 对于非实时性业务，例如统计、决策等，可直接使用医院信息平台中的ODS 库，实现非实时数据交互，避免对医院临床业务系统造成压力。

ODS 资源库既能基本反映医院的实时运营状态，又不会给 HIS 的实时业务服务带来压力，同时也能够满足管理需要。大部分的统计报表、数据分析和数据挖掘工作都可以在 ODS 资源库上完成。

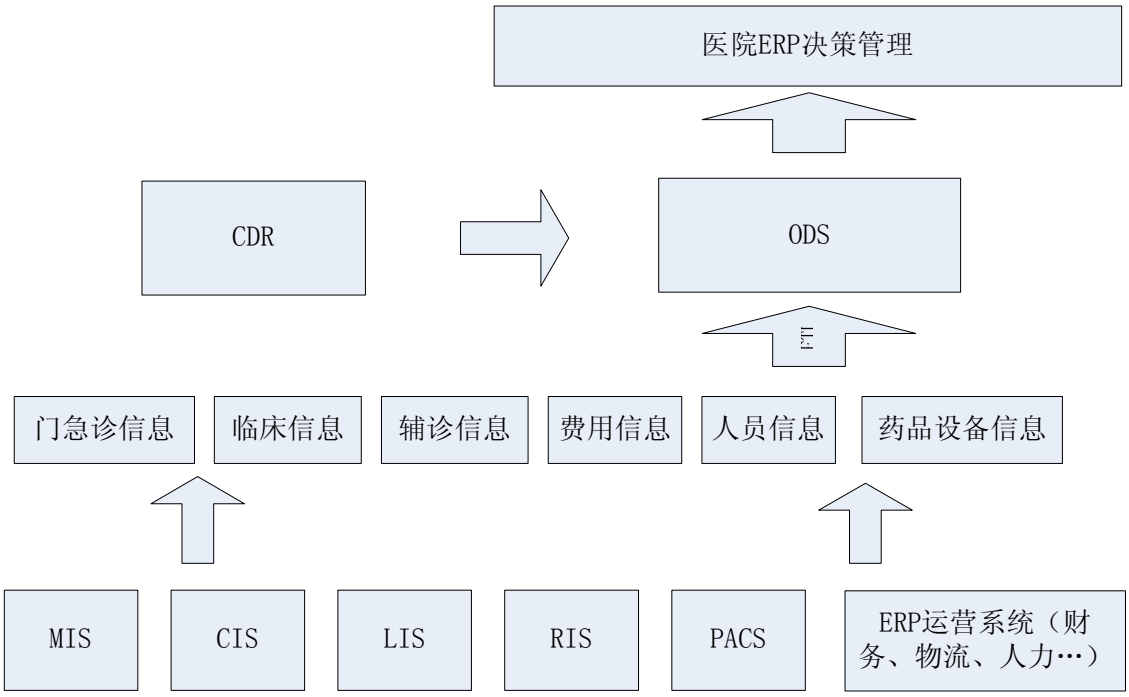


图 6-23 HRP 与平台 ODS 数据交互图

在此过程中主要使用平台提供的以下服务：

表 6-20 使用平台数据服务列表

功能	子功能	功能描述
系统服务	平台注册服务	注册交互平台、系统、接口等相关信息
	交互设置	设置交互的相关参数，包括交互的系统、交互的频率、交互的协议、流程等
ODS 数据服务	数据抽取	从业务系统中抽取数据
	数据清洗	清洗“脏数据”
	数据转换	按照管理需求转换数据格式

	数据查询	提供多维度的数据查询

6.2.2.3 案例：费用信息交互

案例描述：

患者到医院就诊，在医生开具处方后，患者到门诊收费处交费，门诊收费员根据物价收费，在收到患者现金后给患者打印收费发票，完成收费过程。财务以日为单位进行收入记账，医疗系统的收费信息传递至医院信息平台，平台根据配置将收费数据转发到财务系统，生成当日门诊收入凭证，完成财务系统与收费系统的数据交互。同时费用数据每天被定时抽取到 ODS 库中，供成本核算、财务统计查询使用。

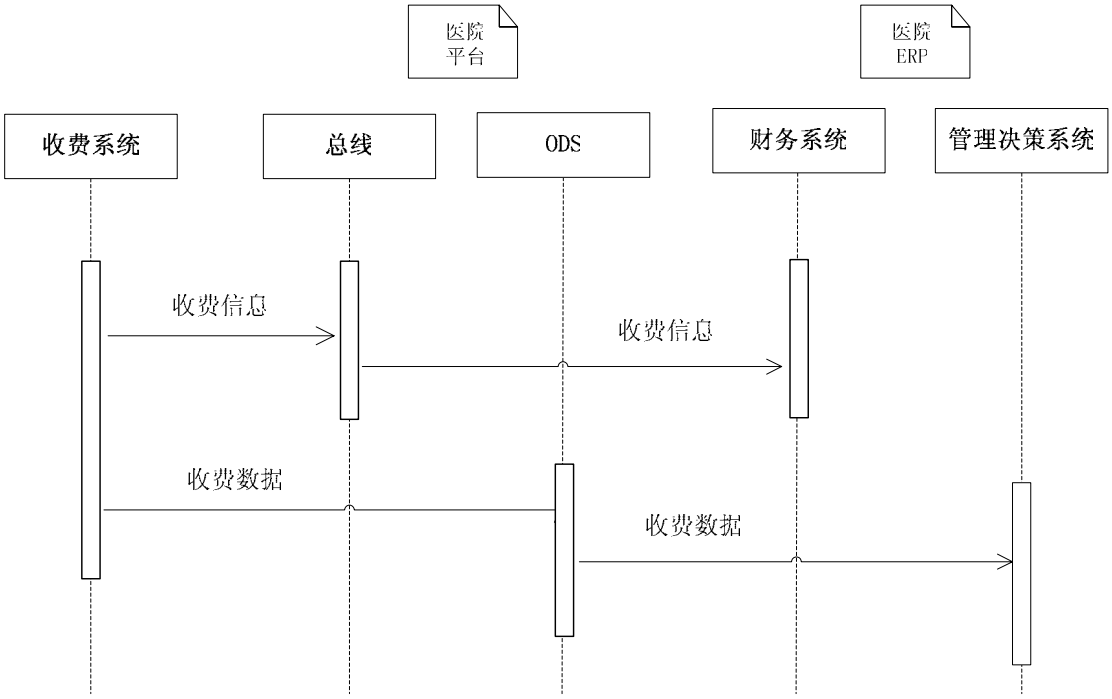


图 6-24 收费数据交互活动图

交互过程：

1) HIS 系统生成收费信息并将其发送到医院信息平台总线服务上；
2) 总线接收到信息后检查消息格式，并根据需要转换编码（如收费项目、疾病编码、药品目录等）；
3) 总线根据路由规则将消息转发到事先注册的所有消费接口；

4) 收费信息被路由到财务系统；
5) 财务系统处理收费信息并生成收费凭证；
6) 医院信息平台每天在非业务繁忙期定时调用 ETL 服务将包括收费数据的各类业务数据抽取到 ODS。
7) HRP 管理决策系统根据需要调用 ODS 数据查询接口获取信息。
8) HRP 管理决策系统利用获取的数据形成统计分析报表。

6.2.3 与区域卫生信息平台的互联互通

区域医疗是医院信息化发展的第三个阶段。区域医疗是为了支持医院在区域范围内的信息共享、业务协同。通过医院信息平台与区域卫生信息平台的对接，实现两级平台信息共享、业务协同。跨医院之间的信息共享、业务协同包括区域一卡通、区域诊疗信息共享、区域医疗协同、区域辅助医疗和区域医疗公众服务等应用。

- 要实现区域信息共享、业务协同，首先必须实现患者身份唯一识别。区域医疗一卡通就是用于解决这一问题。
- 两级平台上传、下载诊疗信息，需要通过代理完成，代理从医院信息平台采集健康档案需要的信息，上传给区域信息平台。代理从区域信息平台下载健康档案，供医院信息平台的电子病历浏览器调阅。医院端信息共享代理的建设解决诊疗信息上传、下载的问题。
- 医院要完成跨院转诊、转检以及远程医疗等业务，需要区域卫生信息平台提供服务，建立链接。同时医院也要将本院的服务注册到区域卫生信息平台之上，才能被其他机构调用。区域医疗协同系统就是解决跨机构业务协同的问题。
- 区域卫生信息平台上，有患者的健康档案（包含患者完整的诊疗记录）、诊疗安全警示等医疗辅助决策系统，只有依托完整的诊疗记录才能发挥真正作用。医生应该能在工作站上调用区域平台上的医疗辅助决策系统，帮助自己做出准确、高效的诊断。区域医疗辅助决策系统实现以上功能，并解决如何被医院端调用。
- 患者希望通过互联网方便的预约门诊、查看报告、了解各家医院的医疗

资源信息，这就需要各家医院将这些信息通过服务注册到区域卫生信息平台上，区域平台通过门户进行整合，为公众提供完整信息。区域医疗公众服务系统实现这些功能，并注册到区域平台之上。

6.2.3.1 需求分析

6.2.3.1.1 区域一卡通需求分析

为了实现跨医院的信息共享和业务协同，首先要实现对患者身份跨医院的识别。从患者持卡就医情况来看，目前主要使用的有两类卡，一类是医院外部发行的社会保障卡、医保卡、二代身份证等，一类是医院自己发行的自费就诊卡。对于持外部发行的卡的患者，可以从卡号唯一识别患者身份；对于自费就诊患者（该人群数量相当庞大），由于在医院之间存在重号的可能性，因此自费就诊卡卡号只能在医院内部作为身份唯一识别，而不能在区域内作为身份唯一识别的依据。为了实现医院间的患者相关业务信息的跨院互认，须建立代替各家医院自行发行的自费就诊卡，即区域统一就诊卡。

6.2.3.1.2 区域医疗协同需求分析

为了合理利用各基层医疗卫生机构的服务功能和网点资源，促使基本医疗逐步下沉社区，社区群众危重病、疑难病的救治到大型医院，形成“小病在社区、大病进医院、康复回社区”的就医格局，需要实现社区/乡镇卫生院与二三级医院之间的转诊、转检。

为了充分利用区域卫生资源，发挥二、三级医院在人才、技术及设备等方面的优势，支持医疗卫生资源薄弱的地区，需要区域远程医疗。

6.2.3.1.3 区域辅助医疗需求分析

有了患者完整的健康档案之后，可以以此形成辅助知识库，为医生提供辅助医疗的服务。一方面可以通过重复用药提醒、重复检验提醒和重复检查提醒，减少不必要的用药、检验和检查，降低医疗费用；另一方面通过药物过敏警示和治疗安全警示系统降低医疗风险，保障治疗安全，提高医疗质量。

6.2.3.1.4 区域医疗公众服务需求分析

患者可以借助区域医疗公众服务，预约各类医疗服务；查询各类检验检查结果；对各类医疗卫生资源进行查询等。区域医疗公众服务通过电子化的手段向患者提供服务，包括短信、电子邮件、电话传真及门户网站等方式，可以方便患者就医。

6.2.3.2 功能设计

6.2.3.2.1 区域医疗一卡通系统

医疗一卡通系统的卡管理系统提供给应用层使用，应用层将患者信息注册到医院信息平台，并通过信息共享代理将信息上传到到区域卫生信息平台的卡管理中心。

医疗一卡通系统包括两大部分功能，分别是卡管理功能和卡管理中心功能。卡管理功能实现发卡、补卡、换卡、挂失、解挂、注销、解锁、密码重置、修改密码、黑名单等。卡管理中心功能实现密钥管理、卡资料管理、制卡发行、卡维护管理等。除了以上两大类功能，还要实现对卡相关的法规、制度和标准规范的管理功能。

6.2.3.2.2 区域医疗协同

区域医疗协同服务包括转诊/转检系统和远程医疗系统。

从医院的角度，双向转诊/转检包括转入、转出服务。转诊/转检系统包括下列功能：

- 支持基于区域平台的转诊事务管理和诊疗文档流转。
- 支持灵活的审批程序，支持自动/半自动基于审批规则的审批。
- 转诊患者（位置）跟踪。
- 支持转诊病历交换，支持标准转诊通讯协议。
- 支持跨区域平台之间的转诊事务管理和诊疗文档流转。

远程医疗系统包括两部分功能：会诊管理系统和视频会议系统。

- 会诊管理系统用于会诊过程管理和控制，包括会诊申请、会诊安排、会

诊提醒、诊疗档案预备和调转、会诊开展、会诊审计、会诊费用核算、会诊结束处理等功能。

- 视频会议系统将不同会场的实时现场场景和语音互连起来，在远程会诊中用于沟通患者（包括求诊方医生）和专家双方。

6.2.3.2.3 区域辅助医疗

区域辅助医疗包括治疗安全警示系统、药物过敏警示系统和重复治疗提醒系统等。

治疗安全警示系统的功能包括：

- 西医药物相互作用审查：对同一处方的西药品或不同处方仍在服用的西药品之间的相互作用审查。
- 中草药配伍禁忌审查：是指传统中草药处方中的“十八反，十九畏”审查。
- 西药与中成药配伍禁忌审查：对西药和中成药之间的配伍禁忌进行审查。
- 患病人群药物禁忌审查：对患有某些慢性疾病或某些急性疾病尚未痊愈的人群的药物禁忌审查。
- 特殊人群药物禁忌审查：针对老年人、儿童、妊娠期妇女、哺乳期妇女的药物禁忌审查。
- 检查、检验相关的禁忌审查：是指检验、检查与药物、人群之间的禁忌关系审查。
- 治疗相关的禁忌审查：是指治疗与药物、人群的禁忌关系审查。

药物过敏警示系统的功能包括：

- 特定的过敏类药品警示，例如青霉素。
- 患者存在家族过敏史警示。
- 患者属于特殊人群，其中包括孕妇、哺乳期妇女、儿童与老人警示。
- 患者具有过敏性体质警示。

重复治疗提醒系统的功能包括：

- 检验检查信息的采集：医院端，借助区域信息平台，从联网的各家医院采集患者每次诊疗的检验检查记录。

- 重复检验检查提示：医院端，通过嵌入在医生工作站的重复检验检查提示模块，过滤医生开立的每一条检验检查医嘱，进行时间比对计算，发现重复检验检查，在系统界面上及时提示。
- 检验检查知识库字典维护：区域平台端。提供维护工具，对检验检查知识库进行字典维护，维护的内容包括：检验检查项目名称、项目（统一）代码、有效时限等信息。
- 患者检验检查表推送：在患者挂号或者办理入院时，通过就诊医院的信息共享代理向区域卫生信息平台发送该患者的主索引编码和就诊医院的医院代码，区域平台可以根据接收到的主索引编码，快速检索到该患者的检验检查表，并推送指定医院（以医院代码为标识）的信息共享代理上，供医院端的重复检验检查提示模块调用。
- 查询：医院端的授权用户通过信息共享代理，远程查询区域卫生信息平台上的检验检查知识库。

6.2.3.2.4 区域医疗公众服务系统

区域医疗公众服务系统的功能包括：

- 各类医疗服务预约

例如预约门诊，主要是指专家或特需门诊的预约。建立统一的门户实现预约。这个预约需要与医院内部的挂号系统进行数据和流程上的联动。

- 各类检验检查结果查阅

查阅检验检查报告等。建立统一的门户实现查阅。对于某一份检验检查报告，是否允许提供网上查阅结果可让当事人选择。不选择时缺省为可供网上查阅。查阅时需要提供当事人的有关身份标志（社保卡号、就诊卡号或身份证号）。

- 各类医疗资源的查阅

查询医院大型检查设备的配置，查询医院诊疗科室的设置、查询医院病床数量的设置、查询专科专家医生等。

6.2.3.3 案例

6.2.3.3.1 区域医疗一卡通系统

患者身份识别是区域医疗共享所要解决的基本问题。通过患者身份识别，患者可以使用社会保障卡、医保卡、二代身份证，以及统一就诊卡在联网范围内任何一家医院就医。身份识别的基础是实现患者身份的匹配，建立在区域范围内患者主索引。

患者身份识别的技术架构如下图所示：

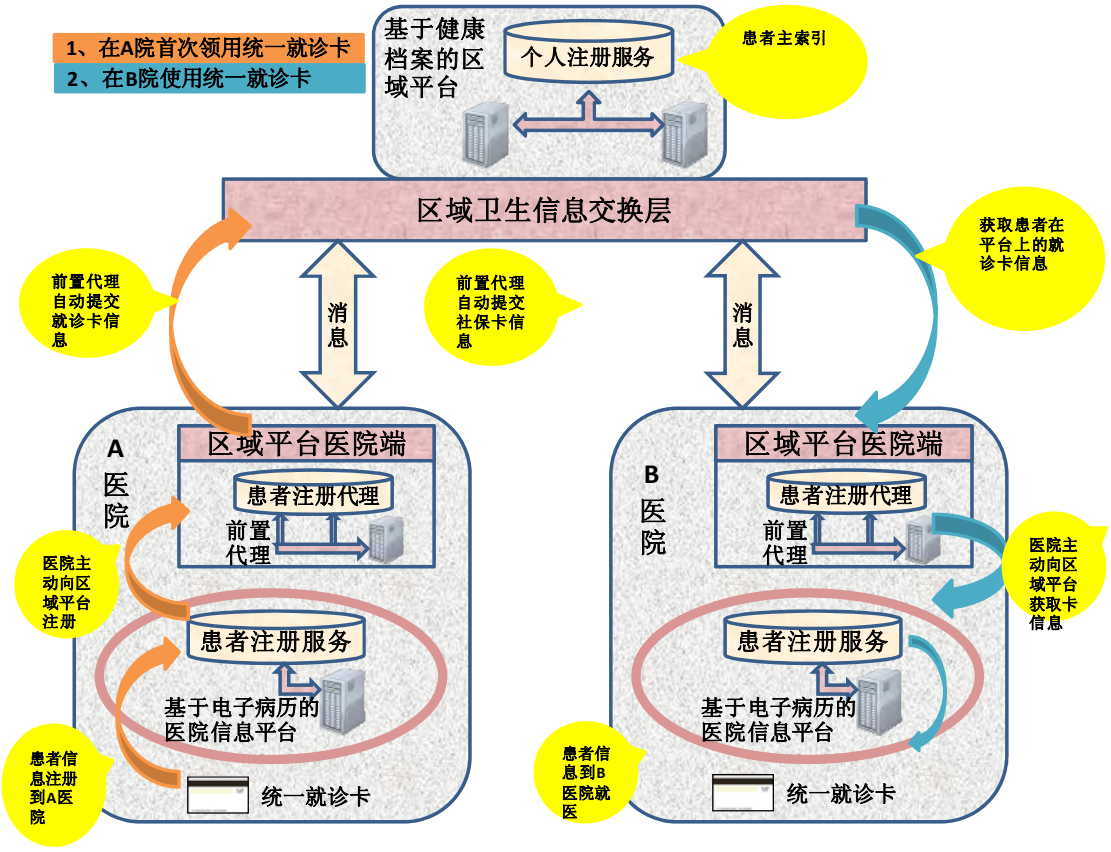


图 6-25 患者身份识别技术架构

这里以患者在 A 医院办理统一就诊卡，以及在 B 医院就医为例，说明技术架构。

患者到医院就医，办理统一就诊卡。医院在办卡的同时，通过区域卫生信息平台医院端上的患者注册代理向区域平台发起患者身份注册请求。区域平台完成患者身份及该统一就诊卡的信息注册。

患者再次持该统一就诊卡到 B 医院就诊时，医院凭就诊卡信息通过区域平台

医院端上的患者注册代理向区域平台发起患者身份查询请求。区域平台返回患者身份及该统一就诊卡的注册信息。

6.2.3.3.2 区域医疗协同

业务协同服务通过区域卫生信息平台，在两个医院信息平台之间建立一个医疗业务流程. 通过业务协同服务，可进行远程会诊、转诊转检、区域辅助医疗等。具体架构如下图所示：

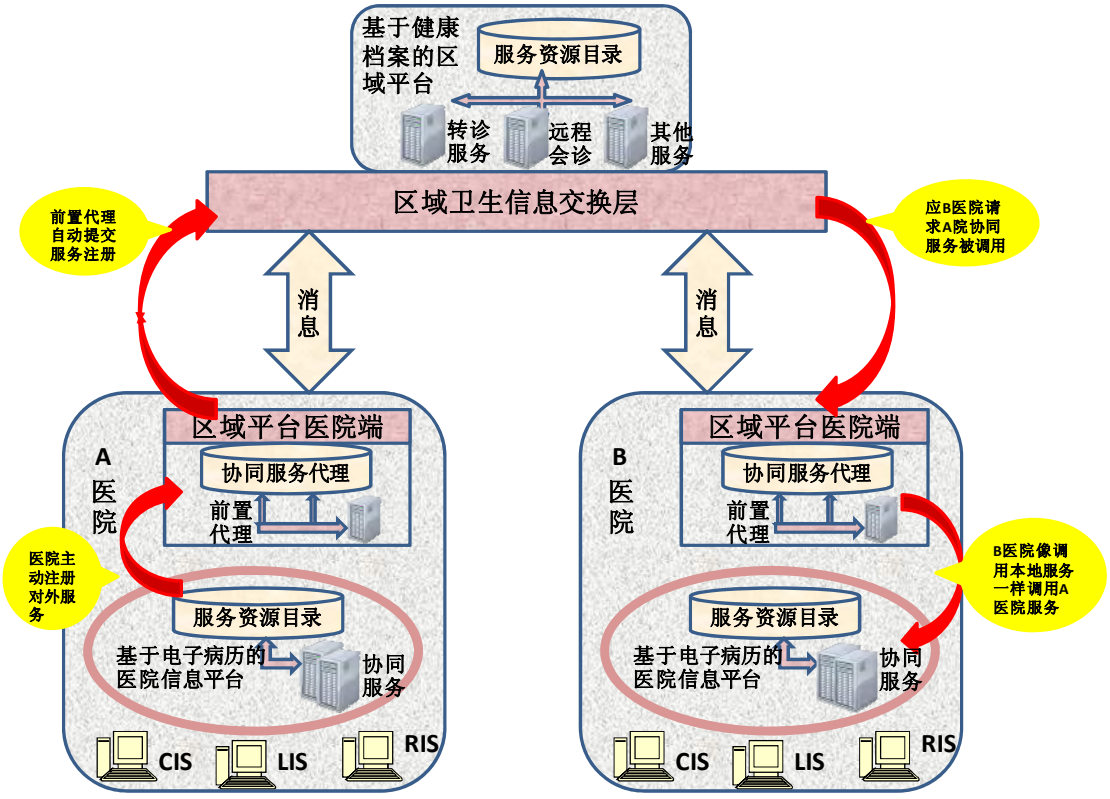


图 6-26 区域医疗协同架构

A 医院将对外提供的协同服务从本地提交到区域卫生信息平台医院端的协同服务代理上，由协同服务代理发起对区域平台上的服务注册。

当 B 医院有对 A 医院的转诊请求时，通过医院信息平台向区域平台医院端的协同服务代理发起请求，协同服务代理查找区域平台上的协同服务资源目录，并向 A 医院发起服务请求。

6.2.3.3.3 区域辅助医疗

辅助医疗服务用于支撑医院端的安全治疗警示、重复用药警示以及药物过敏警示功能，主要面向医疗终端用户，即使用医生工作站的医生。具体架构如下图所示：

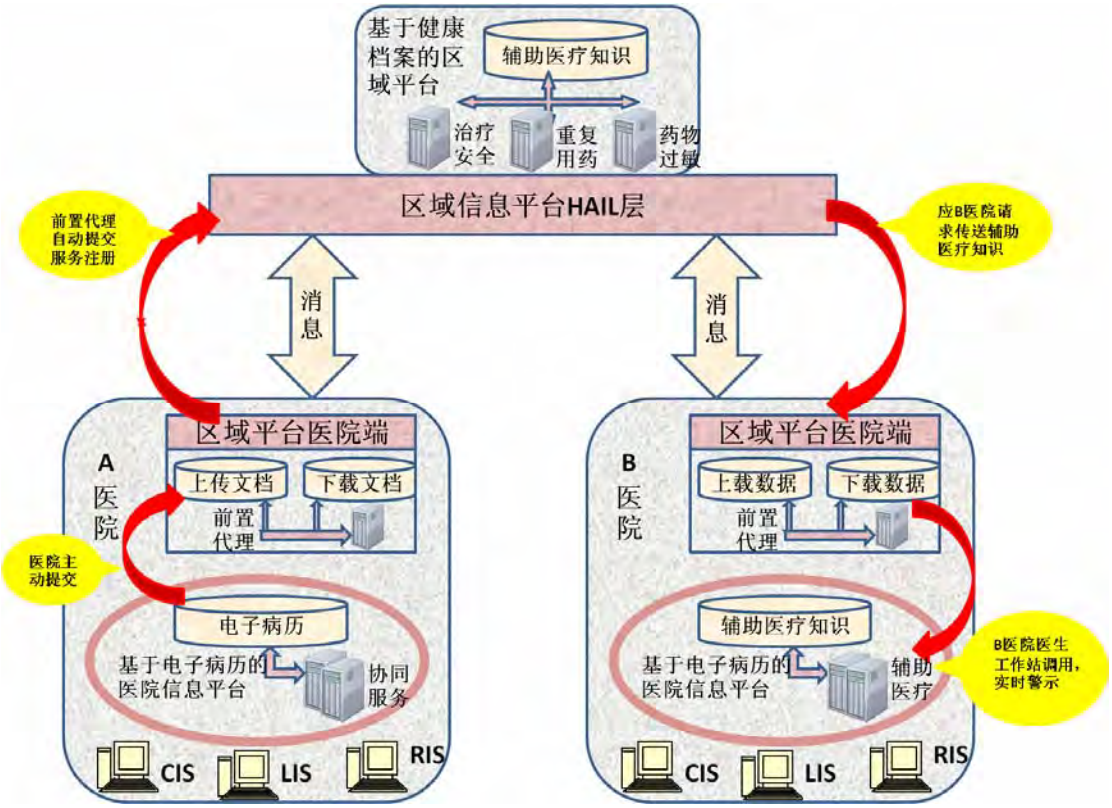


图 6-27 区域辅助医疗架构

以药物过敏服务为例，在医院端的门诊医生工作站和住院医生工作站，医生对患者开立用药医嘱，系统会将每条电子医嘱与该患者的“药物过敏代码表”（代码表从区域卫生信息平台下载）作比对，针对可能存在的用药过敏隐患，给予及时提示，医生则可根据提醒或者更改用药或者坚持原医嘱用药（由医生根据患者的具体情况综合判断决定）。

6.2.3.3.4 区域医疗公众服务系统

公众服务和业务协同服务的工作机制类似，医院将预约服务、查询服务等通过区域卫生信息平台发布给公众。具体架构如下图所示：

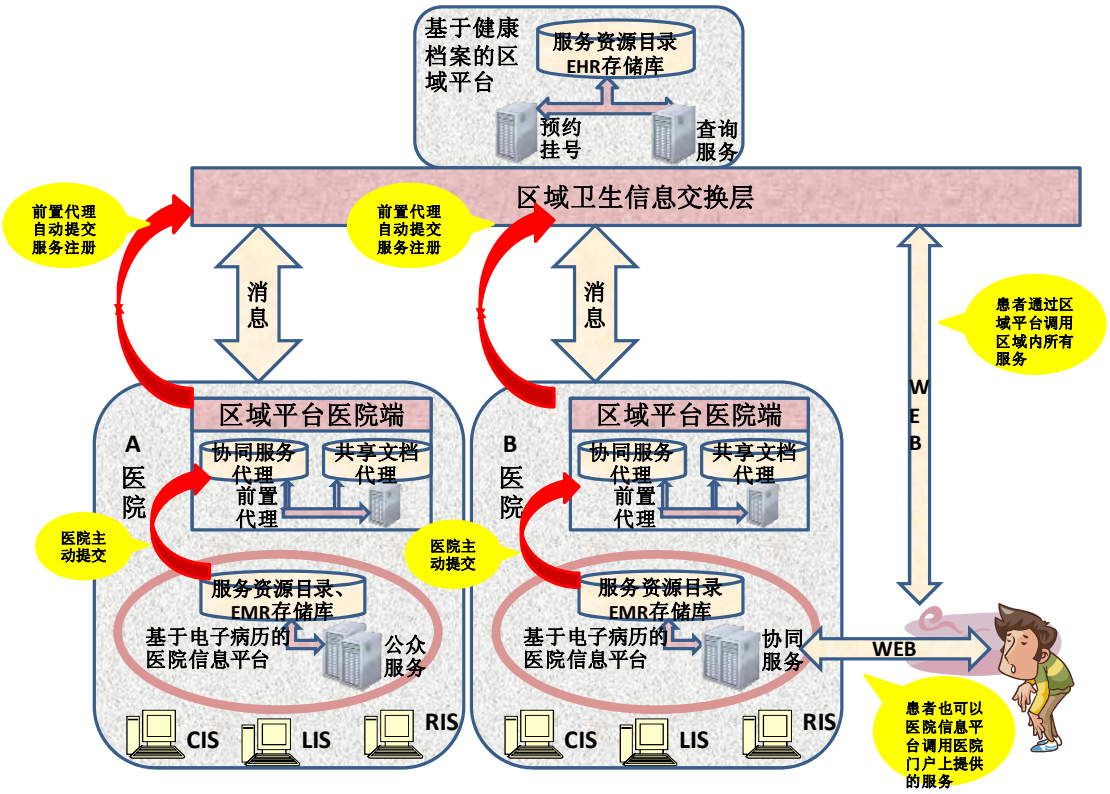


图 6-28 区域医疗公众服务架构

以预约服务为例，医院将服务发布到区域卫生信息平台，需要预约的患者可通过互联网查询，即可预约提供服务的医院专家门诊资源。患者通过填写预约就诊申请单进行专家门诊网上预约，区域平台受理患者的预约请求，将患者预约信息提交到相关医院。

另外，患者也可以直接向医院的门户提出预约，只要医院把医院信息平台上的预约服务向门户发布。

7 安全保障体系

7.1 概述

随着卫生业务对信息系统的依赖程度越来越强，信息化环境也日益恶劣，安全问题越来越突出。在这种情况下，各医疗卫生机构对信息安全保障工作给予了极大重视，卫生部于 2010 年颁布《电子病历基本规范（试行)》，其中第二章第十三条明确规定：“基于电子病历医院信息平台各业务应用应当满足国家信息安全等级保护制度与标准”,各方面的信息安全保障工作都在逐步推进。

为实现基于电子病历的医院信息平台与各类业务应用的动态整合、信息数据规范共享的目标，其安全架构设计需以等级保护为基本指导思想，从技术措施、安全管理两方面构建医院信息平台的综合信息安全保障体系，确保平台承载业务信息的安全可靠及业务服务的连续运行，并可随着未来业务及管理所需的不断发展而动态性调整，最终实现“政策合规、资源可控、数据可信、持续发展”的生存管理与安全运维目的。

7.2 安全等级

《信息系统安全等级保护管理办法》中将信息系统划分为五级，前 3 级分别为：

第一级为自主保护级，信息系统受到破坏后，会对公民、法人和其他组织的合法权益造成损害，但不损害国家安全、社会秩序和共利益。

第二级为指导保护级，信息系统受到破坏后，会对公民、法人和其他组织的合法权益产生严重损害，或者对社会秩序和公共利益造成损害，但不损害国家安全。

第三级为监督保护级，信息系统受到破坏后，会对社会秩序和公共利益造成

严重损害，或者对国家安全造成损害。

7.2.1 定级过程

GB/T22240-2008《信息系统安全等级保护定级指南》为信息系统运营使用单位确定信息系统安全保护等级的工作提供指导，基于电子病历的医院信息平台定级可依据本标准，结合基于电子病历的医院信息平台承载的业务信息情况及服务对象来进行定级细则，保证医院信息平台在不同医院单位地区等级的一致性，以指导各医院用户进行定级工作的开展。

信息系统定级既可以在新系统规划、设计时进行，也可在已建成系统中进行。对于新建系统，尽管信息系统尚未建成，但信息系统的运营使用者应首先分析该信息系统处理哪几种主要业务，预计处理的业务信息和服务安全被破坏所侵害的客体、以及根据可能的对信息系统的损害方式判断可能的客体侵害程度等基本信息，确定信息系统的安全保护等级；对于已建系统，可以通过系统基本情况调查、调查结果分析、等级确定、编制定级报告等环节完成定级工作。

基于电子病历的医院信息平台定级过程，需首先通过定级调查，了解各单位对使用医院信息平台及各业务系统的情况，了解定级对象信息系统与单位其他信息系统的关系。根据用户需求或工作需要，定级调查活动既可以针对单位整个信息系统进行，也可在用户指定的范围内进行。

- ✓ 识别单位基本信息

调查了解基于电子病历的医院信息平台负有安全责任的医院的性质、隶属关系、所属行业、业务范围、地理位置等基本情况，以及其上级主管机构的信息。了解单位基本信息有助于判断单位的职能特点，单位所在行业及单位在行业所处的地位和作用，由此判断单位主要信息系统的宏观定位。

- ✓ 识别管理框架

调查了解基于电子病历的医院信息平台所在单位的组织管理结构、管理策略、部门设置和部门在业务运行中的作用、岗位职责。了解基于电子病历的医院信息平台的管理、使用、运维的责任部门，特别是当基于电子病历的医院信息平台在各单位医院所分布于不同的物理区域的情况变化时，应了解不同区域系统运行的安全管理责任。安全管理的责任单位就是等级保护备案工作的责任单位。了解管理框架还有利于将来对整个单位制定等级保护管理框架及单个定级对象等级管理策略。

✓ 识别业务种类、流程和服务

调查了解基于电子病历的医院信息平台内部处理的业务种类，各项业务具体要完成的工作内容、服务目标和业务流程等。了解这些业务与单位职能的关联，单位对定级对象信息系统完成业务使命的期待和依赖程度，由此判断该信息系统在单位的作用和影响程度。调查还应关注每个信息系统的业务流，以及不同信息系统之间的业务关系，因为不同信息系统之间的业务关系和数据关系表明其他信息系统对该信息系统的服务的关联和依赖。应重点了解定级对象信息系统中不同业务系统提供的服务在影响履行单位职能方面具体方式和程度，影响的区域范围、用户人数、业务量的具体数据以及对本单位以外机构或个人的影响等方面。

✓ 识别信息

调查了解基于电子病历的医院信息平台所处理的信息，了解单位对信息的三个安全属性的需求，了解不同业务数据在其保密性、完整性和可用性被破坏后在单位职能、单位资金、单位信誉、人身安全等方面可能对国家、社会、本单位造成的影响，对影响程度的描述应尽可能量化。了解数据信息还应关注信息系统的数据流，以及不同信息系统之间的数据交换或共享关系。

✓ 识别网络结构和边界

调查了解基于电子病历的医院信息平台所在单位的整体网络状况和安全防护情况，包括网络覆盖范围（全国、全省或本地区），网络的构成（广域网、城

域网或局域网等），内部网段/VLAN 划分，网段/VLAN 划分与系统的关系，与上级单位、下级单位、外部用户、合作单位等的网络连接方式，与互联网的连接方式。目的是了解定级对象信息系统自身网络在单位整个网络中的位置，该信息系统所处的单位内部网络环境和外部环境特点，以及该信息系统的网络安全保护与单位内部网络环境的安全保护的关系。

✓ 识别主要的软硬件设备

调查了解与基于电子病历的医院信息平台相关的服务器、网络、终端、存储设备以及安全设备等，设备所在网段，在系统中的功能和作用。信息系统的安全保护等级仅与其重要性有关，与具体设备情况没有关系，但由于在划分信息系统时，不可避免地会涉及到设备共用问题，调查设备的位置和作用主要就是发现不同信息系统在设备使用方面的共用程度。

✓ 识别用户类型和分布

调查了解基于电子病历的医院信息平台管理用户和一般用户、内部用户和外部用户、本地用户和远程用户等类型，了解用户或用户群的数量分布、各类用户可访问的数据信息类型和操作权限。了解用户类型和数量，有助于判断系统服务中断或系统信息被破坏可能影响的范围和程度。

✓ 等级分析并形成定级结果

定级人员需要将基于电子病历的医院信息平台中的不同类型重要信息分别分析其安全性受到破坏后所侵害的客体及对客体的侵害程度，取其中最高结果作为业务信息安全保护等级。再将定级对象信息系统中不同类型重要系统服务分别分析其受到破坏后所侵害的客体及对客体的侵害程度，取其中最高结果作为业务服务安全保护等级。最终安全保护等级由业务信息安全等级和系统服务安全等级较高者决定。

按照“谁主管，谁负责”的原则，现将审批流程说明如下：信息系统各运营

使用医院按照本方案确定信息系统安全保护等级后，填写备案表，按要求到公安机关办理备案手续。

7.2.2 等级变更

在信息系统的运行过程中，信息系统安全保护等级应随着信息系统所处理的信息和业务状态的变化进行适当的变更，尤其是状态变化可能导致业务信息安全或系统服务受到破坏后的受侵害客体和对客体的侵害程度有较大的变化，可能影响到系统的安全保护等级时，应重新定级。重新定级后，应按要求向公安机关重新备案。

7.2.3 医院信息平台安全等级建议

基于电子病历的医院信息平台所涉及信息包括：病人的个人信息、诊疗数据、电子病历、住院信息等。这些业务信息遭到破坏或失窃，所侵害的客体是公民、法人和其他组织的合法权益。一旦业务信息遭到非法入侵、修改、增加、删除等不明侵害（形式可以包括丢失、破坏、损坏等），会对公民、法人和其他组织的合法权益造成影响和损害，可以表现为：影响正常工作的开展，导致业务能力下降，造成不良影响，引起法律纠纷等。程度表现为严重损害，即工作职能收到严重影响，业务能力显著下降，出现较严重的法律问题，较大范围的不良影响等。根据以上描述可以确定基于电子病历的医院信息平台承载的业务信息数据安全保护等级不低于第二级。

表 7-1 业务信息数据安全保护等级定级

业务信息安全被破坏时所侵害的客体	对相应客体的侵害程度		
	一般损害	严重损害	特别严重损害
公民、法人和其他组织的合法权益	第一级	第二级	第二级
社会秩序、公共利益	第二级	第三级	第四级
国家安全	第三级	第四级	第五级

基于电子病历的医院信息平台属于为国计民生提供服务的信息系统，其服务范围为区域范围内的普通公民、医院等。该业务系统遭到破坏后，所侵害的客体是公民、法人和其他组织的合法权益，同时也侵害社会秩序和公共利益。客观方面表现得侵害结果为：1 影响正常工作的开展，导致业务能力下降，造成不良影响，引起法律纠纷等，从而对公民、法人和其他组织的合法权益造成侵害；2 造成社会不良影响，为公众服务的医疗卫生机构的业务受到影响，从而对社会秩序公共利益造成严重侵害。根据《信息系统安全等级保护定级指南》的要求，出现上述两个侵害客体时，优先考虑社会秩序和公共利益，另外一个不做考虑。上述定级分析的结果程度表现为：对社会秩序和公共利益造成一般损害，因此该平台提供业务服务安全保护等级为不低于“第二级”。

表 7-2 系统服务安全等级定级

系统服务被破坏时所侵害的客体	对相应客体的侵害程度		
	一般损害	严重损害	特别严重损害
公民、法人和其他组织的合法权益	第一级	第二级	第三级
社会秩序、公共利益	第二级	第三级	第四级
国家安全	第三级	第四级	第五级

综上，可知基于电子病历的医院信息平台整体的安全保护等级为不低于二级，系统服务等级为不低于二级。

表 7-3 整体安全保护等级定级

信息系统名称	业务信息安全等级	系统服务安全等级
基于电子病历的医院信息平台	不低于第二级	不低于第二级

依据《信息系统安全等级保护定级指南》规定：信息系统的安全保护等级由“业务信息安全等级”和“系统服务安全等级”的较高者决定。结合上述对基于电子病历的医院信息平台的分析，得到其安全保护等级整体上不低于第二级。

表 7-4 安全保护等级定级结论

信息系统名称	安全保护等级
基于电子病历的医院信息平台	不低于第二级

根据上述建议保护等级，基于电子病历的信息平台需按照信息系统等级保护二级（或以上）的要求进行安全建设，建设完毕后电子病历的信息平台可具有抵御自然灾害及恶意攻击的能力，可全面防范计算机病毒和恶意代码危害并对攻击行为予以检测，对安全事件可进行记录审计，在平台的信息或业务应用遭到损害后，可具备恢复系统正常运行状态的能力。

经过总体考虑某些医院的信息系统内部承载了重要人物的电子病历或基本信息，其遭受破坏后，对社会秩序和公共利益造成严重损害，即会出现较大范围的社会不良影响和较大程度的公共利益的损害等，对于此情况，医院需按照本院的特殊要求，自主定级并上报公安系统，如经过论证后确认平台上承载的信息数据敏感程度较高，可参照涉密信息系统安全保护相关要求，向国家保密部门报批后予以建设，对于这些个体情况，本章节不进行单独说明。

7.3 风险分析

风险分析是实现基于电子病历医院信息平台安全建设的必要步骤，为各医院在针对此平台的建设过程中提供充分的参考依据。

7.3.1 信息和信息系统分析

信息和信息系统构成了医院信息平台的信息资产。基于电子病历的医院信息平台的使用对象主要是医院工作人员，最终服务对象是病患。医疗人员为了更好的为患者提供可靠的、连续的医疗卫生服务，需要依赖平台提供的众多服务。

医院信息平台中的业务数据的类型主要包括文档数据、操作型数据、辅助决策型数据。文档数据是以文档形式存在于平台中的临床和电子病历等业务数据，例如检验报告、处方等，这些数据是结果数据。操作型数据一般是指平台从业务

系统中采集、汇总、供实时业务查询和统计使用的数据。辅助决策数据是指存储在数据仓库中，以主题方式组织，是经过二次加工的历史数据。这些信息是需要安全保护的重点对象，其可用性、机密性和完整性均需要进行一定程度的保障。

从逻辑上，基于电子病历的医院信息平台的核心业务模式为集中式，整个平台建设主要以信息平台数据中心为核心。医院信息平台网络基础设施平台由内、外两大网络部分组成。外部网络对外收集和提供信息(比如向外部网络进行医学资料信息查询等)，内部网实现信息管理和系统开发。详细的网络设计参见“网络与通信基础架构”章节。

7.3.2 安全风险分析

安全风险是指由于系统内存在的脆弱性、人或自然的威胁导致安全事件发生的可能性及其造成的影响。安全风险的大小主要取决于以下四个方面：资产的价值、资产的脆弱性、面临的威胁程度，以及已经采取的防范措施。

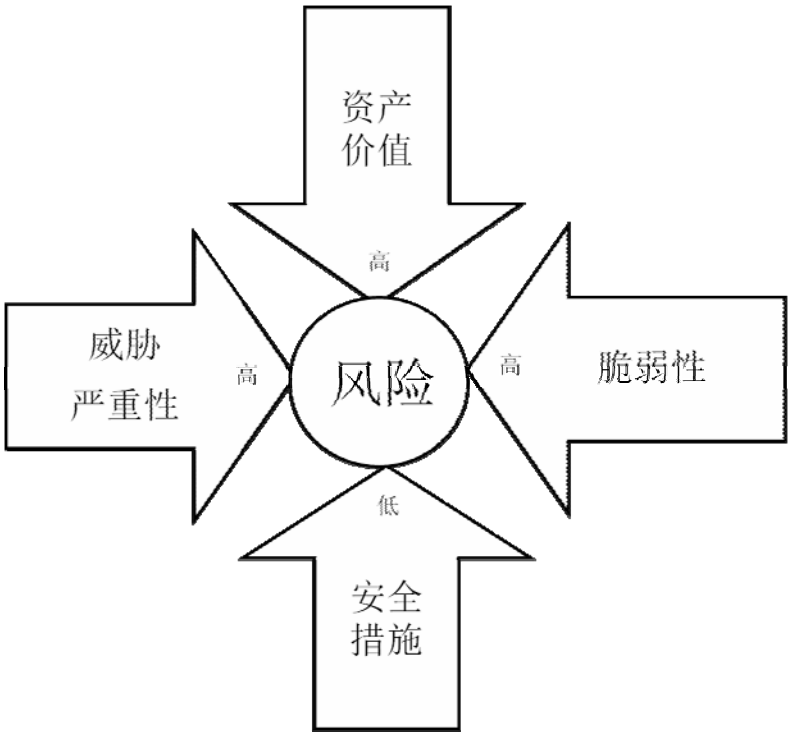


图 7-1　安全风险要素分析

参照上图，当一个系统具有了信息化的核心资产（服务器上保存的重要数据保，比如患者信息），这些资产存在弱点和漏洞（比如承载这些信息的数据库具有 SQL 注入漏洞），又同时存在被安全威胁攻击的可能（比如黑客已经开发出了针对这种漏洞的蠕虫和攻击方法等），而且系统没有部署相应的防御手段（比如网络或主机入侵防御系统等），那么就会导致安全风险，从而给系统造成损失。

因此，医院信息平台的安全风险和这四个方面紧密相关，在实际建设过程中，各医院可根据电子病历医院信息平台的承载的信息、依托的资产及服务范围等实际情况，参照 GB/T20984-2007《信息安全技术 信息安全风险评估规范》展开风险分析工作，以有效解决上述解决要素之间的关系，保证平台的整体安全。

7.3.3 资产分析

在医院信息平台网络中，数据库服务器、应用集成平台服务器和内部应用系统等承载了关键的数据信息，需要进行重点的防护，避免非授权访问和攻击等安全事故发生。

7.3.4 威胁分析

威胁是指可能对信息系统资产或所在组织造成损害事故的潜在原因；威胁虽然有各种各样的存在形式，但其结果是一致的，都将导致对信息或资源的破坏，影响信息系统的正常运行，破坏信息系统服务的有效性、可靠性和权威性。

基于电子病历的医院信息平台面临的主要威胁如下：

✓ 自然灾害

自然灾害包括：地震、水灾、火灾、风灾等。它们可以对网络系统造成毁灭性的破坏，其特点是：发生概率小，但后果严重。一旦发生这些自然灾难将对 RHIN 平台内网中的系统所依附的基础设施造成严重威胁。

✓ 身份假冒、口令窃取威胁

身份鉴别是网络安全的基本要求，而医院信息系统的登录方式大多采用“用户名+口令”方式，存在身份假冒威胁等，一旦医护人员的身份被窃取，将直接影响到患者信息、电子病历等的安全性和隐秘性。

✓ 数据泄露和破坏威胁

医院信息平台中存在大量隐私信息，而这些数据在传输过程中极易被窃取或监听。一旦数据丢失或被篡改，将造成很大的影响。另一方面，随着便携式数据处理和存储设备的广泛应用，由于设备丢失而导致的数据泄漏威胁也越来越严重。

✓ 计算机病毒威胁

病毒是系统最常见、威胁最大的安全隐患，主要表现为利用系统软件或应用软件中的程序错误或安全漏洞来获得对计算机系统的非法访问和攻击。医院信息系统中，一旦将病毒或木马引入其中，而网内的现有杀毒系统代码更新不及时，将可能造成严重的系统瘫痪及资源的泄漏。

✓ 系统漏洞威胁攻击

医院信息平台的网络系统中很有可能存在着可被攻击者利用的安全弱点、漏洞以及不安全配置等，主要表现在操作系统、网络服务、TCP/IP 协议、应用程序（如数据库、浏览器等）、网络设备等几个方面，正是这些弱点给蓄意或无意的攻击者以可乘之机，一旦系统的漏洞利用成果，势必影响到系统的稳定、可靠运行，更严重的导致系统瘫痪和数据丢失，从而影响医院的公众形象。

✓ 通讯业务流传输侦听威胁

医院信息平台作为医院内部跨系统的数据交互平台，网络中存在大量的信息交互，非法人员可以通过对信息流向、流量、通信频度和长度等参数的分析，获

取平台内部的隐私信息。

✓ 电力中断

电力中断会破坏计算机信息系统的可用性或者导致数据丢失。应采用不间断电源（UPS）系统的部署运用，减少因电力构成的威胁。

因此，只有同时解决好上述问题，才可能真正的确保医院信息平台的安全。

7.4 需求分析

7.4.1 安全需求

《信息安全等级保护管理办法》（公通字〔2007〕43号）、《关于开展全国重要信息系统安全等级保护定级工作的通知》（公信安〔2007〕861号）、《信息安全技术信息系统等级保护安全设计技术要求》（GB/T 25070-2010）等文件等级保护标准规范提出了安全信息系统应当包括安全应用支撑平台和应用软件系统两个组成部分，在应用支撑平台方面提出了应当按照计算环境、区域边界、通信网络三个环节进行分等级的安全防护建设，同时在此基础上还需要建设集中的安全管理中心，对部署在计算环境、区域边界、通信网络上的安全策略与安全机制实现集中管理。

其中，安全计算环境主要针对主机安全性保障提出，对于医院信息平台，应实现二级增强的计算环境所要求的身份鉴别、访问控制、安全审计以及数据保密性和完整性等内容，此外，应根据实际情况，建立数据的备份及存储恢复措施，如条件具备，可构建集中的数据和系统灾备中心，保证在发生安全事件时能够尽快恢复数据、系统，快速恢复业务等；

安全区域边界针对隔离与访问控制而提出，对于医院信息平台，应实现二级增强的区域边界所要求的防火墙隔离、安全审计、入侵防护以及恶意代码监测与过滤等内容；

安全通信网络则针对网络及通讯的安全保障而提出，对于医院信息平台，应当实现二级增强的安全通信网络所要求的通信机密性、完整性保护、网络设备安全性保护、网络设备冗余等内容；

安全管理中心则关注上述三个层面所采取的安全措施的集中管理，包括系统管理、安全管理等相关内容。

其次，物理安全方面，要根据实际情况建立相应的安全防护机制；需要加强计算机房的安全建设，机房必须具备防水、防潮、抗震、防雷击、防盗窃、防静电、防电磁辐射的措施。

安全管理方面，要考虑政策、法规、制度、安全培训等，制定切实有效的管理制度和运行维护机制。

7.4.2 隐私保护需求

电子病历是由一系列关于个人健康资料的数字化档案库构成，如病人的身份确认、病历记载、实验室检验、影像诊断报告、处置、治疗、用药等信息。加强对电子病历的隐私保护是基于电子病历的医院信息平台重点关注的问题，《电子病历基本规范（试行）》要求：“对操作人员的权限试行分级管理，保护患者隐私”。

患者隐私保护应对医务人员进行身份审查，根据病种、角色等多维度授权对于用户登录，当医务人员因工作需要查看或访问非直接相关患者的电子病历资料时患者电子病历时，应警示使用者依照规定使用患者电子病历资料，系统应自动生成、保存使用日志，对电子病历数据的创建、修改、删除等任何操作都将自动生成、保存审计日志，用于日后的审计。

同时，应加强对关键个人病历信息（字段级、记录级、文件级）进行加密存储保护。从而使患者的隐私得到更好的保护。

7.5 总体设计

基于电子病历的医院信息平台安全架构设计参照信息系统等级保护技术设

计要求，以安全需求为驱动，结合平台所承载的业务信息数据及系统服务情况，在计算环境、区域边界、通信网络、安全管理方面构建结构化信息安全体系架构，安全措施彼此间存在互补、增强，并与物理安全防护措施结合，整体上形成一个策略、组织、技术和运维结合的信息安全保障体系，保证平台信息的安全及业务的连续，并适应随着未来业务应用和管理需求的不断发展而动态性调整，最终达到“整体合规、资源可控、数据可信、持续发展”的生存管理与安全运维目的。

7.5.1 设计思想

医院信息平台安全方案设计过程中，需进行详细的需求分析，并充分利用现有资源，在可用性、经济性基础上进行。主要分为两大部分：包括安全技术体系和安全管理体系，两者以安全策略为指导，既有机结合，又相互支撑。

✓ 构建纵深的防御体系

医院信息平台安全保障体系建设方案包括技术和管理两个部分，本方案针对医院信息平台的通信网络、区域边界、计算环境、业务应用平台等各个层面，采用访问控制、统一监管、集中审计、防病毒、集中身份认证、应用加密、集中数据备份等多种技术和措施，实现医院信息平台业务应用的可用性、完整性和保密性保护，同时充分考虑各种技术的组合以及功能的互补性，合理利用措施，从外到内形成一个纵深的安全防御体系，保障信息系统整体的安全保护能力。

✓ 保证一致的安全强度

医院信息平台的安全保证体系建设应采用分级分层的方法，采取强度一致的安全措施，并采取统一的防护策略，使各安全措施在作用和功能上相互补充，形成动态的防护体系。因此，在建设手段上，本方案在平台上实现二级信息系统的基本防护，比如统一的防病毒系统、统一认证平台和统一的审计系统，然后在基本保护的基础上，再根据各个计算环境的重要程度，采取进一步的高强度的保护措施。

✓ 建立统一的支撑平台

建设全网统一的认证平台，实现高强度的应用安全保护，统一支持平台能够实现：统一的认证入口及单点登录，即终端系统一次认证并可按照自己的权限访问相关资源；统一的权限分配，实现资源、角色、权限的统一分配；统一的资源管理，统一认证平台使系统管理人员更清晰的分析并管理资源的分配情况，完成安全策略的配置和部署。

✓ 进行集中的安全管理

信息安全管理的目标就是通过采取适当的控制措施来保障信息的保密性、完整性、可用性，从而确保信息系统内不发生安全事故，即使发生也能有效控制事故风险。通过建设集中的安全管理平台，实现对信息资产、安全事件、安全风险、访问行为等的统一分析与监管，通过关联分析技术，使系统管理人员能够迅速发现问题、定位问题，有效应对安全事件的发生。

7.5.2 设计依据

(1) 国家相关文件

✓ 中办发 17 号文件《国家信息化领导小组关于我国电子政务建设指导意见》

✓ 中办[2003]27 号文件《国家信息化领导小组关于加强信息安全保障工作的意见》

✓ 四部委于 2004 年 9 月 15 日发布公通字[2004]66 号《信息安全等级保护工作的实施意见》（公通字[2004]66 号）

✓ 四部委 2007 年 06 月 17 日发布（2007）公通字 43 号《 信息安全等级保护管理办法》

✓ 公信安 2009 年 10 月 27 日《关于开展信息安全等级保护安全建设整改工作的指导意见》

- ✓ 关于开展全国重要信息系统安全等级保护定级工作的通知（公信安[2007]861 号）
- ✓ 信息安全等级保护备案实施细则（公信安[2007]1360 号）
- ✓ 关于开展信息安全等级保护安全建设整改工作的指导意见(公信安[2009]1429 号)
- ✓ ……

(2) 国家相关标准

- ✓ GB 17859-1999 计算机信息系统安全保护等级划分准则
- ✓ GB/T 22239-2008 信息安全技术 信息系统安全等级保护基本要求
- ✓ GB/T 25070-2010 信息安全技术信息系统等级保护安全设计技术要求
- ✓ GB/T XXXXX-XXXX 信息安全技术信息系统安全等级保护实施指南
- ✓ GB/T 22240-2008 信息安全技术信息系统安全等级保护定级指南
- ✓ GB/T20271-2006 信息安全技术 信息系统通用安全技术要求
- ✓ GB/T20270-2006 信息安全技术 网络基础安全技术要求
- ✓ GB/T20272-2006 信息安全技术 操作系统安全技术要求
- ✓ GB/T20273-2006 信息安全技术 数据库管理系统安全技术要求
- ✓ GB/T20282-2006 信息安全技术 信息系统安全工程管理要求
- ✓ GB/T21082-2007 信息安全技术 服务器安全技术要求
- ✓ GB/T 20988-2007《信息系统灾难恢复规范》
- ✓ ……

7.5.3 总体框架

基于电子病历的医院信息平台安全体系框架在国家政策、法律法规要求的指引的前提下，以安全基础设施为依托，与平台的业务流程、应用架构和数据资源紧密结合，从安全技术、安全管理为要素进行框架设计说明。

基于电子病历的医院信息平台安全体系框架如下图所示：

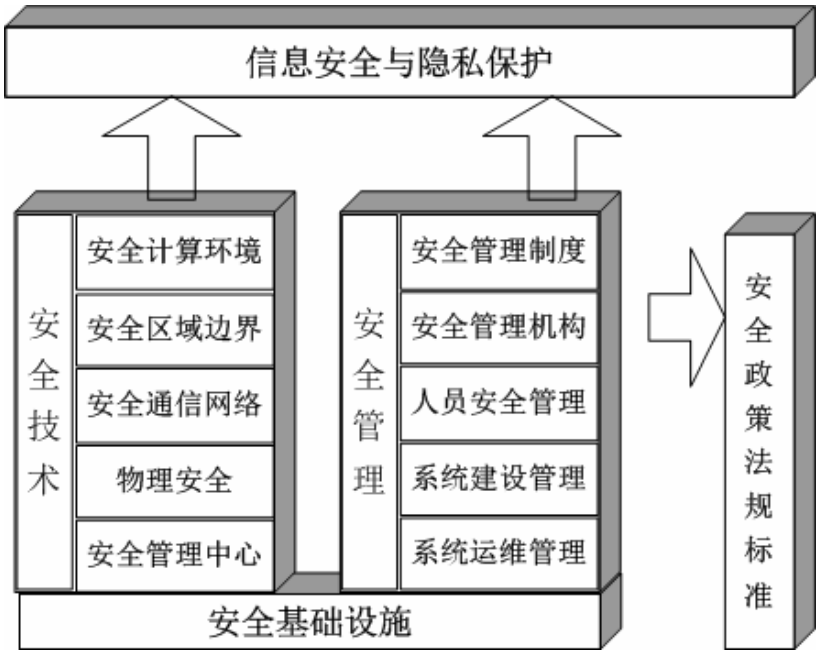


图 7-2　安全体系总体框架

基于电子病历的医院信息平台安全体系总体框架包括：安全技术、安全管理、安全基础设施三部分：

■　安全技术

✓　安全计算环境：安全计算环境解决基于电子病历的医院信息平台的计算机系统硬件和系统软件以及外部设备及其连接部件的系统安全，包括用户身份真实有效、资源的访问控制、主机安全审计、重要数据的完整和可用性及数据的存储与备份恢复方面的安全。

✓　安全区域边界：安全区域边界首先确立基于电子病历的医院信息平台的边界，并确定医院信息平台所在的安全计算环境与安全通信网络之间部件的安

全，包括网络结构、边界的访问控制、协议过滤、安全审计、恶意代码防护及边界的入侵监控等。

✓ 安全通信网络：安全通信网络解决基于电子病历的医院信息平台所在的安全计算环境用于信息传输实施安全保护的部件的安全，包括数据传输的完整性和保密性、网络可信接入、抗抵赖等。

✓ 物理安全：物理安全是基于电子病历的医院信息平台所依附的设备、设施以及其他媒体免遭地震、水灾、火灾等环境事故以及人为操作失误或错误及各种计算机犯罪行为导致的破坏过程。

✓ 安全管理中心：安全管理中心是实现围绕基于电子病历的医院信息平台所制定的安全策略及所依托的安全计算环境、安全区域边界和安全通信网络上的安全机制得到统一管理，强制其策略下发及实现的过程管理等。

■ 安全管理

安全管理建设需以基于电子病历的医院信息平台所服务对象为基础，来建立完善的安全管理体系，即建立相应的信息安全管理机构、制定相应的信息安全管理制度、设置平台运行所需的人员、岗位，建立对系统在运行开发过程中的制度，同时通过日常巡检、咨询、评估等运行管理来发现安全隐患并予以改进与提升。

■ 安全基础设施

安全基础设施主要为基于电子病历的医院信息平台安全运行所需的防护部件，通过安全基础设施的安全互联、接入控制与边界防护、区域安全、通信安全、数据传输安全和安全管理等，为形成一体化的安全防护体系奠定基础。

7.5.4 隐私保护说明

隐私保护及信息安全是医院信息平台所要重点解决的问题，应从患者同意，匿名化服务，依据病种、角色等多维度授权，关键信息（字段级、记录级、文件级）加密存储等方面展开。电子病历等医疗数据进行调阅时，包括强身份认证需求、角色授权需求、责任认定需求、电子签名及时间戳等方面的需求。同时，应用系统应通过交互数据加密、集中授权、应用审计等功能来确保患者的隐私安全。

各医院根据要求不同，采用相应的适宜技术保护隐私，按照《电子病历基本规范（试行）》以及相关法规，可以采取的技术手段包括如下几方面，：

✓ 身份保护和鉴别服务

医院信息系统应当为患者建立个人信息数据库（包括姓名、性别、出生日期、民族、婚姻状况、职业、工作单位、住址、有效身份证件号码、社会保障号码或医疗保险号码、联系电话等），授予唯一标示号码并确保与患者的医疗相应记录。

医院信息系统应当为操作人员提供专有的身份标识和识别手段，并设置相应权限；操作人员对本人身份标识的使用负责。

✓ 身份管理服务

为更高层次服务提供基础服务，例如用户注册、认证、授权，其中包括用户的唯一标识、查找用户的标识、挂起/取消用户访问权。

✓ 访问控制服务

对操作人员的权限实行分级管理，保护患者的隐私。医院信息系统应当设置医务人员审查、修改的权限和时限、实习医务人员、试用期医务人员记录的病历等医疗数据，应当经过在本医疗机构合法执业的医务人员审阅、修改并予电子签名确认。医务人员修改时，医院信息系统应当进行身份识别、保存历次修改痕迹、标记准确的修改时间和修改人员信息。

✓ 加密服务

加密服务包括密钥管理、数据库加密以及数据存储加密三方面内容。其中，密钥管理是指创建和管理数据存储的加密密钥；数据库加密指加解密数据库表中的数据字段（列）和记录（行）以保护电子病历以及医院信息平台中处于试用状态的其它保密的关键系统数据；数据存储加密指加解密文件和其它数据块，用于保护在联机存储、备份或长期归档中的数据，从而实现关键信息（字段级、记录

级、文件级）加密存储。

✓ 数字签名服务

医务人员采用身份标识登录电子病历等业务系统完成各项记录等操作并予确认后，系统应当进行电子签名。数字签名由用户创建，以确保临床数据的不可否认性，包括数据文件、诊疗报告、记录中的字段域、安全声明、XML文档以及被转换为XML文档的HL7消息或对象中的元素。

✓ 匿名化服务

包括患者的隐私和安全，确保在信息平台中以及提供正常医疗服务以外的（例如医疗保险等）传递中使用的资料不向非授权用户透露患者的身份。

✓ 应用审计服务

该服务提供对每个事务所涉及到的系统、用户、医护工作者、患者/居民、医疗数据等等的报告功能。这些服务对于满足其他业务需求，如系统管理、事务监控、记录重要的与隐私和安全有关的事件等，也是至关重要的。

✓ 许可指令管理服务

许可指令管理服务转换由立法、政策和个人特定许可指令带来的隐私要求，并将这些需求应用到医院信息平台环境中。在提供访问或传输患者电子病历等医疗数据之前，该服务应用于电子病历以确定患者或个人的许可指令是否允许或限制这些医疗数据的公开。

7.6 安全技术保障

7.6.1 确定保护对象

根据对基于电子病历的医院信息平台自身业务信息特点、服务对象、安全防

护目标等不同确定保护对象，以实现医院信息平台安全防护策略、技术措施及管理手段的得到有效实施，保护对象确定平台的计算环境确定、区域边界的确定、通信网络的确定几部分。

7.6.1.1 确定计算环境

根据医院信息平台的信息处理流程和功能的不同，对平台划分为七个计算环境，如下图所示：

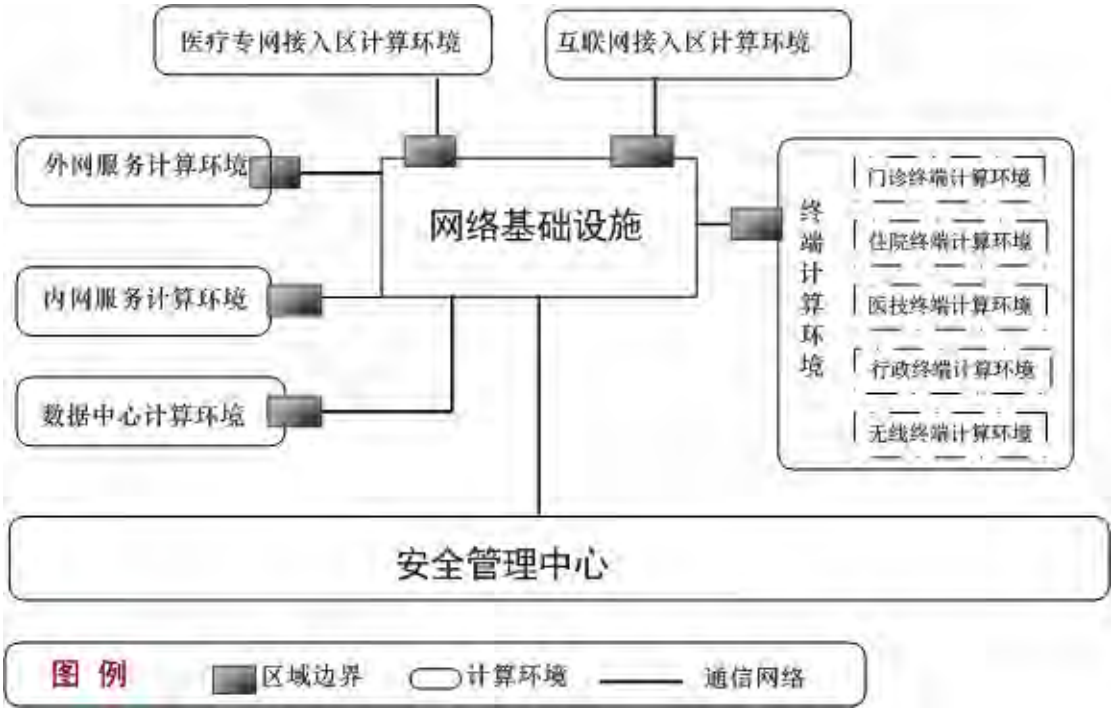


图 7-3　保护对象示意图

如上图所示，各计算环境描述如下：

- ✓ 互联网接入区计算环境：包括互联网出口处网络设备等基础设施，完成医院内网与互联网的隔离。

- ✓ 医疗专网接入区计算环境：实现医院医疗数据向区域卫生信息平台的上传共享等，可实现与区卫平台、疾控中心以及医保等的网络互连。

- ✓ 外网服务计算环境：包含了为外部提供服务的服务器，包括对外的 WEB 服务等。

- ✓ 内网服务计算环境：包括 HIS、LIS、EMR 等医院业务系统。

- ✓ 数据中心计算环境：包括数据库服务器群以及数据备份等设备。

- ✓ 终端计算环境：分为门诊终端计算环境、住院终端计算环境、医技终端计算环境、行政终端计算环境以及无线终端计算环境五个子计算环境。

- ✓ 安全管理中心：实现对整个医院信息系统的集中网络管理以及安全管理等。

7.6.1.2 确定区域边界

根据前面信息系统描述，对医院信息平台进行安全计算环境划分，主要分为外部边界和内部边界两种区域边界，其中需要保护的外部边界包括：

- ✓ 互联网接入域边界：该边界隔离了医院内部网络与外部互联网。

- ✓ 专网接入区边界：实现与区卫平台、疾控中心等外部信息系统的数据交换及通信。

医院内部边界主要包括：

- ✓ 外网服务区域边界：隔离了终端用户及外网服务区，以及服务区及数据中心，通过该边界来进行数据传输及调用。

- ✓ 内网应用区域边界：重点隔离了终端区域与内部应用区域，医护人员工作站等终端进行后台业务时，将通过此边界实现对应用软件的访问；

- ✓ 终端用户域边界：隔离了终端用户区域与内部业务服务区域，终端通过此边界完成对应用软件等的访问。

✓ 数据中心区边界：隔离了数据中心与内、外服务区域。

7.6.1.3 确定通信网络

根据信息系统描述，医院信息平台的通信网络中保护对象包括：

✓ 互联网接入设施：路由器

✓ 外网接入设施：路由器

✓ 安全设备：防火墙等

✓ 交换设备：交换机

7.6.2 计算环境安全

基于电子病历的医院信息平台计算环境安全包括用户身份鉴别、访问控制、系统安全按审计、数据保密性与完整性、数据备份与恢复、恶意代码防护等。

围绕医院信息平台安全配置是确保计算环境中主机系统具备的安全功能在业务环境中充分、有效对抗威胁的保证，其主要配置内容应包括主机身份鉴别（鉴别方式、强度、失败处理）、访问控制（控制范围、严格程度以及实现方式）、业务安全应用（软件开发架构体系、访问控制模型、授权管理模型、安全机制选择与实现方式、编码安全规范与代码审核）、安全审计（实现方式、对象和项目的选择、日志存储与保护、数据查询与报警）、数据备份与恢复（业务影响分析、备份范围、时间间隔、设备冗余、远程集群支持、应急预案设计与演练等）等。

具体标准可依据《信息系统安全等级保护基本要求》《信息系统等级保护安全设计技术要求》，同时可以参照《信息系统通用安全技术要求》、《网络基础安全技术要求》、《信息系统灾难恢复规范》等。

7.6.2.1 用户身份鉴别

身份鉴别机制是其它安全机制的基础措施，只有实现了有效的用户身份鉴

别，才能保证访问控制、安全审计、入侵防范等安全机制和措施发生效用。身份鉴别可分为主机身份鉴别和应用身份鉴别两方面。

(1) 主机身份鉴别

为提高主机系统安全性，保障各种应用的正常运行，对主机系统需要进行一系列的加固措施，相应的安全策略包括：

- ✓ 在登录操作系统和数据库系统时，可采用数字证书等进行身份鉴别，从而实现比用户名/口令更为严格的双因子认证。
- ✓ 配置用户名/口令时，检验口令复杂度，不合格的口令被拒绝，其次，设置定期更换要求；
- ✓ 启用登陆失败处理功能，登陆失败后采取结束会话、限制非法登录次数和自动退出等措施。
- ✓ 远程管理时应启用 SSH 等管理方式，加密管理数据，防止被网络窃听。

(2) 应用身份鉴别

为提高应用系统系统安全性应用系统需要进行一系列的加固措施，利用 PKI/CA 技术，为基于电子病历的医院信息平台提供全面的数字证书服务，实现统一的用户信息管理以及强身份认证管理。基于 CA 认证体系，建立医院信息平台应用安全支撑平台，并与信息平台应用系统结合实现安全身份鉴别，相应的安全策略包括：

- ✓ 对登录用户进行身份标识和鉴别，且保证用户名的唯一性。
- ✓ 根据基本要求配置用户名/口令，必须具备一定的复杂度；口令必须具备采用 3 种以上字符、长度不少于 8 位并定期更换；
- ✓ 启用登陆失败处理功能，登陆失败后采取结束会话、限制非法登录次数

和自动退出等措施。

- ✓ 应用系统如具备上述功能则需要开启使用，若不具备则需进行相应的功能开发，且使用效果要达到以上要求。

7.6.2.2 访问控制

二级系统的重点要求是实现自主访问控制。应在安全策略控制范围内，使用户对自己创建的客体具有各种访问操作权限，并能将这些权限的部分或全部授予其他用户；自主访问控制主体的粒度应为用户级，客体的粒度应为文件或数据库表级；自主访问操作应包括对客体的创建、读、写、修改和删除等。由此主要控制的是对应用系统的文件、数据库等资源的访问，避免越权非法使用。平台的安全技术实现上，采用主流的 PKI（Public Key Infrastructure，公钥基础设施）技术，通过数字证书来实现高安全性的用户统一管理，并实现可靠的权限管理及安全的单点登录；授权管理技术实现上，采用基于角色访问控制模型，以及访问控制列表（ACL）的授权管理方式。

通过 CA（Certificate Authority）认证技术与应用系统结合，形成“用户—角色—权限”三者之间的对应关系，从而可以对用户实行严格的访问控制，实现基于角色的集中授权管理，以确保应用系统不被非法或越权访问，防止信息泄漏。基于统一身份认证及统一授权管理的用户访问控制总体框架如下图所示：

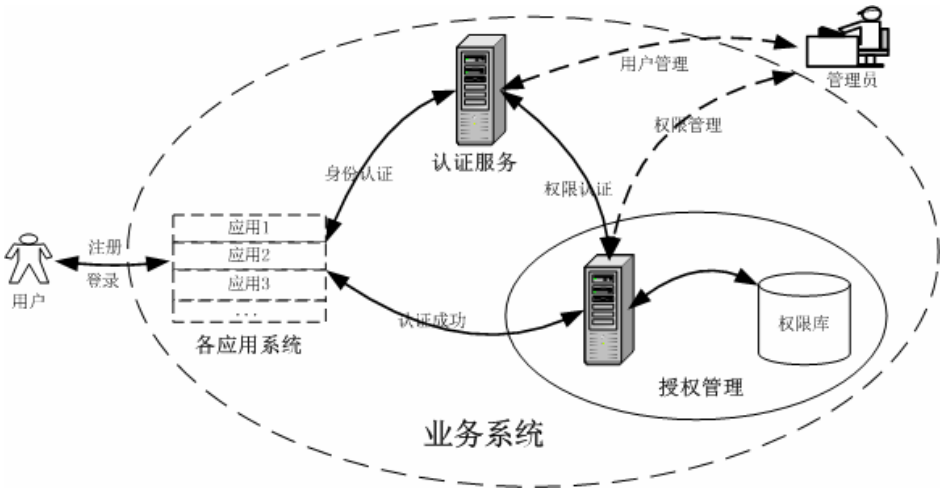


图 7-4　访问控制框架

基于数字证书的用户信息管理模式实现对涉及医院信息平台安全要素的统一管理，包括统一身份管理、角色管理、医院信息资源管理、授权管理等。

7.6.2.3 系统安全审计

系统审计包含主机审计和应用审计两个层面：

(1) 主机审计：

通过部署终端安全管理系统，启用主机审计功能，或部署主机审计系统，实现对主机监控、审计和系统管理等功能。

- ✓ 监控功能包括服务监控、进程监控、硬件操作监控、文件系统监控、打印机监控、非法外联监控、计算机用户账号监控等。

- ✓ 审计功能包括文件操作审计、外挂设备操作审计、非法外联审计、IP 地址更改审计、服务与进程审计等。审计范围覆盖到服务器上的每个操作系统用户和数据库用户；内容包括重要用户行为、系统资源的异常使用和重要系统命令的使用等系统内重要的安全相关事件；审计记录包括事件的日期、时间、类型、主体标识、客体标识和结果等；保护审计记录，避免受到未预期的删除、修改或覆盖等。

- ✓ 系统管理功能包括系统用户管理、主机监控代理状态监控、安全策略管理、主机监控代理升级管理、计算机注册管理、实时报警、历史信息查询、统计与报表等。

(2) 应用审计：

应用层安全审计是对业务应用系统行为的审计，需要与应用系统紧密结合，此审计功能应与应用系统统一开发。应用系统审计功能记录系统重要安全事件的

日期、时间、发起者信息、类型、描述和结果等，并保护好审计结果，阻止非法删除、修改或覆盖审计记录。应用系统如具备上述功能则需要开启使用，若不具备则需进行相应的功能开发，且使用效果要达到以上要求。

其次，部署数据库审计系统对用户行为、用户事件及系统状态加以审计，范围覆盖到每个用户，从而把握数据库系统的整体安全。

7.6.2.4 数据保密性

医院信息平台承载着患者电子病历等隐私数据以及诸多业务操作的中间数据，其保密性要求极高。在保密性方面，主要需要考虑数据丢失和数据泄漏两方面的威胁，数据丢失主要依靠数据备份等机制完成，在本文其它章节有详细描述。

数据泄漏造成的根源来自外部黑客攻击和内部数据泄漏，而就医院信息平台的实际情况而言，内部威胁占据主要比例。不论是内部蓄意泄漏，还是外部黑客攻击，大部分通过以下几个渠道完成：

物理途径——从桌面计算机、便捷计算机和服务器拷贝数据到移动存储介质；通过打印机打印带出医院或者通过传真机发送。

网络途径——通过局域网、无线网络、FTP、HTTP、HTTPS 发送数据，这种方式可以是黑客攻击“穿透”计算机后造成，也可能是内部员工故意从计算机上发送。

应用途径——通过电子邮件、IM 即时信息、屏幕拷贝，P2P（Peer-to-Peer，点对点）应用或者“特洛伊木马”窃取信息。

综上所述，医院信息平台的数据保密性主要从以下几方面解决：

- ✓ **防信息泄漏**

防信息泄漏技术通过对安全计算环境内部敏感信息输出的各种方式进行控

制，目的是防止内部敏感信息被有意或无意外漏。通过在客户端使用防信息泄漏类技术实现数据保护，并完成统一管理；通过数据保护客户端对用户的网络行为进行检测，阻断数据泄漏行为；通过数据保护客户端对具体应用进行检测，阻断数据泄漏行为；通过客户端程序，有效的审计各类数据调用行为，并记录全部用户行为；

- ✓ **设备控制**

对接入计算机的各类外置设备进行控制，防止机密信息通过这类外接设备发生泄漏；针对网络打印机、U 盘等各类高危外设的使用进行审计并记录；一旦发现非法使用，可以第一时间阻断数据泄漏行为；

- ✓ **磁盘和数据加密**

包括文件加密、整盘加密以及移动介质加密等。 文件加密类技术用于防御攻击者窃取存储于文件中的数据，目的是保障文件中存储数据的安全。整盘加密类技术通过对整盘数据进行整体加密来实现数据保密，目的是在数据整盘存储层面保障数据安全。移动介质加密类技术通过对 U 盘等移动介质进行加密处理，防止意外丢失造成的数据泄漏。通过以上技术手段，能够对特定的文件进行加密和控制，并通过管理平台设定统一的管理策略，就算数据由于无意的合法行为造成泄漏，非授权用户也无法进行访问。

7.6.2.5 数据完整性

医疗数据被视为敏感信息，检验检查等医疗数据作为诊断结果的重要依据，其内容一旦发生改变，将造成严重的医疗事故，对医院和患者带来重大的损失。《电子病历基本规范》（试行）要求：“具备对电子病历创建、编辑、归档等操作的追溯能力”，因此医院信息平台中涉及到医疗数据的传输、存储，可以采用电子签名及时间戳等相关技术来保证医疗数据的完整性以及可追溯性。

目前公认的可靠的电子签名是通过基于 PKI 和消息摘要技术的数字签名技

术实现的，通过数字签名和验证服务能够保障数据本身的完整性，实现相关业务操作的抗抵赖。

7.6.2.6 备份与恢复

备份与恢复主要包含两方面内容，首先是指数据备份与恢复，另外一方面是关键网络设备、线路以及服务器等硬件设备的冗余。

数据是最重要的系统资源。数据丢失将会使系统无法连续正常工作。数据错误则将意味着不准确的事务处理。可靠的系统要求能立即访问准确信息。将综合存储战略作为计算机信息系统基础设施的一部分实施不再是一种选择，而已成为必然的趋势。数据备份系统应该遵循稳定性、全面性、自动化、高性能、操作简单、实时性等原则。备份系统先进的特性可提供增强的性能，易于管理，广泛的设备兼容性和较高的可靠性，以保证数据完整性。广泛的选件和代理能将数据保护扩展到整个系统,并提供增强的功能，其中包括联机备份应用系统和数据文件，先进的设备和介质管理，快速、顺利的灾难恢复以及对光纤通道存储区域网（SAN）的支持等。

对于核心交换设备、外部接入链路以及系统服务器进行双机、双线的冗余设计，保障从网络结构、硬件配置上满足不间断系统运行的需要。

7.6.2.7 恶意代码防范

各类恶意代码尤其是病毒、木马等是对网络的重大危害，病毒在爆发时将使路由器、三层交换机、防火墙等网关设备性能急速下降，并且占用整个网络带宽。

针对病毒的风险，建议将病毒消灭或封堵在终端源头。在所有终端主机和服务器上部署网络防病毒系统，加强终端主机的病毒防护能力并及时升级恶意代码软件版本以及恶意代码库。

在安全管理中心，可以部署防病毒服务器，负责制定和终端主机防病毒策略，在网络内网建立全网统一的一级升级服务器，在下级节点建立二级升级服务器，

由管理中心升级服务器通过互联网或手工方式获得最新的病毒特征库，分发到数据中心节点的各个终端，并下发到各二级服务器。在网络边界通过防火墙进行基于通信端口、带宽、连接数量的过滤控制，可以在一定程度上避免蠕虫病毒爆发时的大流量冲击。同时，防毒系统可以为安全管理平台提供关于病毒威胁和事件的监控、审计日志，为全网的病毒防护管理提供必要的信息。

主要执行以下安全策略：

- ✓ 在应用服务器上安装服务器版的防病毒软件，可以捍卫服务器免受病毒、特洛伊木马和其它恶意程序的侵袭，不让其有机会透过文件及数据的分享进而散步到整个用户的网络环境，提供完整的病毒扫描防护功能；

- ✓ 文件系统对象的实时保护策略：服务器防病毒系统通过对文件系统所有需要的模块进行分析，以及阻止恶意代码的执行，为文件服务器的文件系统提供实时的防病毒保护。具体包括：

  - ■ 监听对文件系统的访问；

  - ■ 使用反病毒引擎对可疑对象和染毒对象进行探测；

  - ■ 当检测到可疑对象和染毒对象时执行预设：阻止染毒对象或可疑对象；在清除病毒之前将其保存在备份区域；启动反病毒引擎以清除或删除染毒对象；将可疑对象放置在隔离区或将其删除；

  - ■ 在程序运行过程中，向用户和本地管理员通报所发生的与其有关的事件；

  - ■ 收集被检查过的对象的数据；

- ✓ 隔离可疑对象策略：服务器防病毒系统隔离与备份组件隔离任何可疑对象，为了使防病毒厂商对其进行进一步的分析，该组件对恶意代码进行

安全隔离。这个组件也可以使恶意代码的安全检测和清除方法得到发展。

- ✓ 隔离和备份组件执行以下策略：
  - ■ 保存或按要求保存检测到的可疑对象；
  - ■ 按要求发送可疑对象到防病毒厂商进行分析，同时允许其发展检测及清除病毒的安全方法；
  - ■ 在接受防病毒厂商针对病毒的更新后，重新检测存储在隔离区的对象，用于确定对象的状态及清除病毒的必要性；
  - ■ 按要求恢复隔离区的对象。
- ✓ 通过集中隔离工具，可将感染病毒档案集中隔离到一台服务器；
- ✓ 通过病毒追踪工具，当有病毒通过网络共享扩散时，可侦测到感染病毒的机器；
- ✓ 实现强大、完善的日志管理策略。

7.6.3 区域边界安全

基于电子病历的医院信息平台区域边界安全设计包括对其所涉及的网络网内各区域进行安全设计，设计内容包括对区域边界访问控制、边界安全审计、边界入侵防护、边界恶意代码防范、边界完整性保护方面内容。

具体标准可依据《信息系统安全等级保护基本要求》《信息系统等级保护安全设计技术要求》，同时可以参照《网络基础安全技术要求》等。

7.6.3.1 边界访问控制

医院网络边界总体上主要分为四类，第一是医院办公网与 Internet 之间的边界；第二是医院业务网与第三方网络之间的边界；第三是医院业务网与办公网网络间的边界；第四是医院业务网、办公网内部不同安全域之间的边界（详见前面章节区域边界划分）。通过对网络的边界风险与需求分析，得知在网络层需进行访问控制，通过部署防火墙产品，实现对所有流经防火墙的数据包按照严格的安全规则进行过滤，将所有不安全的或不符合安全规则的数据包屏蔽，杜绝越权访问，防止各类非法攻击行为。同时可以和内网安全管理系统、网络入侵检测系统等进行安全联动，为网络创造全面纵深的安全防御体系。

在各安全区域边界部署防火墙，部署效果如下：

- ✓ **网络安全的基础屏障**

防火墙能极大地提高一个内部网络的安全性，并通过过滤不安全的服务而降低风险。由于只有经过精心选择的应用协议才能通过防火墙，所以网络环境变得更安全。防火墙同时可以保护网络免受基于路由的攻击，如 IP 选项中的源路由攻击和 ICMP 重定向中的重定向路径。防火墙可以拒绝所有以上类型攻击的报文并通知防火墙管理员。

- ✓ **强化网络安全策略**

通过以防火墙为中心的安全方案配置，能将所有安全软件（如口令、加密、身份认证、审计等）配置在防火墙上。与将网络安全问题分散到各个主机上相比，防火墙的集中安全管理更经济。例如在网络访问时，一次一密口令系统和其它的身份认证系统完全可以不必分散在各个主机上，而集中在防火墙一身上。

- ✓ **对网络存取和访问进行监控审计**

如果所有的访问都经过防火墙，那么，防火墙就能记录下这些访问并做出日志记录，同时也能提供网络使用情况的统计数据。当发生可疑动作时，防火墙能

进行适当的报警，并提供网络是否受到监测和攻击的详细信息。另外，收集一个网络的使用和误用情况也是非常重要的。首先的理由是可以清楚防火墙是否能够抵挡攻击者的探测和攻击，并且清楚防火墙的控制是否充足。而网络使用统计对网络需求分析和威胁分析等而言也是非常重要的。

- ✓ **防止内部信息的外泄**

通过利用防火墙对内部网络的划分，可实现内部网重点网段的隔离，从而限制了局部重点或敏感网络安全问题对全局网络造成的影响。再者，隐私是内部网络非常关心的问题，一个内部网络中不引人注意的细节可能包含了有关安全的线索而引起外部攻击者的兴趣，甚至因此而曝露了内部网络的某些安全漏洞。使用防火墙就可以隐蔽那些透漏内部细节如 Finger，DNS 等服务。

- ✓ **精确流量管理**

通过部署防火墙设备，不仅可以实现精准访问控制与边界隔离防护，还能实现阻止由于病毒或者 P2P 软件引起的异常流量、进行精确的流量控制等。对各级节点安全域实现全面的边界防护，严格控制节点之间的网络数据流。

7.6.3.2 边界安全审计

各安全区域边界已经部署了相应的安全设备负责进行区域边界的安全。对于流经各主要边界（比如数据中心区域边界、互联网接入区域边界等）需要设置必要的审计机制，进行数据监视并记录各类操作，通过审计分析能够发现跨区域的安全威胁，实时地综合分析出网络中发生的安全事件。一般可采取开启边界安全设备的审计功能模块，根据审计策略进行数据的日志记录与审计。同时审计信息要通过安全管理中心进行统一集中管理，为安全管理中心提供必要的边界安全审计数据，利于管理中心进行全局管控。边界安全审计和主机审计、应用审计、网络审计等一起构成完整的、多层次的审计系统。

7.6.3.3 边界入侵防护

在各区域边界，防火墙起到了协议过滤的主要作用，根据安全策略在偏重在网络层判断数据包的合法流动。但面对越来越广泛的基于应用层内容的攻击行为，防火墙并不擅长处理应用层数据。

在网络边界和主要安全区域边界均已经设计部署了防火墙，对每个安全计算环境进行严格的访问控制。鉴于以上对防火墙核心作用的分析，需要其他具备检测新型的混合攻击和防护的能力的设备和防火墙配合，共同防御来自应用层到网络层的多种攻击类型，建立一整套的安全防护体系，进行多层次、多手段的检测和防护。入侵防护系统（IPS）就是安全防护体系中重要的一环，它能够及时识别网络中发生的入侵行为并实时报警并且进行有效拦截防护。

IPS 是继“防火墙”、“信息加密”等传统安全保护方法之后的新一代安全保障技术。它监视计算机系统或网络中发生的事件，并对它们进行分析，以寻找危及信息的机密性、完整性、可用性或试图绕过安全机制的入侵行为并进行有效拦截。IPS 就是自动执行这种监视和分析过程，并且执行阻断的硬件产品。

将 IPS 串接在防火墙后面，在防火墙进行访问控制，保证了访问的合法性之后，IPS 动态的进行入侵行为的保护，对访问状态进行检测、对通信协议和应用协议进行检测、对内容进行深度的检测。阻断来自内部的数据攻击以及垃圾数据流的泛滥。由于 IPS 对访问进行深度的检测，因此，IPS 产品需要通过先进的硬件架构、软件架构和处理引擎对处理能力进行充分保证。

7.6.3.4 边界恶意代码防范

与主机、服务器防病毒软件不同，病毒过滤网关运行在区域边界上，分析不同安全域之间的数据包，对其中的恶意代码进行查杀，防止病毒在网络中进行传播。

某些病毒在网络传播中，在没有感染到主机时，对网络已经造成危害，比如

蠕虫病毒，而防病毒网关针对这些病毒产生扫描数据包，采取“空中抓毒”的安全机制，在边界处过滤了危害性的数据包，从而为网络创造一个安全的环境。

防病毒网关与部署在主机、服务器上的防病毒软件配合，形成覆盖全面，分层防护的多级病毒过滤系统，本方案中在医院信息平台与互联网的边界处部署防病毒网关，并进行如下安全策略：

- ✓ 病毒过滤策略：防病毒网关对 SMTP、POP3、HTTP 和 FTP 等应用协议进行病毒扫描和过滤，通过恶意代码特征过滤，对病毒、木马、蠕虫以及移动代码进行过滤、清除和隔离，有效防止可能的病毒威胁，将病毒阻断在敏感数据处理区域之外。

- ✓ 恶意代码防护策略：防病毒网关支持对数据内容进行检查，可以采用关键字过滤等方式来阻止非法数据进入敏感数据区里区域。

- ✓ 蠕虫防范策略：实时检测日益泛滥的蠕虫攻击，并对其进行实时阻断，从而有效防止信息网络因遭受蠕虫攻击而陷于瘫痪。

- ✓ 病毒库升级策略：通过自动和手动两种升级方式完成病毒库的及时更新。

- ✓ 日志审计策略：开启病毒日志、访问日志和系统日志记录，并设置策略使其能够被日志审计系统收集。

7.6.3.5 边界完整性保护

边界完整性检查核心是要对内部网络中出现的内部用户未通过准许私自联到外部网络的行为进行检查，维护网络边界完整性。通过部署终端安全管理系统可以实现这一目标。

在医疗卫生行业中医院业务网是医院网络的核心，当中运行着大量医院门诊、医疗影响、病历等数据，网络中的任何一台机器的安全隐患直接影响到整个

医院网络的正常工作，为了解决医院业务网中的安全问题，即解决医院业务网中主机服务器和计算机终端的安全问题，以及网络间的安全访问问题，我们在医院业务网中建议采用终端管理技术。

终端安全管理系统其中一个重要功能模块就是非法外联控制，探测内部网中非法上互联网的计算机。非法外联监控主要解决发现和管理用户非法自行建立通路连接非授权网络的行为。通过非法外联监控的管理，可以防止用户访问非信任网络资源，并防止由于访问非信任网络资源而引入安全风险或者导致信息泄密。

✓ 终端非法外联行为监控

发现终端试图访问非授权网络资源的行为，如试图与没有通过系统授权许可的终端进行通信，自行试图通过拨号连接互联网等行为。对于发现的非法外联行为，可以记录日志并产生报警信息。

✓ 终端非法外联行为管理

禁止终端与没有通过系统授权许可的终端进行通信，禁止拨号上网行为。

7.6.4 安全通信网络安全

基于电子病历的医院信息平台通信网是其所涉及的通信网络，包括骨干网络、城域网络和其他通信网络（租用线路）等，设计内容包括通信过程数据完整性、数据保密性、保证通信可靠性的设备和线路冗余、通信网络的网络管理等。具体标准可依据《信息系统安全等级保护基本要求》《信息系统等级保护安全设计技术要求》，并参照《网络基础安全技术要求》等。

7.6.4.1 网络结构安全

网络结构的安全是网络安全的前提和基础，对于医院信息网络，选用关键网络设备时需要考虑业务处理能力的高峰数据流量，要考虑冗余空间满足业务高峰期需要；带宽要保证接入网络和核心网络满足业务高峰期需要；绘制与当前运行

情况相符的网络拓扑结构图；根据各部门的工作职能、重要性和所涉及信息的重要程度等因素，划分不同的网段或 VLAN。

7.6.4.2 网络安全审计

网络、安全设备是信息流通的必然结点，每个网络设备都会产生相应的日志信息，通过对日志信息的全面、深入分析，可以了解设备的工作状况，网络状况以及安全事件等信息。要对各类系统产生的安全日志实现全面、有效的综合分析，就必须为网络安全管理员建立一个能够集中收集、管理、分析各种安全日志的安全审计管理中心，把管理员从庞杂的日志信息分析中解放出来，提供一个方便、直观、高效的审计平台，大大提高了安全管理员的工作效率和质量，更加有效地保障了网络的安全运行，通过部署安全审计系统实现的如下策略来保证网络的安全性。

网络安全审计系统主要用于监视并记录网络中的各类操作，侦察系统中存在的现有和潜在的威胁，实时地综合分析出网络中发生的安全事件，包括各种外部事件和内部事件。

在网络交换机处旁路部署网络行为监控与审计系统，形成对全网网络数据的流量监测并进行相应安全审计，同时和其它网络安全设备共同为集中安全管理提供监控数据用于分析及检测。

网络行为监控和审计系统将独立的网络传感器硬件组件连接到网络中的数据会聚点设备上，对网络中的数据包进行分析、匹配、统计，通过特定的协议算法，从而实现入侵检测、信息还原等网络审计功能。

网络行为监控和审计系统采用旁路技术，不用在目标主机中安装任何组件。同时网络审计系统可以与其它网络安全设备进行联动，将各自的监控记录送往安全管理安全域中的安全管理服务器，集中对网络异常、攻击和病毒进行分析和检测。

7.6.4.3 网络设备防护

为提高网络设备的自身安全性，保障各种网络应用的正常运行，对网络设备需要进行一系列的加固措施，包括如下策略：

- ✓ 对登录网络设备的用户进行身份鉴别，用户名必须唯一；
- ✓ 对网络设备的管理员登录地址进行限制；
- ✓ 身份鉴别信息具有不易被冒用的特点，口令设置需 3 种以上字符、长度不少于 8 位，并定期更换；
- ✓ 具有登录失败处理功能，失败后采取结束会话、限制非法登录次数和当网络登录连接超时自动退出等措施；
- ✓ 启用 SSH 等管理方式，加密管理数据，防止被网络窃听。

7.6.4.4 通信完整性和保密性

电子病历等医疗数据包含大量患者的隐私，这些数据一旦泄露将直接导致患者利益受损，甚至对经济、社会稳定造成影响。因此医院信息平台中涉及到医疗数据的传输需要采用加密保护，保证医疗数据通讯的完整性和保密性。

常用的传输加密技术包括基于 SSL 协议的传输通道加密，以及基于数字信封技术的信源加密。

基于 SSL 协议的传输通道加密，可采用 SSL VPN 硬件设备保证远程数据传输的保密性，也可采用服务器证书，在医院信息平台配置单向的 SSL 加密传输通道；

基于数字信封技术的信源加密，可采用 PKI 中间件产品实现对数据源的加密和签名处理，从而保证医院信息平台关键数据的通讯完整性和保密性。

7.6.4.5 网络可信接入

医院信息平台需要建立网络用户和医护人员自然人属性之间一对一的关系，从而便于医院信息中心了解谁在使用网络以及使用网络的用户数量，并针对每个人员使用网络的情况进行有效的监控和审计。

网络可信接入实现网络用户和自然人属性之间的对应，其功能包括：

- ✓ 接入医院网络需经数字证书的实名认证；
- ✓ 经过所属接入域管理员授权许可之后方可接入受控网络；
- ✓ 能够对接入受控网络的用户使用的网络时间以及网络行为进行集中统一的查询统计和监控。

网络可信接入提供完善的接入控制，可支持医院局域网、医院间广域网、VPN以及各种无线接入方式，通过网络层接入和数字证书的结合，实现实名的网络接入。

7.6.5 安全管理中心

由于医院信息网络复杂，用户多，技术人员水平不一。为了能准确了解系统的运行状态、设备的运行情况，统一部署安全策略，应进行安全管理中心的设计，建立统一的系统管理和审计管理平台是有效帮助管理人员实施好安全措施的重要保障，是实现业务稳定运行、长治久安的基础。其次，在实现针对安全计算环境、区域边界和通信网络的安全防护后，基本形成了全面的安全防护体系，符合等级保护的技术安全要求和技术方案设计规范，但是随着安全体系的建设，各种安全设备以及安全服务手段的引入给安全管理带来极大的挑战，系统需要一套有效的网络安全保障，来对全网进行统一的安全管理，确保医院信息平台不发生安全事故、少发生安全事故或者发生安全事故时能够及时处理以减少由于安全事件带来的损失。

此外根据等级保护相关政策，信息系统的安全管理也是一个非常重要的方面，系统必须具备相当的安全运维能力，能够有效进行资产管理、介质管理、网络安全管理、系统安全管理以及恶意代码防范管理等内容，从信息系统整体保护能力方面，要求信息系统能够实现统一安全策略、统一安全管理等技术。

7.6.5.1 集中网络管理

通过建立集中的网络管理机制，对基于电子病历的医院信息平台运行中的网络进行统计、监控和分析，并以此为依据，采用划分网段、负载平衡等动态措施提高网络的性能。 集中网络管理应至少包括配置管理、性能管理、故障管理、安全管理等内容。

- 配置管理：

通过配置管理，随时了解网络系统的拓扑结构，网络节点的状态，包括连接前静态设定的和连接后动态更新的状态。配置管理包括客体管理、状态管理和关系管理等三个方面。

- 性能管理：

性能管理包括工作负荷监测、概要功能、软件管理功能和时间管理等功能。

- 故障管理：

故障管理负责在系统运行时对异常情况的检测、隔离和更正。故障管理包括警报告管理、事件报告管理、日志控制功能、测试管理功能等几个方面。

- 安全管理：

安全管理包括安全特性的管理和确保管理信息的安全。

7.6.5.2 统一数字身份管理

统一的数字身份管理包括统一身份管理与授权管理。身份管理和授权管理是访问控制的前提，身份管理对用户的身份进行标识与鉴别；授权管理对用户访问资源的权限进行标识与管理。统一身份管理与授权管理系统作为安全管理中心的一部分，部署于安全管理区域。

基于电子病历的医院信息平台在各医院得到应用后，平台上各用户的身份管理必将成为网络信任体系建设中的基础内容。在网络空间中，用户不可能以真实实体的形态存在，只能通过电子化的身份凭证来代表或标识。传统的认证方式就是对一个用户的某个身份凭证进行认证，如用户名/口令。然而在复杂的多应用环境下，简单的凭证定义已不满足跨域访问要求，需要对每个用户构建起以数字身份为核心思想的综合信任机制，将其基本信息与各种特定领域的信息标识进行统一管理，并体现为不同的具体凭证，为各类应用提供基于数字身份的可靠认证和授权控制。

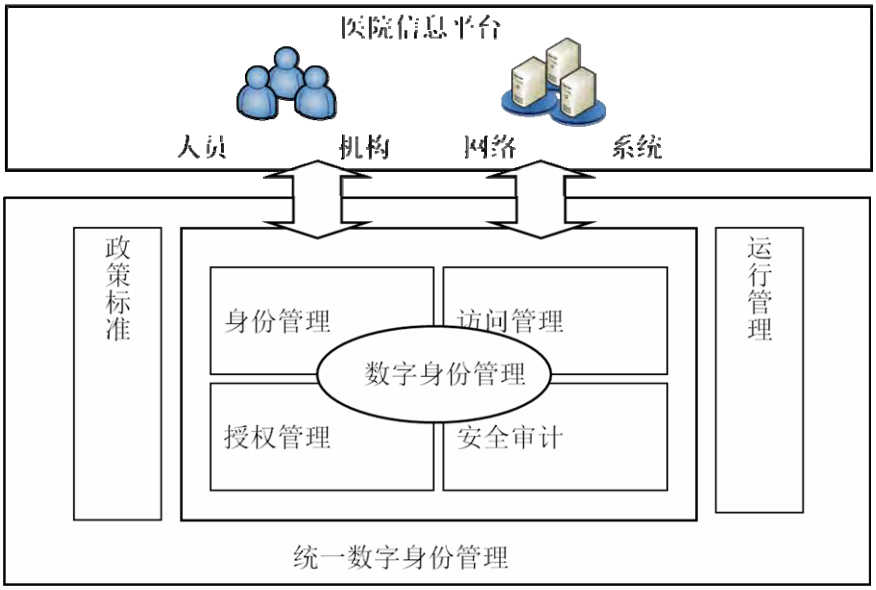


图 7-5　统一数字身份管理

如上图所示，作为整个医院信息平台各类实体的数字身份管理支撑，统一数字身份管理将提供统一身份管理、授权管理、审计管理等功能，从而构建以“认证、授权和责任认定”为核心思想的网络信任体系。

(1) 身份管理

统一数字身份管理的核心，负责对各类实体信息进行数字身份的定义和标识，管理用户信息、部门信息、角色信息、信息系统、用户与角色关系信息的维护，实现数字身份流程化管理，控制数字身份的整个生命周期，需实现以下功能：

- ✓ 应保证用户具有唯一的标识，并采用统一的数据库对用户身份信息进行管理。

- ✓ 应采用数字证书+USB KEY 的双因素认证方式实现强身份鉴别，并对其进行安全存储与管理。

- ✓ 应支持用户能够进行统一的身份鉴别。

- ✓ 应支持用户访问权限的统一管理。

(2) 授权管理

根据对用户的身份认证结果，按照授权管理模型和策略的要求，提供用户授权访问的信息资源，需实现以下功能：

- ✓ 依据用户的职权属性和系统信息的安全属性，制定授权策略；

- ✓ 按照用户身份信息，基于授权策略建立自主访问控制列表；

- ✓ 授权管理。按照分域控制、分类防护要求，按部门、按人员的职责确定其所访问的范围；

- ✓ 应支持部门进行分层次授权，避免集中授权复杂性，提高授权的准确性；

- ✓ 提供与应用系统模块信息的同步接口；提供与授权信息的同步接口；提供授权信息的在线查询接口。

⑶ 安全审计

实现对用户所有登录认证操作及授权访问行为的全面记录和监控，确保所有操作处于可控和可审计状态，需实现以下功能：

- ✓ 基本的行为审计记录功能，支持访问医院信息平台各类行为的安全审

计；

- ✓ 基于网络数据流的安全审计；支持审计自动转储和审计在线查询；
- ✓ 具备对医院信息平台内部数据访问行为的安全审计；
- ✓ 支持授权用户通过审计查阅工具进行审计数据的查询，审计数据应易于理解；
- ✓ 具备审计日志数据的完整性保护；
- ✓ 可实现各种安全设备审计数据的集中管理。

7.6.5.3 统一安全管理

通过建立集中的安全监控管理机制，实现对所保护的安全设备和系统对象状态的统一配置管理，监控安全设施系统资源的变化，并根据变化情况和事件记录，及时调整安全策略，执行有效的防控措施。需实现以下功能：

(1) 安全设备集中管理

通过在安全设备监管平台中录入医院安全设备信息，可实现对设备和系统对象的配置管理，同时，通过对安全事件与关注资产的关联分析，为风险管理、事件监控协同工作和分析以及预警等提供基础。

(2) 安全策略统一管理

网络安全的整体性要求需要有统一安全策略和基于工作流程的管理。通过为医院的网络安全管理人员提供统一的安全策略，为网络中安全策略的部署工作做指导，有利于在全网形成安全防范的合力，提高全网的整体安全防御能力，同时可以进一步完善整个网络的安全策略体系建设，为指导各项安全工作的开展提供行动指南，有效解决目前因缺乏口令、认证、访问控制等方面策略而带来到安全风险问题。

(3) 安全状态统一监测预警

通过对防病毒控制台、入侵检测系统控制台、身份认证服务器、防火墙等设备的事件搜集以及对这些事件的整合、分析，实现全网的安全事件集中监测和处理。其次，安全预警是一种有效的预防措施，通过对资产以及脆弱性的综合分析得到网络中资产的安全风险，从而及时发布有关的安全漏洞信息和解决方案，督促和指导医院安全管理部分及时做好安全防范工作，防患于未然。

7.6.5.4 集中日志审计

通过建立集中日志审计机制，实现对医院信息平台依托的各类安全设备（防火墙、入侵检测系统（IDS）、防病毒软件等）、操作系统（Windows、Linux 和 Unix 等）、应用服务的日志进行集中收集、管理、分析和保存。

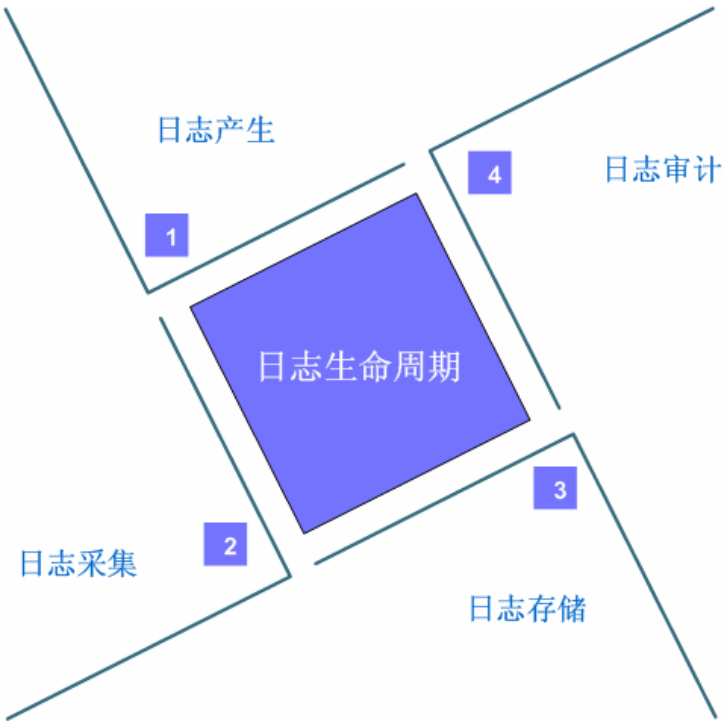


图 7-6 集中日志审计

通过建立基于电子病历的医院信息平台的集中日志审计平台，实现上图中日志的集中审计与管理，具体内容如下：

- 日志数据采集：根据医院信息平台依托的网络结构、支撑系统、业务系统各资源主机、网络设备、应用系统的类型和网络分布，采取本地型日志采集方式和网络型日志采集方式，对全网的设备、应用以及网络操作进行全面的日志采集。
- 规范审计记录：由于医院信息平台依托的设备种类繁多，每种设备由于业务不同，日志上报的格式和内容项都有所不同。因此日志审计产品必须对采集到的各种设备日志格式进行统一，同时尽可能保留审计记录来源信息，为后续的审计分析提供依据。
- 策略日志过滤、归并：医院信息平台网络中，各个设备运行繁忙，日志信息量非常大，日志集中管理与审计系统可根据相关策略对原始日志进行过滤和归并，以减轻日志数据在网络中的传输压力和数据中心的存储压力。
- 本地型日志审计与网络型日志审计相结合的审计体系。本地型日志记录本地操作，通过多种采集机制汇总到日志集中管理与审计系统；网络型日志则通过网络旁路抓包的方式获取网络操作，两者结合可构成综合的审计体系。
- 多维关联分析需求：对于来自各个资源的日志信息，提供多维的关联分析功能，将一个用户在多个设备上的操作进行横向关联分析，形成针对用户为主题的操作行为审计；对于发生在多个设备上的事件进行关联分析，形成一个完整的事件流操作过程审计；对于多个用户对本设备的操作，形成本设备被访问的安全审计报告等。
- 日志存储需求：由于日志信息是来自初始数据，因此要求对日志的存储提供加密方式的存储机制，同时，对于存储的日志不能进行修改和删除。为了提高存储的容量，能够提供压缩存储的机制。
- 符合等级保护合规要求：根据等级保护安全审计要求，定期对审计信息进行汇总及报表非分析。

综上所述，集中日志审计平台为不同的网络设备提供了统一的事件管理分析平台，可有效实现全网的安全预警、入侵行为的实时发现、入侵事件动态响应，通过与其它安全设备的联动来真正实现动态防御。

7.6.6 物理安全保护

物理安全是指基于电子病历的医院信息平台资产所处的物理环境的安全。物理安全方面的威胁主要包括电磁泄露、通信干扰、信号注入、人为破坏、自然灾害、设备故障等。物理安全设计可以从安全技术设施和安全技术措施两方面进行，具体依据标准《信息系统安全等级保护基本要求》、《信息系统等级保护安全设计技术要求》等。

各医院根据实际情况，通过实施物理安全控制可以防止对医院信息平台物理资源的非授权物理访问，控制物理风险，降低信息资产破坏造成损失。

医院信息平台所在的物理安全保护设计如下：

(1) 物理位置选择

- ✓ 医院信息平台所在的机房与办公场地应选择在具有防震、防风和防雨等能力的建筑内；
- ✓ 医院信息平台所在的机房场地避免设在建筑物的高层或地下室及用水设备下层或隔壁。

(2) 物理访问控制

- ✓ 医院信息平台所在的机房出入口应安排专人值守，控制、鉴别和记录进入的人员；
- ✓ 医院信息平台所在的机房的来访人员应经过申请和审批流程，限制和监控其活动范围；
- ✓ 医院信息平台所在的应对机房划分区域进行管理，区域和区域之间设置物理隔离装置，在重要区域前设置交付或安装等过渡区域；
- ✓ 医院信息平台所在的重要区域应配置电子门禁系统，控制、鉴别和记录进出入的人员。

(3) 防盗窃和防破坏

- ✓ 医院信息平台主要设备放置在机房内；
- ✓ 医院信息平台设备或主要部件进行固定，并设置明显且易除去的标记；
- ✓ 医院信息平台所使用的通信线缆铺设在隐蔽处，可铺设在地下或管道中；
- ✓ 医院信息平台使用的介质分类标识，存储在介质库或档案室中；

- ✓ 利用光、电等技术设置机房防盗报警系统；
- ✓ 医院信息平台所在的机房设置监控报警系统。

(4) 防雷击

- ✓ 医院信息平台所在的机房建筑应设置避雷装置；
- ✓ 医院信息平台所在的机房应设置防雷保安器，防止感应雷；
- ✓ 医院信息平台所在的机房应设置交流电源地线。

(5) 防火

- ✓ 医院信息平台所在的机房应设置火灾自动消防系统，能自动检测火情并自动报警及灭火；
- ✓ 医院信息平台所在的机房及相关的工作房间和辅助房应采用具有耐火等级的建筑材料；
- ✓ 医院信息平台所在的机房应采取区域隔离防火措施，将重要设备与其他设备隔离开。

(6) 防水和防潮

- ✓ 医院信息平台所在的机房水管安装，不得穿过机房屋顶和活动地板下；
- ✓ 医院信息平台所在的机房应采取措施防止雨水通过机房窗户、屋顶和墙壁渗透；
- ✓ 医院信息平台所在的机房应采取措施防止机房内水蒸气结露和地下积水的转移与渗透；
- ✓ 医院信息平台所在的机房应安装对水敏感的检测仪表或元件，对机房进行防水检测和报警。

(7) 防静电

- ✓ 医院信息平台所在的机房主要设备应采用必要的接地防静电措施；
- ✓ 医院信息平台所在的机房机房应采用防静电地板。

(8) 温湿度控制

医院信息平台所在的机房应设置温、湿度自动调节设施，使机房温、湿度的变化在设备运行所允许的范围之内。

(9) 电力供应

- ✓ 医院信息平台所在的供电线路上配置稳压器和过电压防护设备；

- ✓ 医院信息平台所在的机房应提供短期的备用电力供应，至少满足主要设备在断电情况下正常运行；
- ✓ 医院信息平台所在的机房设置冗余或并行的电力电缆线路为计算机系统供电；

(10) 电磁防护

各医院根据实际情况适当建立电磁防护措施：

- ✓ 医院信息平台所在的机房采用接地方式防止外界电磁干扰和设备寄生耦合干扰；
- ✓ 医院信息平台所在的机房电源线和通信线缆应隔离铺设，避免互相干扰；
- ✓ 医院信息平台所在的机房应对关键设备和磁介质实施电磁屏蔽。

7.6.7 主要安全技术实现

7.6.7.1 边界访问控制

区域边界防护是关注如何对进出基于电子病历的医院信息平台计算环境边界的数据流进行有效的检测和控制，且能够与其它层面的安全措施协同运作，以提供对域内信息系统综合防护。区域边界防护的首要任务是明确安全边界，总体边界总体上可归为“纵向边界、横向边界”，区域边界安全防护需要达到以下要求：

(1) 纵向边界安全防护

纵向区域边界指部级单位与各省级卫生厅、地市级卫生局外网网络间的边界，安全防护控制要求描述如下：

- ■ 边界访问控制
  - ✓ 在纵向网络边界采取访问控制措施或主动防护措施，对进出边界数据流进行细粒度的流量约束与访问控制；
  - ✓ 对于违背边界访问控制策略的行为可进行日志记录，并定期分析处理，作为风险状况跟踪、策略有效性评估和策略持续改进的依据；
  - ✓ 对于安全重点防护的区域边界，应综合采用较严格的防护措施。
- ■ 远程接入控制
  - ✓ 对远程接入访问平台服务的行为，应采用公钥校验、IPSEC 或 SSL

等方式实现接入认证访问控制；

- ✓ 远程接入的主机应具备统一的桌面终端安全防护措施；
- ✓ 采用网络接入控制机制对远程接入的主机实现校验，需要完成安全状态检查，对不满足要求的接入请求必须进行处理后方可允许接入，同时需要对此类行为进行监控审计；
- ✓ 采用拨号方式的接入请求，在建立拨号连接后，应附加采用 IPSEC 或 SSL 等策略机制进行授权访问；
- ✓ 远程接入应具备身份认证机制，尽量采用公钥技术、动态口令等强认证手段；采用用户名 / 口令认证时，应对口令长度、复杂度、生存周期进行强制要求；应制定用户登录错误锁定及会话超时断开等安全策略保证远程访问的安全控制；
- ✓ 根据用户的不同角色进行授权，权限应严格限制，并由相关负责人审批后方可开通，并依据其业务访问需求定制访问控制策略；
- ✓ 对于第三方远程系统维护，禁止建立永久专用线路连接，应采用 VPN 等技术按需进行系统连接，并实行定期审核、严格管理；
- ✓ 应对于用户接入访问等行为等进行日志记录，并定期分析处理，跟踪潜在和残余的风险。

■ 对外发布服务安全

- ✓ 对于跨越纵向边界所对外提供的网络服务，应对边界访问控制设备强化访问控制列表，限制外发连接，在 IP 地址、协议、端口等层次细化访问控制矩阵；
- ✓ 对跨越外网边界所提供的信息资源服务（如：目录访问服务、信息展现服务）等，应对边界访问控制设备上强化访问控制列表，限制由应用服务器发起的外发连接，在 IP 地址、协议、端口等层次细化访问控制策略；
- ✓ 应对提供服务的类别（如：HTTP、DNS）进行入侵防护，对所传输协议内容进行监控，防止通过公用协议传输攻击代码，发现入侵行为可及时阻断并进行报警及日志记录；
- ✓ 需采用防篡改技术或网站监控技术保证对外发布的服务页面文件不

被恶意篡改或安全事件发生后能够及时恢复；

- ✓ 应采用专用边界防护设备，防止对 DDoS（Distributed Denial of service）类攻击行为的发生。

■ 边界完整性检查

采用管理手段结合专用技术措施（如非法外联、接入控制等技术）防止内部非法外联行为发生，并可准确的定位和阻断报警。

(2) 横向域间边界防护

横向域间防护是指根据对平台所划分的不同防护区域，定制适度的防护策略和控制措施，以保证所交换数据的机密性、完整性和可用性。

■ 网络访问控制

- ✓ 针对各区域边界之间的数据流交换，应采用访问控制措施以确保域内信息资产的安全，边界隔离与访问控制可采用防火墙、网闸及 VLAN 等多种方式实现；
- ✓ 应明确连接域内或域外特定资产的信源地址范围，制定允许受信访问的约束规则；
- ✓ 对于域间异常通信所触发的访问控制策略冲突，审计日志可及时发现并需要定期分析处理。

■ 信息威胁的入侵检测

- ✓ 应对各区域边界间所传输的关键数据流进行威胁因素检测、过滤、告警与取证；
- ✓ 应根据交换数据所采用的服务端口定制检测规则库，以保证检测的效率与准确性；
- ✓ 应制定核心安全事件冲突的即时报警策略，在发生重要安全策略冲突时，第一时间进行应急处理；
- ✓ 对于入侵检测日志应定期分析处理，从安全事件中分析入侵意图及安全趋势，做出合理性建议。

7.6.7.2 入侵检测措施

采用实时入侵检测机制对流经边界的信息流进行入侵检测分析，规避对服务

器发起的应用层攻击风险；同时在发生入侵事件时，应能提供及时的报警信息，必要时给予阻断防护。

入侵检测系统按其实现方式可以分为网络入侵和主机入侵检测系统：

- ✓ 网络的入侵检测系统（Network intrusion detection system，NIDS）：通过嗅探的方式截获通过网络上所有的数据包，通过特征分析、异常统计分析等方法，实时发现网络攻击和异常安全事件。

- ✓ 主机入侵检测系统（Host-based intrusion detection system，HIDS）：部署于要保护的主机上对入侵事件进行检测分析，通过分析主机日志及网络事件发现入侵行为。

在网络入侵检测系统配置前，应在核心交换机上进行端口映射。这步操作会对交换机性能有一定影响，因此部署前，应查看交换机负载并记录，并根据端口映射后的交换机负载来比较确认端口映射不至于影响关键业务，在对服务器进行入侵检测防护时，应当通过入侵检测系统规则选择相对重要的服务器以保证入侵检测的性能。

7.6.7.3 无线安全措施

目前，很多医院使用了 PDA 等无线终端设备，而无线安全又极易被忽略，因此，本节将对无线安全提出措施。无线局域网采用公共的电磁波作为载体，而电磁波能够穿越天花板、玻璃、楼层、砖、墙等物体，因此在一个无线局域网接入点(Access Point)的服务区域中，任何一个无线客户端都可以接收到此接入点的电磁波信号，而非授权的客户端也能接收到数据信号。也就是说，由于采用电磁波来传输信号，非授权用户在无线局域网（相对于有线局域网）中窃听或干扰信息就容易得多。所以为了阻止这些非授权用户访问无线局域网络，使用无线应用时应当引入相应的安全控制措施。

实现无线网络过程中应当考虑以下安全控制措施：

- 隐藏 SSID（Service Set Identifier），SSID 使无线客户端可以识别不同无线网络。参数在设备缺省设定中是被 AP 无线接入点广播出去的，客户端只有收到这个参数或者手动设定与 AP 相同的 SSID 才能连接到无线网络。如果把这个广播禁止，一般的漫游用户在无法找到 SSID 的情况下是无法连接到无线网络。

- 应当启用无线数据加密。采用 WEP（Wired Equivalent Privacy）或 WPA（Wi-Fi Protected Access）等无线加密方式对无线传输的数据进行加密。

- 限制 DHCP 使用：安全配置无线设备的 DHCP 服务，使其仅向无线网段提供地址服务，防止有线网段意外通过无线设备获得 IP 地址。

- SNMP 安全设置：禁用或对 SNMP 服务进行安全设置，使用 SNMP v2c 以上的版本并更改默认的 community 字段。

- 使用访问控制列表对通过无线的可访问资源进行限制。应当使用访问控制列表限制通过无线连接用户对资源的访问权限。或者将 AP 和内部局域网之间部署防火墙进行防护

- 根据终端的不同，可以灵活采用多种认证技术，包括 MAC 地址认证、Portal 认证。

7.6.7.4 病毒检测措施

病毒是一种程序，它通过把代码在不被察觉的情况下镶嵌到另一段程序中，从而达到破坏被感染电脑数据、运行具有入侵性或破坏性的程序、破坏被感染电脑数据的安全性和完整性的目的。按传播方式，病毒代码可以分成以下几类：文件病毒，木马病毒，蠕虫病毒和复合型病毒。

以下为防病毒系统的实现要求：

- 应当对防病毒服务器实现定期更新，在重大病毒预警发布时应及时按需

更新；

- 应配置以提供日志报告，并定期审核报告以监控病毒防护情况；
- 应设置尽量采用增量升级模式在非业务高峰期来分发特征代码；
- 应对病毒可能侵入系统的途径（如软盘、光盘、可移动磁盘、网络接口等）进行控制，严格控制并阻断可能的病毒携带介质在系统内的传播；
- 在网络性能允许的前提下，建议在 Internet 边界处部署防病毒网关或相应防病毒模块。

7.6.7.5 日志审计措施

日志是对用户行为和系统行为进行记录，以备回顾审查。日志审计是保障应用系统信息安全的重要手段。如用户在应用系统上的活动、登入和登出时间，与计算机信息系统内敏感的数据、资源、文本等安全有关的事件，实时记录在日志文件中，便于发现、调查、分析及事后追查责任，为加强管理措施提供依据。

- 应设立统一的日志服务器，将各日志源的日志集中发送到日志服务器上；
- 应开启主机系统、网络设备、安全设备和软件、应用系统和数据库等的日志审计；
- 应制定恰当的日志策略，确定记录日志的设备或系统范围、记录日志的事件类别、记录日志的最大时间范围、日志备份策略、审计日志的处理方式等；
- 日志中应包括事件发生的时间、触发事件的主体与客体、事件的类型、事件成功或失败、事件的结果等内容；
- 应定期检查日志磁盘空间，及时备份和删除日志；

- 应对日志进行分析，关联分析生成可阅读的报告。

7.6.7.6 备份与恢复

关键、重要业务系统软件安全备份功能应当符合公司相关规定中的技术要求。对关键业务系统数据必须制定备份策略，采取备份措施。

- 定期采取手工备份方式对重要文件及保存在数据库中的数据进行备份；
- 定期采取自动备份系统进行应用数据备份，管理员应复核自动备份结果；
- 在业务环境变更或定期执行备份恢复测试；
- 详细的备份恢复措施详见“存储”及“灾难恢复”相关章节。

7.6.7.7 认证与授权管理

身份和访问管理是用来管理数字化身份并控制身份如何访问资源的方法、技术和策略。身份和访问管理包括两部分内容：身份管理和访问管理。

身份管理需要实现用户账号申请、审批、变更及撤销工作流的创建，从整体角度设置信息系统资源，并尽量通过自动化流程降低成本。可借助集成化的单点登录和个性化的企业门户实现自助服务（例如密码重置等）。

访问管理指的是为了满足资源请求而进行控制和授权允许访问的过程。这一过程经常通过一个认证、授权及审计动作次序来完成。鉴定是身份声明获得证明的过程。授权是决定是否允许一个身份执行某一动作或访问某一资源。审计是记录的过程，用来记录已发生的权限安全事件。

卫生部颁发的《卫生系统电子认证服务管理办法》（试行）中指出：“凡涉及国家安全、社会稳定、公众利益的各类重要卫生信息系统，应当按照国家法律法规、信息安全等级保护制度等要求，采用电子认证服务，解决身份认证、授权管

理、责任认定等安全问题”，医院信息平台中的电子病历等信息系统涉及到患者的基本信息、病情病理等敏感信息，应使用数字证书来实现医护人员的强身份认证。

医院的医生、护士以及技师等医护人员通过数字证书登录信息系统，进行授权下的医疗业务应用操作，处理完成后的数据通过数字签名/验证服务器进行数字签名，并基于安全信道提交数据中心。为实现上述业务流程，可通过基于数字证书的统一认证管理系统、PK 中间件以及数字签名/验证服务器等实现，利用统一身份认证管理系统实现统一的安全身份认证和统一的授权管理；PKI 中间件支撑数字证书的基本应用；数字签名/验证服务器为信息平台应用中的数据提供完整性保障，实现应用操作过程中的抗抵赖功能，确保信息平台应用中关键业务操作的安全性。关于身份认证、访问管理的相关措施遵循以下原则：

- 当医院规模较大，应用数量众多，用户数量庞大时，应当考虑对用户身份进行集中管理、统一认证；
- 应当制定对于用户帐号权限的申请、审批、变更及撤销流程；
- 应当基于最小化授权原则对用户授予其执行业务操作的最小权限；
- 应当制定对于用户行为及重要资源访问的审计措施；
- 重要的医疗信息系统采用基于数字证书的强身份认证、责任认定机制，需满足卫生部颁布的《卫生系统电子认证服务规范》、《卫生系统数字证书格式规范》、《卫生系统数字证书介质技术规范》、《卫生系统数字证书应用集成规范》和《卫生系统数字证书服务管理平台接入规范》等电子认证服务体系规范；

7.6.7.8 资产与行为监控

按服务性质不同，可将主机系统安全防护整体上划分为应用服务器安全防护、桌面主机安全防护，以下将对其并分别提出安全防护要求。

(1) 服务系统安全防护

应用服务器的安全应从操作系统安全和数据库安全两个层面进行设计：

■ 操作系统基础防护：

✓ 依据操作系统厂商或专业安全组织提供的安全列表进行安全加固；

✓ 制定用户管理策略、帐号及权限申请、审批、变更、撤销流程，定义用户口令管理策略；

✓ 禁止多个用户共享帐号；应制定用户登录错误锁定、会话超时退出等安全策略；

✓ 限制管理员权限使用，一般日常操作中，应使用一般权限用户，仅在必要时切换至管理员帐号进行操作；

✓ 应采用第三方安全工具增强操作系统安全性，如主机防火墙、主机入侵检测、病毒防护系统等；

✓ 应引用系统级资产防护措施，强化服务器系统的本地操作行为控制和监控能力；

✓ 应对重要系统文件进行数字签名检查，以避免系统被植入非法程序；

✓ 应使用弱点扫描工具定期对系统漏洞进行扫描，同时定期对漏洞库更新升级，扫描应在非关键业务时段进行，制定适度的扫描计划，对于扫描出的漏洞应及时进行处理；

✓ 进行远程系统管理应采取加密、散列等措施对经网络传输的认证信息进行处理，并对允许连接的客户端进行限制；

✓ 应及时更新厂商发布的核心安全补丁，更新补丁之前应在测试系统中进行测试，并制定详细的回退方案；

✓ 应定期对操作系统及运行于操作系统之上的业务应用系统、数据库系统数据进行备份，并定期或在操作环境发生变更时进行备份恢复测试；

✓ 应以系统日志方式对用户行为、系统资源异常访问等安全事件进行审计，应加强对日志记录的保护，避免被意外删除、修改或覆盖等。

■ 身份认证与账号管理：

✓ 应制定安全策略实现账号及权限申请、审批、变更、撤销流程；

✓ 关键系统应采用两种或两种以上组合的认证技术进行身份认证，如动态

口令、物理设备绑定、生物识别技术及数字证书等方式的任意组合；

- ✓ 应制定用户登录错误锁定、会话超时退出等安全策略；
- ✓ 限制管理员权限使用，可在必要时切换至管理员账号进行操作；
- ✓ 应根据管理角色分配权限，实现基于角色的权限分离，加强最小权限的设置，操作系统特权用户不得同时作为数据库管理员；
- ✓ 应严格限定默认账号的访问权限，重命名系统默认账号，修改账号时的初始口令，及时删除不用的、过期的账号。

■ 访问控制：

- ✓ 应对系统资源启用访问控制功能，依据安全策略严格限定用户对敏感资源的访问；
- ✓ 对于关键系统应对重要信息资源设置敏感标记，制定访问控制策略，严格控制用户对有敏感标记的重要信息资源进行操作。

■ 安全审计：

- ✓ 应以系统日志方式对用户行为、系统资源异常访问等安全事件进行审计，同时加强对日志记录的保护，避免被意外删除、修改或覆盖；
- ✓ 审计范围应覆盖到服务器每个操作系统用户和数据库用户；
- ✓ 定期根据日志记录数据进行事件分析，对于关键系统应生成审计报表。

■ 资源控制：

- ✓ 对重要服务器的 CPU、硬盘、内存、网络等资源的使用状况进行监测，服务水平降低到预定的最小值应进行报警；
- ✓ 进行操作系统远程管理维护时，应以终端接入方式、网络地址范围等条件限制终端登录；

■ 系统备份：

- ✓ 定期对操作系统、业务系统及数据库系统程序进行备份；
- ✓ 定期或在操作系统环境、数据库、应用系统发生变更时，进行备份恢复测试。

■ 恶意代码防护

- ✓ 采用基于网络的防病毒套件进行恶意代码防护；
- ✓ 定期更新软件特征码，以保证特征码及时有效更新；

- ✓ 制定严格的安全策略，限制用户自行下载安装不明软件；
- ✓ 管理员集中监测恶意代码事件报告，并进行相关处理。

■ 补丁更新管理

- ✓ 及时更新操作系统及核心应用安全补丁，可采用集中补丁分发系统；
- ✓ 应监测各桌面终端安全补丁更新情况，并发现问题及时进行处理。

■ 主机资产管理

- ✓ 应采取措施对资产使用、变更状况进行监控管理，在主机的资产发生变化时，应产生报警信息通知管理员；
- ✓ 应采取措施控制主机设备使用，如限制主机中对于软盘、光盘、移动硬盘、优盘等移动介质的使用；
- ✓ 应限制使用者自行连接外部设备，如拨号 Modem、摄像头等可能对网络安全造成影响的设备。

■ 桌面安全管理

- ✓ 根据实际情况，采用 Windows 域管理方式，针对不同安全需求定制不同的 Windows 域分发策略；
- ✓ 采用专用终端安全管理系统及策略进行桌面安全管理；
- ✓ 采用终端准入控制措施对接入的主机安全状态进行检查，如防病毒软件、主机防火墙的安装情况及策略版本情况等，并在通过身份认证后方允许接入网络或资源访问；
- ✓ 采用可集中管理的入侵检测防护措施进行防护，或采用集合防火墙、入侵检测/防护等终端管理套件进行统一的桌面安全管理。
- ✓ 安全审计：对于客户端连接关键系统进行的业务操作，则需对执行重要业务操作的客户端实现安全审计。
- ✓ 审计范围应覆盖到每个操作系统用户；
- ✓ 应以系统日志方式对用户行为、系统资源异常访问等重要安全事件进行审计；
- ✓ 应定期根据日志记录数据进行事件分析，并生成审计报表。

7.6.7.9 安全登录管理

- ✓ 网络设备登录认证建立开启设备自身的策略审核机制，设置有效的

登录口令和账户；

- ✓ 采用用户名/口令方式进行的登录认证时，应禁止多个管理员共享用户名/口令；应制定登录错误锁定、会话超时退出等安全策略；
- ✓ 特权用户进行权限分离优化与设置，使配置管理员不应拥有更改或删除操作日志的权限；
- ✓ 采用 HTTPS、SSH 等安全远程手段拟补 HTTP、Telnet 等方式登录的弱点，实现系统的或设备的登录；
- ✓ 采用各种远程管理方式进行远程服务器或网络设备维护时，应限制可连接的客户端身份、地址范围、行为模式和时限等约束条件；
- ✓ 采用定期的安全加固方式对设备的配置信息、策略等进行定期的检测修改或加固；
- ✓ 对于平台所依附的所有网络及安全设备建立定期的脆弱性检测机制，发现所存在的漏洞弱点并及时修补，同时应制定完善的应急或回退计划以保证紧急情况下的措施采用；
- ✓ 建立设备的集中日志审计机制（或开启服务器对网络设备的运行状况、异常流量、用户行为等审核策略），并确保审计记录的完整性；
- ✓ 对每次网络设备或安全设备配置更新后，需对配置文件备份进行备份，防止配置意外更改或丢失；
- ✓ 按照平台上各类业务应用的服务级别分别设置边界的带宽使用率，设定策略或采用专业的流量管理技术手段保证在发生拥堵时优先确保重要业务信息流传输畅通；
- ✓ 采用链路冗余或集群等方式保证平台业务服务器及核心的网络交换设备、安全系统及通信线路在发生故障或安全事件时的持续可用性。

7.6.7.10 业务流量保护

对于平台系统所在的网络区域边界，采取流量监控措施对采集、上报到平台业务区域的数据流量实行监控管理，并定制流量策略及阀值报警策略，定期实现对异常流量的分析。

7.6.7.11 物理安全措施

物理安全是指医院信息平台中信息资产所处的物理环境的安全。物理安全是计算机与网络的设备硬件自身的安全和信息系统硬件的稳定性运行状态。虽然物理安全在信息安全控制中相对简单容易理解，但物理安全往往是内部人员恶意入侵的攻击链中很重要的一个起始环节，是内部安全控制中不可或失的重要方面之一。物理安全防护详细的设计内容参见 7.6.6 物理安全防护章节。

7.6.8 不同等级系统互联互通

明确等级划分之后，不同等级的系统间面临着互联互通的问题，系统间需要进行数据交换。

不同安全等级的系统互联互通，应遵循以下原则：

- 不同等级安全域互联后各级系统须能够满足本级各项基本技术要求，高安全等级的系统要充分考虑引入低安全等级系统后带来的风险，不能因为互联而无法达到相应的基本要求，破坏本等级的安全边界。

- 互联手段中重点是互联边界应采取相应的边界保护、访问控制等安全措施，防止高等级系统的安全受低等级系统的影响。边界产品可有针对性的选择防火墙、入侵防护等边界安全设备。

- 根据系统业务要求和安全保护要求，制定互联互通安全策略，包括访问控制策略和数据交换策略等，严格控制数据在不同等级之间的流动。

7.7 安全管理设计

医院应当建立电子病历等医疗数据信息安全保密制度，设定医务人员和有关医院管理人员调阅、复制、打印电子病历的相应权限，建立电子病历使用日志，记录使用人员、操作时间和内容。未经授权，任何单位和个人不得擅自调阅、复制电子病历。同时，建立、健全电子病历使用的相关制度和规程，包括人员操作、

系统维护和变更的管理流程，出现系统故障时的应急预案等。

具体标准可依据《信息系统安全等级保护基本要求》，并参照《信息系统安全管理要求》等进行。

7.7.1 安全管理设计

结合医院信息平台业务情况，安全体系管理层面设计主要是依据《信息系统安全等级保护基本要求》中的管理要求而设计。分别从以下方面进行设计：

7.7.1.1 安全管理制度

根据安全管理制度的基本要求制定各类管理规定、管理办法和暂行规定。从安全策略主文档中规定的安全各个方面所应遵守的原则方法和指导性策略引出的具体管理规定、管理办法和实施办法，是具有可操作性，且必须得到有效推行和实施的制度。

制定严格的制定与发布流程，方式，范围等；

定期对安全管理制度进行评审和修订，修订不足及进行改进。

7.7.1.2 安全管理机构

根据基本要求设置安全管理机构的组织形式和运作方式，明确岗位职责；

设置安全管理岗位，设立系统管理员、网络管理员、安全管理员等岗位，根据要求进行人员配备，配备专职安全员；

建立授权与审批制度；

建立内外部沟通合作渠道；

定期进行全面安全检查，特别是系统日常运行、系统漏洞和数据备份等。

7.7.1.3 人员安全管理

根据基本要求制定人员录用，离岗、考核、培训几个方面的规定，并严格执行；规定外部人员访问流程，并严格执行。

7.7.1.4 系统建设管理

根据基本要求制定系统建设管理制度，包括：系统定级、安全方案设计、产品采购和使用、自行软件开发、外包软件开发、工程实施、测试验收、系统交付、安全服务商选择等方面。从工程实施的前、中、后三个方面，从初始定级设计到验收评测完整的工程周期角度进行系统建设管理。

7.7.1.5 系统运维管理

根据基本要求进行信息系统日常运行维护管理，利用管理制度以及安全管理中心进行，包括：环境管理、资产管理、介质管理、设备管理、网络安全管理、系统安全管理、恶意代码防范管理、密码管理、变更管理、备份与恢复管理、安全事件处置、应急预案管理等，使系统始终处于相应等级安全状态中。《电子病历基本规范（试行）》第十六条第一项规定：“具备保障电子病历数据安全的制度和措施，有数据备份机制，有条件的医疗机构应当建立信息系统灾备体系。应当能够落实系统出现故障时的应急预案，确保电子病历业务的连续性”。因此，基于电子病历医院信息平台应采取相关措施满足上述要求，从而确保业务连续性。

7.7.2 安全管理措施实现

表 7-5 安全管理措施实现

要求类别		基本要求	解决方案
安全管理	管理制度	a) 应制定信息安全工作的总体方针和安全策略，说明机构安全工作的总体目标、范围、原则和安全框架等； b) 应对安全管理活动中重要的管理内容	根据安全管理制度的基本要求制定各类管理规定、管理办法和暂行规定。从安全策略主文档中规定的

要求类别		基本要求	解决方案
制度		建立安全管理制度； c） 应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。	安全各个方面所应遵守的原则方法和指导性策略引出的具体管理规定、管理办法和实施办法，是具有可操作性，且必须得到有效推行和实施的制度。 制定严格的制度制定与发布流程，方式，范围等； 定期对安全管理制度进行评审和修订，修订不足及进行改进。
	制定与发布	a） 应指定或授权专门的部门或人员负责安全管理制度的制定； b） 应组织相关人员对制定的安全管理制度进行论证和审定； c） 应将安全管理制度以某种方式发布到相关人员手中。	
	评审与修订	应定期对安全管理制度进行评审，对存在不足或需要改进的安全管理制度进行修订。	
安全管理机构	岗位设置	a） 应设立安全主管、安全管理各个方面的负责人岗位，并定义各负责人的职责； b） 应设立系统管理员、网络管理员、安全管理员等岗位，并定义各个工作岗位的职责。	根据基本要求设置安全管理机构的组织形式和运作方式，明确岗位职责； 设置安全管理岗位，设立系统管理员、网络管理员、安全管理员等岗位，根据要求进行人员配备，配备专职安全员； 建立授权与审批制度； 建立内外部沟通合作渠道； 定期进行全面安全检查，特别是系统日常运行、系统漏洞和数据备份等。
	人员配备	a） 应配备一定数量的系统管理员、网络管理员、安全管理员等； b） 安全管理员不能兼任网络管理员、系统管理员、数据库管理员等。	
	授权与审批	a） 应根据各个部门和岗位的职责明确授权审批部门及批准人，对系统投入运行、网络系统接入和重要资源的访问等关键活动进行审批； b） 应针对关键活动建立审批流程，并由批准人签字确认。	
	沟通与合作	a） 应加强各类管理人员之间、组织内部机构之间以及信息安全职能部门内部的合作	

要求类别		基本要求	解决方案
		与沟通； b） 应加强与兄弟单位、公安机关、电信公司的合作与沟通。	
	审核与检查	安全管理员应负责定期进行安全检查，检查内容包括系统日常运行、系统漏洞和数据备份等情况。	
人员安全管理	人员录用	a） 应指定或授权专门的部门或人员负责人员录用； b） 应规范人员录用过程，对被录用人员的身份、背景和专业资格等进行审查，对其所具有的技术技能进行考核； c） 应与从事关键岗位的人员签署保密协议。	根据基本要求制定人员录用，离岗、考核、培训几个方面的规定，并严格执行； 规定外部人员访问流程，并严格执行。
	人员离岗	a） 应规范人员离岗过程，及时终止离岗员工的所有访问权限； b） 应取回各种身份证件、钥匙、徽章等以及机构提供的软硬件设备； c） 应办理严格的调离手续。	
	人员考核	应定期对各个岗位的人员进行安全技能及安全认知的考核。	
	安全意识教育和培训	a） 应对各类人员进行安全意识教育、岗位技能培训和相关安全技术培训； b） 应告知人员相关的安全责任和惩戒措施，并对违反违背安全策略和规定的人员进行惩戒； c） 应制定安全教育和培训计划，对信息安全基础知识、岗位操作规程等进行培训。	
	外部人员	应确保在外部人员访问受控区域前得到授	

要求类别		基本要求	解决方案
	访问管理	权或审批，批准后由专人全程陪同或监督，并登记备案。	
系统建设管理	系统定级	a） 应明确信息系统的边界和安全保护等级； b） 应以书面的形式说明信息系统确定为某个安全保护等级的方法和理由； c） 应确保信息系统的定级结果经过相关部门的批准。	根据基本要求制定系统建设管理制度，包括：系统定级、安全方案设计、产品采购和使用、自行软件开发、外包软件开发、工程实施、测试验收、系统交付、安全服务商选择等方面。从工程实施的前、中、后三个方面，从初始定级设计到验收评测完整的工程周期角度进行系统建设管理。
	安全方案设计	a） 应根据系统的安全保护等级选择基本安全措施，依据风险分析的结果补充和调整安全措施； b） 应以书面形式描述对系统的安全保护要求、策略和措施等内容，形成系统的安全方案； c） 应对安全方案进行细化，形成能指导安全系统建设、安全产品采购和使用的详细设计方案； d） 应组织相关部门和有关安全技术专家对安全设计方案的合理性和正确性进行论证和审定，并且经过批准后，才能正式实施。	
	产品采购和使用	a） 应确保安全产品采购和使用符合国家的有关规定； b） 应确保密码产品采购和使用符合国家密码主管部门的要求； c） 应指定或授权专门的部门负责产品的采购。	
	自行软件开发	a） 应确保开发环境与实际运行环境物理分开；	

要求类别		基本要求	解决方案
		b） 应制定软件开发管理制度，明确说明开发过程的控制方法和人员行为准则； c） 应确保提供软件设计的相关文档和使用指南，并由专人负责保管。	
	外包软件开发	a） 应根据开发要求检测软件质量； b） 应确保提供软件设计的相关文档和使用指南； c） 应在软件安装之前检测软件包中可能存在的恶意代码； d） 应要求开发单位提供软件源代码，并审查软件中可能存在的后门。	
	工程实施	a） 应指定或授权专门的部门或人员负责工程实施过程的管理； b） 应制定详细的工程实施方案，控制工程实施过程。	
	测试验收	a） 应对系统进行安全性测试验收； b） 在测试验收前应根据设计方案或合同要求等制订测试验收方案，在测试验收过程中应详细记录测试验收结果，并形成测试验收报告； c） 应组织相关部门和相关人员对系统测试验收报告进行审定，并签字确认。	
	系统交付	a） 应制定系统交付清单，并根据交付清单对所交接的设备、软件和文档等进行清点； b） 应对负责系统运行维护的技术人员进行相应的技能培训； c） 应确保提供系统建设过程中的文档和指导用户进行系统运行维护的文档。	

要求类别		基本要求	解决方案
	安全服务商选择	a） 应确保安全服务商的选择符合国家的有关规定； b） 应与选定的安全服务商签订与安全相关的协议，明确约定相关责任； c） 应确保选定的安全服务商提供技术支持和服务承诺，必要的与其签订服务合同。	
系统运维管理	环境管理	a） 应指定专门的部门或人员定期对机房供配电、空调、温湿度控制等设施进行维护管理； b） 应配备机房安全管理人员，对机房的出入、服务器的开机或关机等工作进行管理； c） 应建立机房安全管理制度，对有关机房物理访问，物品带进、带出机房和机房环境安全等方面的管理作出规定； d） 应加强对办公环境的保密性管理，包括工作人员调离办公室应立即交还该办公室钥匙和不在办公区接待来访人员等。	根据基本要求进行信息系统日常运行维护管理，利用管理制度以及安全管理中心进行，包括：环境管理、资产管理、介质管理、设备管理、网络安全管理、系统安全管理、恶意代码防范管理、密码管理、变更管理、备份与恢复管理、安全事件处置、应急预案管理等，使系统始终处于相应等级安全状态中。
	资产管理	a） 应编制与信息系统相关的资产清单，包括资产责任部门、重要程度和所处位置等内容； b） 应建立资产安全管理制度，规定信息系统资产管理的责任人员或责任部门，并规范资产管理和使用的行为。	
	介质管理	a） 应确保介质存放在安全的环境中，对各类介质进行控制和保护，并实行存储环境专人管理； b） 应对介质归档和查询等过程进行记录，并根据存档介质的目录清单定期盘点；	

要求类别		基本要求	解决方案
		c） 应对需要送出维修或销毁的介质，首先清除其中的敏感数据，防止信息的非法泄漏； d） 应根据所承载数据和软件的重要程度对介质进行分类和标识管理。	
	设备管理	a） 应对信息系统相关的各种设备（包括备份和冗余设备）、线路等指定专门的部门或人员定期进行维护管理； b） 应建立基于申报、审批和专人负责的设备安全管理制度，对信息系统的各种软硬件设备的选型、采购、发放和领用等过程进行规范化管理； c） 应对终端计算机、工作站、便携机、系统和网络等设备的操作和使用进行规范化管理，按操作规程实现关键设备（包括备份和冗余设备）的启动/停止、加电/断电等操作； d） 应确保信息处理设备必须经过审批才能带离机房或办公地点。	
	网络安全管理	a） 应指定人员对网络进行管理，负责运行日志、网络监控记录的日常维护和报警信息分析和处理工作； b） 应建立网络安全管理制度，对网络安全配置、日志保存时间、安全策略、升级与打补丁、口令更新周期等方面作出规定； c） 应根据厂家提供的软件升级版本对网络设备进行更新，并在更新前对现有的重要文件进行备份；	

要求类别		基本要求	解决方案
		d） 应定期对网络系统进行漏洞扫描，对发现的网络系统安全漏洞进行及时的修补； e） 应对网络设备的配置文件进行定期备份； f） 应保证所有与外部系统的连接均得到授权和批准。	
	系统安全管理	a） 应根据业务需求和系统安全分析确定系统的访问控制策略； b） 应定期进行漏洞扫描，对发现的系统安全漏洞及时进行修补； c） 应安装系统的最新补丁程序，在安装系统补丁前，应首先在测试环境中测试通过，并对重要文件进行备份后，方可实施系统补丁程序的安装； d） 应建立系统安全管理制度，对系统安全策略、安全配置、日志管理和日常操作流程等方面作出规定； e） 应依据操作手册对系统进行维护，详细记录操作日志，包括重要的日常操作、运行维护记录、参数的设置和修改等内容，严禁进行未经授权的操作； f） 应定期对运行日志和审计数据进行分析，以便及时发现异常行为。	
	恶意代码防范管理	a） 应提高所有用户的防病毒意识，告知及时升级防病毒软件，在读取移动存储设备上的数据以及网络上接收文件或邮件之前，先进行病毒检查，对外来计算机或存储设备接入网络系统之前也应进行病毒检查；	

要求类别		基本要求	解决方案
		b） 应指定专人对网络和主机进行恶意代码检测并保存检测记录； c） 应对防恶意代码软件的授权使用、恶意代码库升级、定期汇报等作出明确规定。	
	密码管理	应使用符合国家密码管理规定的密码技术和产品。	
	变更管理	a） 应确认系统中要发生的重要变更，并制定相应的变更方案； b） 系统发生重要变更前，应向主管领导申请，审批后方可实施变更，并在实施后向相关人员通告。	
	备份与恢复管理	a） 应识别需要定期备份的重要业务信息、系统数据及软件系统等； b） 应规定备份信息的备份方式、备份频度、存储介质、保存期等； c） 应根据数据的重要性及其对系统运行的影响，制定数据的备份策略和恢复策略，备份策略指明备份数据的放置场所、文件命名规则、介质替换频率和数据离站运输方法。	
	安全事件处置	a） 应报告所发现的安全弱点和可疑事件，但任何情况下用户均不应尝试验证弱点； b） 应制定安全事件报告和处置管理制度，明确安全事件类型，规定安全事件的现场处理、事件报告和后期恢复的管理职责； c） 应根据国家相关管理部门对计算机安全事件等级划分方法和安全事件对本系统产生的影响，对本系统计算机安全事件进行	

要求类别		基本要求	解决方案
		等级划分； d） 应记录并保存所有报告的安全弱点和可疑事件，分析事件原因，监督事态发展，采取措施避免安全事件发生。	
	应急预案管理	a） 应在统一的应急预案框架下制定不同事件的应急预案，应急预案框架应包括启动应急预案的条件、应急处理流程、系统恢复流程、事后教育和培训等内容； b） 应对系统相关的人员进行应急预案培训，应急预案的培训应至少每年举办一次。	

8 项目管理

8.1 概述

基于电子病历的医院信息平台建设是一项复杂的系统工程，建设规模大、建设周期长、投资高，涉及到众多的硬件提供商和软件提供商以及众多的项目参与人员。为确保项目在规定的时间、规定的资源条件下实现建设目标，需要使用现代项目管理的理论和方法进行项目建设的管理。

本章节对医院信息化建设项目管理存在的问题进行分析，使用现代项目管理知识体系对基于电子病历的医院信息平台建设进行项目管理给出指导意见，供建设单位参考。

8.1.1 项目管理存在问题

8.1.1.1 管理意识问题

医院领导思想观念滞后于信息化。医院院长很多为医学方面的专家，他们在自己的学科领域具有深厚的造诣，也不乏领导及管理的能力。但是一些医院领导缺乏足够的信息化相关知识，信息化的理念停留在经验的认识与思考上。他们虽然开始接受信息化可以帮助医院更快地、更好地运行，可以增强综合竞争能力的观点，但对于医院信息化带来的崭新的观念、崭新的运作方式往往认识和准备不足，不愿放弃驾轻就熟的传统管理方式去改变现状。往往倾向于用信息技术来使原有手工的工作方式变得自动化，使用计算机来加快它们而不改进现有的工作流程。

医院在进行信息化建设时不注重项目管理，往往将项目管理的事情交给了承建商。各承建商各自管理项目的实施，没有统一组织、统一协调。由于没有对项目进行统一的管控，项目问题较多。

8.1.1.2 范围管理问题

信息资源战略职能定位存在偏差。医院领导往往把医院信息系统的建设和管理看成是信息部门的事，仅仅投入资金上系统并不能解决信息化的所有问题；没有花费足够的时间科学地论证信息资源战略，制订医院信息化建设近期、中期和长期的规划、方向和目标；存在一些急于求成，期望一步到位实现信息化的想法；企图“即插即用”，简单地把 IT 与医院信息化划等号。

由于没有进行统一的规划，导致在项目实施时不能明确项目范围，随着项目的进展往往随意调整项目范围，而项目的进度、成本、人力资源没有相应调整，导致项目质量不能符合要求。

8.1.1.3 需求管理问题

需求不明确，变更频繁。在项目初期没有进行详细的需求调研和需求分析导致需求不完整、不明确；在项目实施过程中，没有进行充分的论证而随意进行需求的变更，不断提出软件客户化的要求。由于没有对需求的变更进行严格的管理和控制，导致项目不能按期完成。

8.1.1.4 人才建设问题

信息部门的地位普遍不高。1995 年在医院等级评审中提出医院信息科(处)的建制，但不少信息部门仍隶属院长办公室管理,计算机室人员编制至今没有明确，人员编制偏少。

信息管理技术人才短缺。医院信息系统是涉及计算机技术与医院管理等多学科的边缘科学，它要求具有信息学、医学、工程学、管理学等多方面的知识。医院领导对于人员配备的重要性不够重视。信息部门技术力量薄弱，结构素质不全，很难找到复合型管理人员或组合型技术人员，几乎全部为单一计算机专业或医学专业人员。

信息人员待遇偏低。不少医院把信息管理技术人员作为后勤人员来对待。他

们的薪酬往往低于医务人员，与 IT 公司技术人员相差尤为悬殊。在获得技术职称、继续教育方面也有很多不便。

企业三驾马车之一的高级信息主管(Chief Information Officer, CIO)制度在医院尚未建立。由于医院信息系统的复杂性和各种问题，信息人员经常加班加点，而且时常面对来自各方面的压力。责任与待遇分离，很难吸引或留住适合医院信息管理的高级人才。

8.1.2 项目管理的重要性

无论是小项目还是大项目，在项目进展过程中必须对项目进行管理和控制。通过项目管理可以很好的控制项目范围、项目进度、项目成本以及项目质量的平衡关系，确保项目的成功。从国外国内项目管理的经验来看，进行有效的项目具有以下意义：

- ✓ 有效控制项目范围：通过项目范围计划管理、项目范围确认等手段对项目范围进行控制，可以把握项目总体目标，有效控制需求变化，使项目的范围控制在合理范围内。
- ✓ 确保项目实施进度：通过制定项目进度计划，将项目任务进行细化，可以减少对任务进度控制的难度，减少因某项目任务的延期而导致项目整体延期。
- ✓ 有效控制项目成本：通过项目成本估算、项目成本预算可以比较准确的预测项目的成本、保证项目资金的筹集，在项目过程中通过对实际发生成本的监控及修正达到有效控制项目成本的目的。
- ✓ 可以确保项目质量：通过项目的质量计划及质量控制可以在项目的整个生命周期对项目的质量、产品的质量进行有效的控制，提高项目质量和效益。
- ✓ 加强项目团队合作：按照项目人力资源管理、项目沟通管理的理论和方法，进行项目团队建设，通过合理有效的激励机制，增强团队合作精神，提高项目组成员的工作积极性和工作效率。
- ✓ 降低项目潜在风险：通过制定项目风险管理计划，对项目风险进行分析、提前做好风险规避或风险缓解措施，使项目的风险降低到最小限度，或者将已发生风险对项目进度、成本、质量的影响降低到最小限度。

8.1.3 项目管理基本内容

8.1.3.1 项目管理基本概念

项目：是为创造独特的产品、服务或成果而进行的临时性工作。项目具有明确的起点和终点。当项目目标达成时，或当项目因不会或不能达到目标而中止时，或当项目需求不复存在时，项目就结束了。

项目管理：是将知识、技能、工具与技术应用于项目活动，以满足项目的要求。即从项目开始到项目结束整个生命周期进行计划、组织、指挥、协调、控制和评价，以实现项目的目标。

项目经理：是执行组织委派其实现项目目标的个人，是项目的执行者和管理者，负责从项目启动到项目结束的整个项目过程的管理。

项目管理办公室（PMO）：是负责对所辖各项目进行集中协调管理的一个组织部门。PMO 的职责可涵盖从提供项目管理支持到直接管理项目。

8.1.3.2 项目管理发展历程

从二十世纪 40 年代中期到 60 年代，项目管理主要应用于国防工程建设和工民建工程建设。传统项目管理方法主要致力于项目预算、规划和为达到特定目标而借用的一些运营管理的方法，在相对较小的范围内所开展的一种管理活动。

从 60 年代起，建立起两大国际性项目管理协会，即：以欧洲为主的国际项目管理协会（International Project Management Association，IPMA）和以美国为首的美国项目管理协会（Project Management Institute，PMI）以及各国相继成立的项目管理协会，为推动项目管理的发展发挥了积极的作用、做出了卓越的贡献。

80 年代之后项目管理进入现代项目管理阶段，项目管理的应用领域在这一阶段也迅速扩展到社会生产与生活的各个领域和各行各业，并且在企业的战略发展

和日常经营中起到越来越重要的作用。

8.1.3.3 项目管理知识体系

美国项目管理学会（PMI）在 PMBOK 中把项目管理划分为 5 大过程组、9 大知识领域，一共 42 个过程。

5 大过程组如下：

1. 启动过程组：获得授权，定义一个新项目或现有项目的一个新阶段，正式开始该项目或阶段的一组过程。
2. 规划过程组：明确项目范围，优化目标，为实现目标而制定行动方案的一组过程。
3. 执行过程组：完成项目管理计划中确定的工作以实现项目目标的一组过程。
4. 监控过程组：跟踪、审查和调整项目进展与绩效，识别必要的计划变更并启动相应变更的一组过程。
5. 收尾过程组：为完结所有过程组的所有活动以正式结束项目或阶段而实施的一组过程。

9 大过程知识体系如下：

1. 项目范围管理：是为了实现项目的目标，对项目的工作内容进行控制的管理过程。它包括范围的界定，范围的规划，范围的调整等。
2. 项目时间管理：是为了确保项目最终的按时完成的一系列管理过程。它包括具体活动界定，活动排序，时间估计，进度安排及时间控制等项工作。很多人把 GTD 时间管理引入其中，大幅提高工作效率。
3. 项目成本管理：是为了保证完成项目的实际成本、费用不超过预算成本、费用的管理过程。它包括资源的配置，成本、费用的预算以及费用的控制等工作。
4. 项目质量管理：是为了确保项目达到客户所规定的质量要求所实施的一系列管理过程。它包括质量规划，质量控制和质量保证等。

5. 人力资源管理：是为了保证所有项目关系人的能力和积极性都得到最有效地发挥和利用所做的一系列管理措施。它包括组织的规划、团队的建设、人员的选聘和项目的班子建设等一系列工作。
6. 项目沟通管理：是为了确保项目信息的合理收集和传输所需要实施的一系列措施，它包括沟通规划，信息传输和进度报告等。
7. 项目风险管理：涉及项目可能遇到各种不确定因素。它包括风险识别，风险量化，制订对策和风险控制等。
8. 项目采购管理：是为了从项目实施组织之外获得所需资源或服务所采取的一系列管理措施。它包括采购计划，采购与征购，资源的选择以及合同的管理等项目工作。
9. 项目集成管理：是指为确保项目各项工作能够有机地协调和配合所展开的综合性和全局性的项目管理工作和过程。它包括项目集成计划的制定，项目集成计划的实施，项目变动的总体控制等。

42 个项目管理过程与项目管理过程组、项目管理知识领域的对应关系见下表：

表 8-1 项目管理过程组与知识领域表

知识领域	项目管理过程组				
	启动过程组	规划过程组	执行过程组	监控过程组	收尾过程组
项目整合管理	制定项目章程	制定项目管理计划	指导与管理项目执行	监控项目工作 实施整体变更控制	结束项目或阶段
项目范围管理		收集需求 定义范围 创建工作分解结构		核实范围 控制范围	
项目时间管理		定义活动 排列活动顺序估算活动资源估算活动持续时间 制定进度计划		控制进度	
项目成本管理		估算成本		控制成本	

		制定预算			
项目质量管理		规划质量	实施质量保证	实施质量控制	
项目人力资源管理		制定人力资源计划	组建项目团队 建设项目团队 管理项目团队		
项目沟通管理	识别干系人	规划沟通	发布信息 管理干系人期望	报告绩效	
项目风险管理		规划风险管理 识别风险 实施定性风险分析 实施定量风险分析 规划风险应对		监控风险	
项目采购管理		规划采购	实施采购	管理采购	结束采购

8.2 启动阶段

8.2.1 项目招标

8.2.1.1 编制采购计划

基于电子病历的医院信息平台建设项目采购是一项复杂的工作，涉及到不同的软件和硬件以及不同的厂商，需要考虑如何采购、采购什么、采购多少、采购时机、所采购产品和服务的质量及性能指标、当前价格、市场供求情况等因素，根据项目的进度计划和资源计划编制出详细可行的项目采购计划。

项目采购计划应该包括以下内容：

✧ 项目采购工作总体安排

- ✧ 确定采购所用合同类型
- ✧ 确定项目采购估价办法
- ✧ 确定项目采购工作责任
- ✧ 项目采购文件的标准化
- ✧ 资源供应商的管理方法
- ✧ 确定采购协调工作办法

8.2.1.2 编制采购合同

为了保证采购计划的有效性，按时、高质量的获得硬件、软件或服务资源，必须制定出项目的招标计划。

合同编制过程包括准备招标所需要的文件和确定合同签订的平等标准的过程，包括何时开标、选择供方、签订合同，以确保采购的各种产品和服务能够在项目进展需要及时到位。

- ✧ 编写招标文件：请求建议书（RFP）或请求报价单（RFQ）。
- ✧ 编写评估标准：用来对建议书或投标书进行评级和打分。评估标准一般包括以下内容：
  - ✓ 产品价格：硬件或软件厂商提供的产品或服务的价格。
  - ✓ 技术能力：硬件或软件厂商是否具有或能够获得所需的技能和知识。
  - ✓ 管理方式：硬件或软件厂商是否具有或能够制定出一套确保项目成功的管理过程。
  - ✓ 技术方案：硬件或软件厂商所提议的技术方法、解决方案和服务是否符合采购文件需求。
  - ✓ 财务能力：硬件或软件厂商是否具有或能够获得所需的财务能力。
  - ✓ 对需求的理解：硬件或软件厂商建议书中对合同说明书的重视程度。
  - ✓ 生产能力和兴趣：硬件或软件厂商是否有能力和兴趣以满足将来的潜在需求。

8.2.1.3 项目采购招标

基于电子病历的医院信息系统项目建设投资规模巨大，必须按照招投标管理办法进行软件、硬件的招标，项目招标流程如下：

1）确定招标人或招标组织者

2）准备招标通知书和招标文件

3）招标公告或招标邀请

4）投标者的资格审查和通知

5）投标文件编写与投标和交保证金

6）询标、开标和评标

7）中标和不中标的通知

8）中标后开展的合同谈判

8.2.2 组织建设

基于电子病历的医院信息平台建设是一项复杂的系统工程，涉及到项目建设方、项目承建方及项目监理方的各种资源，因此建立一套健全有效的组织保障体系是项目管理及项目成功实施的必要条件和保障措施。在组织保障建设中因考虑以下原则：

- 项目组需要建设方、承建方、监理方共同参与，项目组织结构图参见图8-1。
- 成立以医院院长为组长的项目领导小组，负责项目的领导及资源调配，项目领导小组人员及职责参见表8-2。
- 成立以信息中心主任为项目经理的项目执行小组，负责项目的实施及管理，项目执行小组人员及职责参见表8-3。

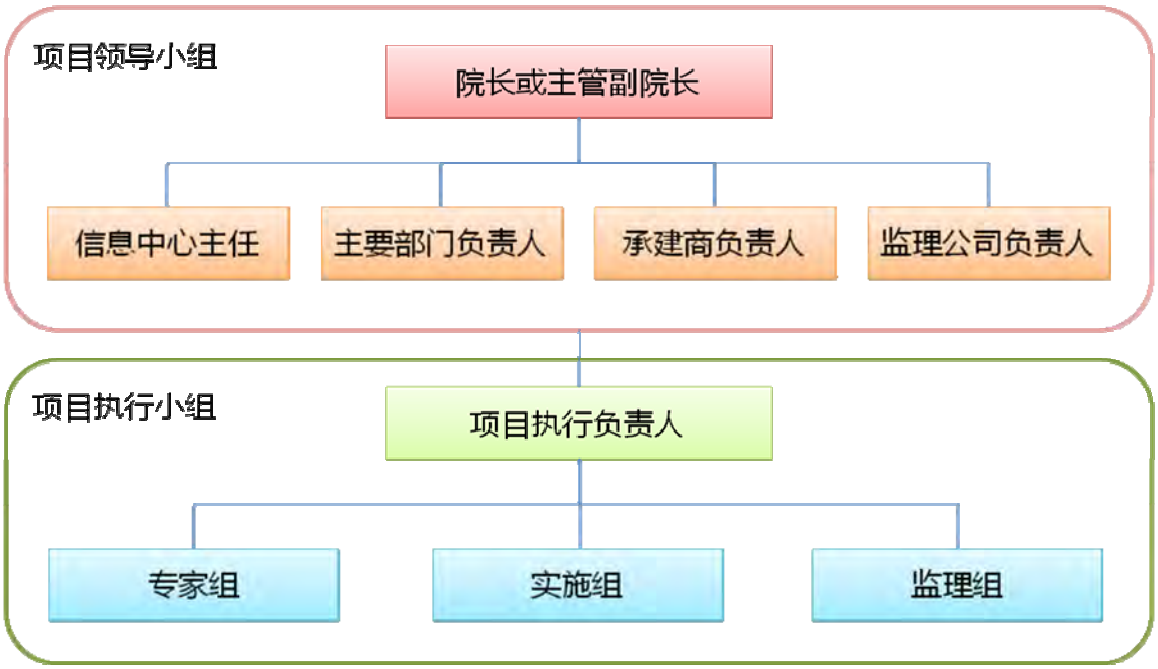


图 8-1 项目组织结构图

表 8-2 项目领导小组人员及职责

类别	人员组成	职责
组长	院长或主管副院长	负责项目的总体控制和管理 负责重大问题的决策和处理 负责项目的资源调配与管理 负责项目计划的审核与确认
组员	信息中心主任	负责项目计划的制定与执行 负责项目协调会议的召集与主持 负责业务流程与应用模式的确认
	主要部门负责人（如财务科、医务科、护理部、设备科等科室负责人）	负责项目所涉及各科室人员的协调
	承建单位负责人	负责承建单位人员的调配及协调
	监理公司负责人	负责监理工程师的协调及资源调配

表 8-3 项目执行小组人员及职责

类别	人员组成	职责

项目执行负责人	信息中心主任	负责项目计划的制定，项目全程管理 负责项目组成员的日常管理与考核
专家组	业务专家、技术专家，可外聘	业务指导、技术指导、阶段工作评审及把关
执行组	信息中心/信息科软硬件工程师 承建厂商项目团队	网络安装、调试、管理及硬件安装、调试、管理 需求调研、需求分析、需求管理 软件开发、客户化修改、技术支持 系统管理员、操作人员的培训 项目实施前的数据准备 项目实施时的现场指导 项目过程质量和产品质量的审计、监控项目管理文档、技术文档、程序版本配置管理
监理组	监理公司监理工程师	质量控制、投资控制、进度控制、变更控制、合同管理、信息管理、安全管理、沟通协调

8.2.3 制度建设

为了保证项目的顺利进行，需要制定各项管理制度，建设单位、承建单位及监理单位各方人员共同遵守，需要建立的管理制度包括以下方面：

- ◆ 日常管理制度：日常的工作要求，劳动纪律等。
- ◆ 项目汇报制定：项目工作日常汇报及重大问题汇报内容、汇报流程。
- ◆ 项目例会制定：确定项目例会的时间、频度、参与人员及会议要求。
- ◆ 需求管理制度：需求调研、需求管理、需求变更、需求跟踪的的流程及规范。
- ◆ 培训考核制度：培训及考核管理。

8.2.4 项目启动

基于电子病历的医院信息系统建设需要医院各个科室或部门人员的参与，因此在项目启动时就应该让所有的人员了解项目的情况。通过召开项目启动会，让各科室负责人向医院所有员工传达项目建设的目的、项目建设的内容、项目建设的周期、项目建设的效果以及在项目建设过程中需要员工配合的工作，使医院所有员工提前了解项目的概况，为项目的顺利实施打下基础。

项目启动会应由院领导主持召开，各科室主任、副主任、护士长等部门负责人以及项目承建单位、监理公司代表参加。

在项目启动会上由院领导介绍项目总体情况并进行全员动员，承建单位、监理单位介绍公司情况、参与项目人员情况及各自承担的工作内容，项目负责人介绍项目详细情况及工作计划。项目启动会结束后要求形成《项目启动会备忘录》，备忘录包括的内容：项目启动会召开时间、地点、人员、各项目小组负责人员及联系方式、院方提出的问题或建议、系统上线的时间或者安排、是否需各承担单位帮助解决的问题；备忘录由建设单位、承建单位、监理单位负责人员签字备案。

8.3 实施阶段

基于电子病历的医院信息平台建设是一项宏大而复杂的系统工程。随着医疗市场和 IT 技术的不断发展和变化，加大了项目建设的周期和复杂性。为了保证前后衔接，避免脱节和重复投资，造成人力、财力、物力的浪费，需要在项目实施中把握以下原则：

- ✧ 整体规划：任何一个信息系统的建设都不可能是一蹴而就，更何况基于电子病历的医院信息平台建设是一项非常庞大，复杂，长期的系统工程。需要先做一个整体的规划，无论从战略上或从战术上，从软硬件系统上都必须先进行整体的调研和规划，才能为后续的建设指明道路和打下基础。
- ✧ 分步实施：基于电子病历的医院信息平台建设过程是一个长期的过程，必须分成多个阶段来完成，以保证项目建设的可行性和可控性。因此必须在总体

规划的指导下，对整个项目科学地划分多个实施阶段，逐步完成各项工程的建设。

- ✧ 成熟先行：基于电子病历的医院信息平台建设包含了各种各样的产品，而各种产品又是在不断发展和完善的。医院的业务和流程也在不断的完善过程中。因此在建设时，不能冒进和盲目跟风，需要根据医院实际情况，选择成熟实用的产品或系统，从系统的底层一步步做起，减少系统建设的风险和浪费。

在项目实施阶段需要制定详细的项目计划，并按计划执行。在执行的过程中对项目进行监控，根据项目管理理论本章节从项目范围、时间、成本、质量、人力资源、沟通及风险等方面如何进行管理进行阐述，供项目建设各方参考。

8.3.1 项目范围管理

8.3.1.1 范围管理计划

制定项目范围管理计划，可以确保项目包含且只包含达到项目成功所需完成的工作。范围计划需要对项目范围进行定义、确认和控制，并制定工作任务分解结构（WBS）。范围管理计划应当包括以下内容：

- ◆ 基于电子病历的医院信息平台建设项目范围说明书。
- ◆ 基于电子病历的医院信息平台建设项目任务分解（WBS）。
- ◆ 基于电子病历的医院信息平台建设项目管理文档和技术文档清单。
- ◆ 基于电子病历的医院信息平台建设项目范围变更申请和处理流程。

8.3.1.2 项目范围控制

在项目进行过程中对项目的范围进行管理、需要对项目的范围进行确认，对范围的变更进行控制，保证项目范围的变更控制在最小的限度。

项目范围确认是指项目利益相关者（项目业主/客户、项目发起人、项目委托人、项目组织等），对于项目范围的正式认可和接受的工作过程。范围确认在

每个项目生命周期收尾阶段进行，此外，在项目执行中的过渡项目可交付成果也应被确认。所有的项目利益相关者都应当确认项目范围，知道项目的范围是什么，项目将要提交的是什么。

基于电子病历的医院信息平台建设项目范围的具体内容请参见第 5 章，各建设单位可按实际情况进行调整。

范围变更控制是指对于项目的目标、产出物和工作的全面控制。由于项目条件和环境的变化会使项目范围发生变动，并造成项目工期、成本或质量等的改变，所以必须对项目范围变更进行严格的控制。根据项目范围管理计划、项目工作分解结构以及项目范围变更的要求对项目范围的变更进行控制，项目范围变更控制工作包括以下内容：

- ✧ 分析和确定影响项目范围变动的因素和环境条件。
- ✧ 管理和控制那些能够引起项目范围变动的因素和条件。
- ✧ 分析和确认各方面提出的项目变动要求的合理性和可行性。
- ✧ 分析和确认项目范围变动是否已发生，以及这些变动的风险和内容。
- ✧ 当项目范围变动发生时，对其进行管理和控制，设法使这些变动朝有益的方向发展，努力消除项目范围变动的不利影响。

8.3.2 项目时间管理

8.3.2.1 项目进度计划

项目时间管理也叫项目进度管理，是项目按时完成的重要管理过程。在制定项目进度计划时要把人员的工作量与花费的时间联系起来，合理分配工作量，利用进度安排的有效分析方法严密监控项目的进展情况，使项目的进度不致被拖延。项目进度计划包括活动定义、活动排序，活动资源估算、活动工期估算。项目进度计划建议采用软件工具进行编制。

基于电子病历的医院信息平台建设内容多、工期长，所以在制定项目计划时

需要制定阶段里程碑，将项目分期建设，以控制项目的风险。建议分以下几个阶段进行建设：

- ✧ 第一阶段：基本业务的数字化，该阶段的目标主要是实现基本业务数字化，以患者服务和医院经济核算为中心，优化业务流程，提高服务质量和工作效率。
- ✧ 第二阶段：医疗与护理的数字化，该阶段的主要任务实现临床管理信息化，以电子病历为核心，实现临床信息的全面整理，规范业务流程，保证医疗质量，提高医护人员工作效率。
- ✧ 第三阶段：管理办公数字化，该阶段的建设以加强管理、辅助决策为目标，完成医院行政部门和其它业务系统的集成和融合，实现全院的办公自动化，建立院内电子知识库，实现知识管理与知识共享，建立医院数据仓库，实施基本的决策分析和数据挖掘。
- ✧ 第四阶段：面向社会的数字化，该阶段以实现社会信息资源共享为目标，建立医院外部网站，对外发布信息和患者自助服务，实现与区域平台的联网，逐步实现区域信息共享，实现远程会诊，远程护理等。
- ✧ 第五阶段：知识利用和创新阶段，该阶段的建设以临床数据深度挖掘，知识创新为目标，建立各学科专科的应用系统，建立完善的医学知识库系统和临床路径，临床指南系统，根据医学发展情况的其他临床支持系统。

8.3.2.2 项目进度控制

项目进度控制是依据项目进度计划对项目的时间进展进行控制，使项目能够按时完成。有效项目进度控制的关键是监控项目的实际进度，及时、定期的将实际进度与项目计划进行比较，对项目进度发生偏差时采取必要和有效的纠正措施。在项目进行过程中需要定期召开项目例会，通过项目例会了解项目进展情况，并对项目进度进行控制，项目进度控制的步骤如下：

- ✧ 分析进度，找出哪些地方需要采取纠正措施。
- ✧ 确定应采取哪种具体纠正措施。

- ✧ 修改计划，将纠正措施列入计划。
- ✧ 重新计算进度，估计计划采取的纠正措施的效果。

8.3.3 项目成本管理

项目成本管理是项目管理重要组成部分，是在项目实施过程中，为了保证完成项目所花费的实际成本不超过预算成本而展开的项目成本估算、项目预算编制和项目成本控制等方面的管理活动。在项目计划阶段主要进行成本估算和成本预算，在项目执行过程中需要进行项目成本控制。

8.3.3.1 项目成本计划

在制定项目成本计划中需要进行成本估算和成本预算。

- ✧ 成本估算：完成项目各活动所需要的资源成本近似估算。成本估算的步骤：
  - ✓ 识别并分析项目成本的构成科目，即项目成本中所包括的资源或服务的类别，比如人力费、硬件费、软件费、集成费等。
  - ✓ 根据已识别的项目成本构成科目，估算每一成本科目的成本大小。
  - ✓ 分析成本估算结果，找出各种可以相互替代的成本，协调各种成本之间的比例关系。
- ✧ 成本预算：将总的成本估算分配到各项子活动或工作任务中，建立成本基线。成本预算步骤：
  - ✓ 分摊项目总成本到项目工作分解结构的各个工作包中，为每个工作包建立预算成本。子包预算成本合计不超过总包总预算成本。
  - ✓ 将每个工作包的预算成本再分配到各项活动上。
  - ✓ 确定各项成本预算支出的时间计划以及每一时间点对应的累计预算成本，制定项目成本预算计划，为资金的配置、合同付款提供依据。

8.3.3.2 项目成本控制

项目成本控制是项目组织为保证在变化的条件下实现其预算成本，按照事先

拟定的计划和标准，通过采用各种方法，对项目实施过程中发生的各种实际成本与计划成本进行对比、检查、监督、引导和纠正，尽量使项目的实际成本控制在计划和预算范围内。随着项目的进展，根据项目实际发生的成本，不断修正原先的成本估算和成本预算。项目成本控制涉及对于各种能够引起项目成本变化因素的控制（事前控制），项目实施过程的成本控制（事中控制）和项目实际成本变动的控制（事后控制）三个方面。项目成本控制具体包括以下内容：

- ✧ 识别可能引起项目成本发生变化的因素，采取措施，使成本变化朝有利的方向发展。
- ✧ 以工作包为单位、监督成本实施情况，分析成本偏差原因，做好实际成本评估工作。
- ✧ 对发生变化的工作包进行管理，采取有针对性达到纠正措施，用以降低成本偏差率。
- ✧ 当成本变化后，应将核准的成本变更和调整后的成本基准计划通知项目的相关人员。
- ✧ 防止不正确的、不合适的或未经授权的项目变动所发生的费用被列入项目成本预算。
- ✧ 在进行成本控制的同时，应该与项目范围变更、进度计划变更、质量控制等相结合。

8.3.4 项目质量管理

项目质量管理过程包括执行组织关于确定质量方针、目标和职责的所有活动，使得项目可以满足其需求。它通过质量计划、质量保证、质量控制程序和过程以及连续的过程改进活动实施来实现项目质量管理。

- ✧ 质量计划：确定适合于项目的质量标准并决定如何满足这些标准。
- ✧ 质量保证：用于有计划、系统的质量活动，确保项目中所有过程满足项目期望。
- ✧ 质量控制：监控具体项目结果以确定其是否符合相关质量标准，制定有

效方案，消除产生质量问题的原因。

8.3.4.1 质量管理计划

质量管理计划应该描述项目质量体系即组织结构、职责、程序、工作过程以及建立质量管理所需要的资源。质量管理计划为项目提出质量控制、质量度量、质量检查和项目持续改进方面的措施。通过阶段评审减少缺陷，降低成本和减少由于返工引起的进度拖延。

8.3.4.2 项目质量控制

为了保障项目的产出物，能够满足项目业主/客户以及项目各利益相关者的需要,需要开展对项目产出物的质量和项目工作质量的质量保证和质量控制工作。

在执行项目质量计划过程中，需要经常性地对整个项目质量计划执行情况进行评估、核查和改进，项目质量保障主要工作内容如下：

- ✧ 制定清晰的质量要求说明
- ✧ 制定科学可行的质量标准
- ✧ 制定组织建设项目质量体系
- ✧ 配备合格和必要的资源，要求项目组配备专职的 QA 人员
- ✧ 持续开展有计划的质量改进活动
- ✧ 对于项目的变更进行全面的控制

项目质量控制是指对于项目质量实施过程的监督和管理工作，项目质量的事前控制、事中控制和事后控制。项目质量控制包括以下两个方面：

- ✧ 项目产品或服务质量控制：检查平台软硬件产品的规格是否符合需求的标准，消除因不符合要求产生的任何影响。
- ✧ 项目管理过程的质量控制：通过项目审计将管理过程的作业与标准实践进行比较，对不符合要求的进行改进。

8.3.5 人力资源管理

项目人力资源管理是指对于项目的人力资源所开展的有效规划、积极开发、合理配置、准确评估、适当激励等方面的管理工作。

为了提高项目团队成员之间的个人技能，提高他们完成项目活动的能力，提高项目团队成员之间的信任感和凝聚力和团队合作精神以提高工作效率在项目建设的过程中需要对项目团队进行建设。项目团队建设可采用以下方式：

- ✧ 提供培训：基于电子病历的医院信息平台会涉及到很多新的技术、新的产品，通过培训提高项目团队综合素质、工作技能和绩效，提高项目团队成员工作满意度。
- ✧ 绩效考核：项目建设各方需要建立内部绩效考核机制，通过对团队成员工作绩效的考察与评价，反映团队成员的实际能力和业绩。
- ✧ 项目激励：通过项目激励激发团队成员的行为动机和潜能，为实现项目的目标服务。

8.3.6 项目沟通管理

项目沟通管理是指对于项目过程中各种不同方式和不同内容的沟通活动的管理。这一管理的目标是保证有关项目的信息能够适时、以合理的方式产生、收集、处理、贮存和交流。沟通要掌握准确性、完整性和及时性原则。为保证沟通的有效性需要采取以下方式：

- ✧ 制定项目沟通协调计划，明确建设单位、承建单位、监理单位负责人负责项目小组间以及小组内部的沟通与协调。
- ✧ 制定项目工作汇报制度，明确工作汇报的时间及汇报内容。
- ✧ 建议承建单位、监理单位负责人列席医院每周办公会议，简要汇报项目进展情况及需院方协调的工作。
- ✧ 定期召开项目例会，提前拟定会议议程并分发给相关人员，以便参会人员提前准备，提高会议效率。会议结束后，由专人记录会议内容并分发

给相关人员。

- ✧ 定期提交项目工作进展报告，总结本期工作内容、安排下期工作任务，并提出项目中的问题、解决方案及需要沟通协调的事宜。
- ✧ 根据项目的需要不定期召开各类专题会议，及时解决项目中存在的问题。
- ✧ 阶段里程碑结束后召开里程碑评审会议，总结经验教训。

8.3.7 项目风险管理

项目风险是指由于项目所处的环境和条件本身的不确定性和项目业主/客户/项目组织或项目其他相关利益主体主观上不能准确预见或控制的影响因素，使项目的最终结果与项目相关利益主体的期望产生背离，并存在给当事者带来损失的可能性或带来机遇的可能性。

为了减少风险对项目带来的危害和损失，在项目过程中必须对风险进行管理。风险管理包括制定风险计划、对风险进行识别、度量及控制。风险管理计划应该描述如何识别风险、如何对风险进行定性和定量的分析、采取何种方式应对风险并对风险进行监视和控制。对项目风险识别的和度量应当贯穿于项目实施全过程，并在整个项目过程中根据项目风险管理计划和项目实际发生的风险与变化，开展项目风险控制活动。

基于电子病历的医院信息平台建设过程中会出现各种各样的风险，对于这些风险需要提前识别并制定相应的应对措施，下面简单列举可能在项目建设过程中出现的风险以及应对措施，供建设单位参考：

- ✧ 人力资源风险
  - ✓ 风险：项目领导小组或项目执行小组人员发生变动；项目执行小组人员缺乏或技术水平不够
  - ✓ 措施：成立以医院院长/主管副院长、各承建单位负责人为核心的项目领导小组，保证人力资源配合合理；在与承建单位签订合同时要求提供各阶段核心人员名单并保持人员的稳定。
- ✧ 项目范围风险

- ✓ 风险：项目目标和范围不清晰，项目过程中随意调整或扩大项目范围
- ✓ 措施：项目立项前进行项目可行性研究及项目论证，明确项目范围

✧ 需求变更风险

- ✓ 风险：需求调研、需求分析不充分，需求不完整、不明确，经常变更
- ✓ 措施：进行详细的需求调研和需求分析，对需求进行评审，各方签字确认，对于需求的变更按照变更流程执行。

✧ 团队合作风险

- ✓ 风险：各承建单位或项目组成员各自为政，缺乏有效沟通和合作
- ✓ 措施：明确各方的责、权、利，定期进行沟通和交流。

8.4 收尾阶段

8.4.1 项目验收

在项目阶段结束或项目整体结束的时候需要对项目进行验收，项目验收需要满足以下标准：

- ✧ 确认项目已经满足了所有需求。
- ✧ 确认已经达到所有的完工标准和退出准则。
- ✧ 为满足项目或阶段的完工或退出准则所需要的活动或措施已被实施。
- ✧ 验证所有的项目可交付物已经提供并被接受。项目应该提交的可交付物参考下表：

表 8-4 项目交付物参考清单

文档类别	文档名称
管理	项目章程
	项目范围说明书
	项目管理计划
	范围管理计划
	成本管理计划
	进度管理计划
	资源管理计划
	沟通管理计划
	风险管理计划

	项目变更报告
	项目会议纪要
	项目验收报告
	风险管理计划
	风险管理报告
工程	可行性研究报告
	需求规格说明书
	概要设计说明书
	详细设计说明书
	测试用例
	测试报告
	用户手册
	操作手册
	程序源代码
	需求变更单
	培训资料
	培训记录
支撑	配置管理计划
	配置管理报告
	质量管理计划
	质量审计报告

8.4.2 项目评估

项目完工后需要对项目的绩效进行评估。主要对项目的水平、效果和影响，投资使用的合同相关性、目标相关性、经济合理性等方面进行全面的评价。项目评估可由建设单位自评或者委托专业机构进行评估。项目评估主要包括信息技术评估和应用效果评估。

信息技术评估指标参照下表：

表 8-5 信息技术评估指标

序号	评估指标	说明
1	完整性	对于关键性数据资源的关键应用采用两段式体检协议，通过授权，保存数据更新的同步及一致性。其它子系统数据采用异步的存储-转发技术

2	安全性	系统通过用户鉴别、分组授权、存取控制等实现数据安全
3	可靠性	系统采用分布式数据库系统，在网络高可靠性的条件下，与有故障时自动恢复到故障点，保存系统业务处理及数据完整
4	易用性	系统通过简单、友好的人机界面实现人机对话，便于操作、维护
5	灵活性	采用控件技术确保应用系统是一个标准灵活的基础结构
6	扩展性	应用系统建立在安全可靠的大型数据库上，网络结构主干为千兆、百兆到桌面。网络连接核心部件模块化，便于功能扩展
7	适应性	应用软件能够适应市场、业务以及用户的需求的不断变化
8	高效性	系统应有快速的响应时间，可以保证消息和数据得到及时、有序的传递及存储
9	易开发	应用系统的开发技术组件化、简便易行，方便开发维护人员对应用系统进行维护、修改及完善
10	可管理	对于应用程序、数据以及系统的管理采用 2/8 原则，已服务器管理为核心，监控系统运行状况
11	互操作	对于异构的应用程序之间通过一套简单的界面实现数据通讯
12	数据分布	系统可以根据需要通过多种途径将数据传递至不同的目的地

应用效果评估主要包括经济效益评估和管理效益评估：

- ✧ 经济效益评估：通过项目建设带来了哪些经济效益。
- ✧ 管理效益评估：通过项目建设是否优化了管理流程、提高了运行效率、减少了管理成本。是否搭建了适应医院长远发展的信息化平台，使医院管理理念和管理模式迈上了新的台阶。通过项目建设是否有利于医院在管理、控制、组织、协调、决策等方面的综合效率得到了提高。

8.5 项目监理

根据《信息系统工程监理暂行规定》，信息系统工程监理师职依法设立且具备相应资质的信息系统工程监理单位，受建设单位委托，依据国家有关法律法规。技术标准和信息系统工程监理合同，对信息系统工程项目实施监督管理。

监理的主要内容为“四控三管一协调”。其中“四控”是指质量控制、投资控制、进度控制、变更控制;“三管”是指合同管理、信息管理和安全管理;“一协调”是指沟通协调，起到建设单位和承建单位之间沟通和协调的桥梁作用。

监理单位协助建设单位制定项目的总体规划和技术方案，以及设备选型方案。监理单位应对整个工程实施的进度、质量、费用以及合同进行监督。

项目建设单位可直接委托监理单位承担项目建设的监理工作，也可以采用招标方式选择监理单位。若采用招标的方式建设单位应当与监理单位签订监理合同，监理合同需要包括以下内容：

- ✧ 监理业务内容;
- ✧ 双方的权利和义务;
- ✧ 监理费用的计取和支付方式;
- ✧ 违约责任及争议的解决方法;
- ✧ 双方约定的其他事项。

监理单位按照以下程序对项目建设进行监理：

1）组建信息系统工程监理机构。监理机构由总监理工程师、监理工程师和其他监理人员组成;

2）编制监理计划，并与业主单位协商确认;

3）编制工程阶段监理细则;

4）在整个项目过程中实施监理;

5）参与项目工程验收并签署监理意见;

6）监理业务完成后，向业主单位提交最终监理档案资料。

9 运维管理

9.1 医院 IT 环境分析

9.1.1 信息技术发展给医院带来的挑战

随着时代的发展和中国的入世，医院信息化管理已成为衡量医院管理水平的标准之一，信息化管理已逐渐进入医疗卫生领域。根据中国卫生部的数据，目前全国有超过 90%的医院在信息化建设方面有不同程度的投入，有 40%的大中型医院尤其重视信息化建设，投入力度更大。即便如此，与信息化投入占医院总收入 2%～4%的国际惯例相比，中国医院差距甚大，平均仅有 0.1%左右。

不同于别的行业，医院信息化不能止步于内部应用。按照目前国内外普遍认同的划分方法，医院信息化一般要经历三个阶段：以人财物为中心的医院管理信息系统、以病人为中心的临床信息系统、以社区服务为中心的局域医疗卫生服务体系。

这些综合信息管理系统建立确保了医院信息化建设的正常开展，但如此多的系统如何有效管理成为医疗信息化的新课题，只有让众多综合信息系统良好运行才能保障医院正常提供各项医疗服务。随着 IT 技术的高速发展，医院信息化建设从基础网络建设，应用系统建设，逐步进入了一个应用和网络融合发展，网络和应用系统复杂度和规模不断成熟和扩大的时期，迫切需要通过有效地科学的管理，通过充分发挥历年建设的 IT 基础设施的作用，体现出 IT 技术能够推动组织的对外服务水平，不断提升服务质量从而为医院带来巨大效益。

9.1.2 医院 IT 环境的复杂性及其问题

目前我国的医疗信息化正处在立足于医院管理信息系统，并向以病人为中心的临床信息系统发展的阶段，临床信息系统系统仍是行业内关注医疗信息化时的重点。在

过去十年里，在卫生部等领导机构的支持下，我国医疗行业的 CIS 系统建设已经步入了一个以开发采用 C/S 结构或 B/S 结构和 GUI 界面为主要标志的阶段。

而对于大部分医院而言，由于资金、信息化认知等众多原因，医院信息化建设并没有进行整体和长期的发展规划，而是有着随医院医疗业务的不断发展和医疗信息化技术的不断进步，逐步增加、逐步完善医院信息化的特点。这就导致了医院信息化环境日趋复杂。以下问题是医院 IT 环境日趋复杂的直观体现：

1）计算机和网络等各类基础设施来自于多年来各种项目的建设，其资源信息分散，记录不完整，难以随时了解每台设备的各种详细信息，如使用、维修保修情况。众多的软件系统为多年来逐步实施，有自己研发的、所在地医保配套的、软件公司开发的，多种多样，具体应用分布分散，较难实现对各信息系统的运行状况进行全面统计、分析、判断。管理人员很难及时、全面地了解 IT 资源使用情况，系统管理决策能力不足。

2）没有明确的职责分工。对于大型信息管理系统，都不可能只由某一个人进行维护，而在多人组成的维护团队中，由于没有明确的职责分工，每个人好像什么都管，又好像什么都不管。没有人对问题进行跟踪，出了问题到最后可能是谁都不管。

3）没有制定维护优先级制度。在遇到一些问题集中发生时，没有合理地设定一个问题优先级，往往按照先后顺序来响应，对一些后发生而相对重要的事情，可能会延误。

4）统计信息反馈不及时。不能及时得到详实的统计信息，每个人各自记各自的，书写不规范，难免有遗漏，并造成统计困难。

5）无法进行故障的分析和预测。由于没有对故障进行记录和分类，无法对已发生的故障进行分析，不能采取措施避免同类故障的再次发生，更不能发现潜在的故障。

6）对维护人员的工作没办法量化，也就无法进行合理的考核。无法衡量维护人员的绩效，无法评估在系统维护中的投入产出情况。

7）没有维护数据库，信息无法及时保存和共享。由于没有对维护知识和经验进

行整理和共享，使得故障处理方法只由当时的维护人员掌握，相同的故障由不同的人员处理时还是从头开始，降低了工作效率。若关键岗位人员离职会影响工作的正常进行。

9.1.3 医院业务对于 IT 环境的依赖

医院业务与其他行业相比，具备其特殊性。临床业务的开展直接与“人命”相关。随着医院业务和医疗信息化的不断发展，大部分医院实现了通过电子分诊、电子发药等 IT 系统开展医疗业务。利用这些业务系统，有效地减少了患者的等待时间，加速了患者的就医流程，在一定程度上缓解"就医难"的问题。实施电子档案也为区域医疗信息的共享互认提供了条件，为缓解"看病贵"提供了解决问题的基础，依靠网络与电子系统作业，提高了工作效率，帮助病人节省了各个环节的等待时间。在此基础上，医院对网络与业务系统的安全、稳定运行提出了更高的要求。如果业务中断或暂停将会造成非常严重的后果，因此医院最为核心关注的问题之一就是如何保障医院临床业务的 7╳24 小时不间断、稳定的运行。随着医疗业务的不断扩展，医院信息系统越来越复杂，医疗业务对信息系统的依赖程度也越来越紧密，信息系统的任何波动，都会直接影响到业务的正常开展；信息系统如果崩溃，对于医疗业务的影响将是致命的。因此，如何清晰的掌握系统的运行情况，把可能出现的故障消灭在萌芽状态，通过科学规范的管理保证医院信息网络的稳定运行，为医院的核心业务提供可靠的技术支持服务，让业务部门满意，同时让医院信息部门的工作人员从忙于‘救火’的角色中解脱，这是医院信息部门面对的问题。

基于上述分析，作为医院临床业务的 IT 支撑环境运维管理是医院信息化建设、管理过程中非常关键的问题。同时由于 IT 技术的发展以及医院 IT 环境的日趋复杂，导致医院 IT 运维管理的难度远远高于其他行业。

9.2 建立医院信息平台的运维管理体系

9.2.1 医院信息平台运维管理体系的建设要求

IT 产业和信息化应用已经步入了深化、整合、转型和创新的关键时期，信息技术与信息系统对医院组织形态、治理结构、管理体制、运作流程的影响日益深化；医院对信息技术和信息系统的依赖性在日益加强；信息系统的安全、管理、风险与控制成为日益突出的问题；IT 与业务应用的融合，是未来发展的核心；信息化应用的关键是持续性、创造价值、风险与控制、整合、绩效管理。在这种发展时期，各种目光都聚焦在治理、审计、服务管理、风险与控制、安全等领域。这些领域正在为 IT 产业和信息化开辟新的天地，成为 IT 产业和信息化在健康规范的轨道上运行的制度保障。

各个医院都希望自己的 IT 系统能够 5╳8 或 7╳24 小时不间断运行，从而确保其上所承载的医疗业务系统正常使用。为了保证 IT 基础设施整体全天候无故障运行的目标，需要构成这些系统的各软、硬件设施都能发挥其应有的作用。建立统一技术、统一管理的 IT 服务管理平台和统一的运维管理机制，透过规范化的管理流程和运维组织模式，实现对 IT 基础设施的集中监控和对 IT 资源的合理使用，为业务系统提供端到端的 IT 服务，从而提高 IT 服务管理质量和运维服务质量。从实际工作来看，我们认为主要应从以下三点来保障系统的无故障运行：

网络不断：网络在 IT 系统中作为数据的载体，保证医疗业务数据向每个角落的延伸和可达性，网络的中断将直接影响医疗业务的正常运行，因此网络的畅通是医疗业务正常进行不可或缺的必要条件之一。

系统不瘫：作为底层基础设施，医疗业务系统同时担当着承载医疗业务和运行业务的重任，系统的正常与否也直接影响着业务的运行，所以保障医疗业务系统不瘫也是医疗业务正常进行不可或缺的必要条件之一。

数据不丢：数据是记录医疗业务的核心资料，在医疗业务的进行中，确保数据的完整和有效性是 IT 管理的核心目标，数据的丢失将导致医疗业务造成重大损失。

9.2.2 医院信息平台运维管理体系的搭建方法

医疗行业信息化运维管理需求和其他行业类似，同样是业务系统和 IT 基础设施的管理和服务。医院信息平台运维管理体系的搭建，总体上来说，应遵循下面的步骤：

1）确定体系内容。

2）结合医院信息化运维现状和医疗资源约束条件或规划目标，形成重点突出、切实可行的管理策略。

3）定期回顾医疗业务的发展，持续改善。

9.2.2.1 建立医院信息平台运维管理体系的传统法

传统法从组织、制度、技术三个维度展开：

1）组织上根据医院业务和发展战略进行针对性调整。传统按职能进行团队划分的模式都要求组织架构进行相应变革，要求根据流程进行角色安排，如一二三线技术支持等。总体目的就是提升医疗工作效率，改进医疗业务的管理效果。

2）在医院制度维度上，要梳理运维工作的管控点、分析点，从而制订相关的制度进行行为约束。制订制度一定要考虑可操作性和可考核性，只有通过结合考核的制度才可能真正落实。因此在实现的操作中，可选择一些“制度点”，逐步推进。

3）技术维度大体上有技术规范的制订、运维支撑体系的建立这两个方面。

技术规范主要针对运维客体（如医院信息技术人员、应用服务器、数据库、操作系统等等），建立诸如备份流程、双机管理、开发规范等技术标准。而运维支撑体系则是通过医院信息化系统来固化医疗业务流程，提升医疗流程效率。

9.2.2.2 建立医院信息平台运维管理体系的 PPT 法

在医院信息平台的运维管理过程中，其底层的基础为 IT 服务管理。IT 服务管理主要包含三个层面：人（医院 IT 运维人员）、流程（医院就诊流程，检验流程，检查流程，付费流程等）、技术（网络技术、操作系统技术等）。如下图所示

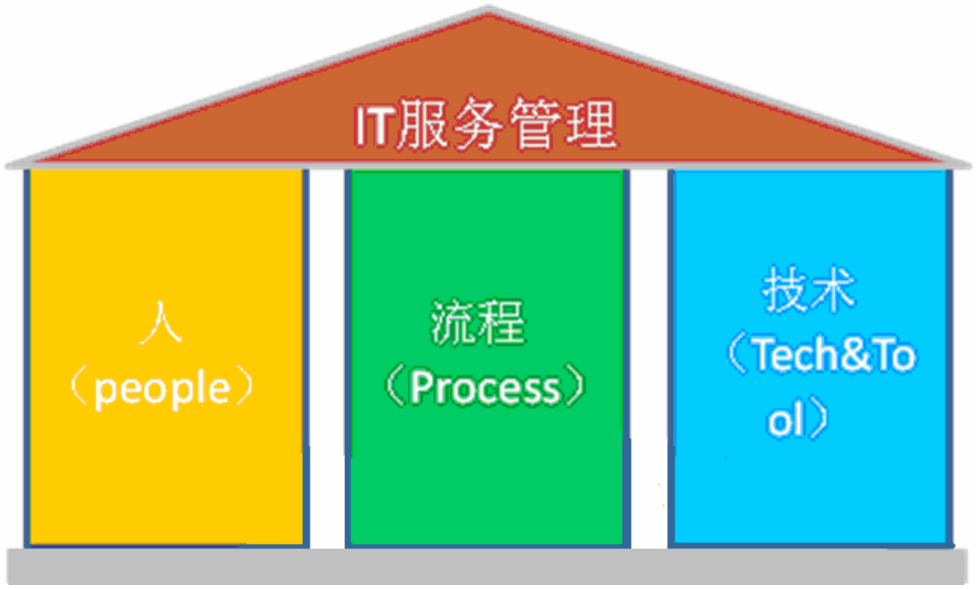


图9-1 IT服务管理的核心组成部分

■ 人员 People

是指医院需要清晰定义 IT 支持人员的角色职责，明确人员的技能等级，进行 IT 部门内部的梯队建设。IT 支持人员的素质与质量最终决定了整个 IT 服务管理实施的质量。

■ 流程 Process

是指业务流程是一个逻辑群组的活动，有规律地为医生、护士以及管理者提供可重复性的业务功能；有明确的流程目标;能达到预期的效果；流转结果可度量； ITIL 是成熟的流程模型，医院能通过流程来实践这些最佳实现方式。

■ 技术 Technology

是指有效的技术手段，可以保证医院做到： 监控 IT 系统（如 HIS、LIS、PACS、EMR、财务系统、OA 系统等）的可用性以及实时性能；监控医院网络中心实现 SLA 要求的质量；配置管理，并跟踪 IT 系统配置的变化；诊断，快速定位问题原因并对症下药；预测与预防，预测资源的使用情况，并能采取相关的预防措施；提供仪表盘，以可视化的方式展现医院 IT 服务模型、IT 服务报表与指标、网络拓扑等，让领导更方便地了解 IT 系统现状，并做出决策。

9.2.2.3 建立医院信息平台运维管理体系的要素法

以下是搭建医院信息平台运维管理体系的五要素法：

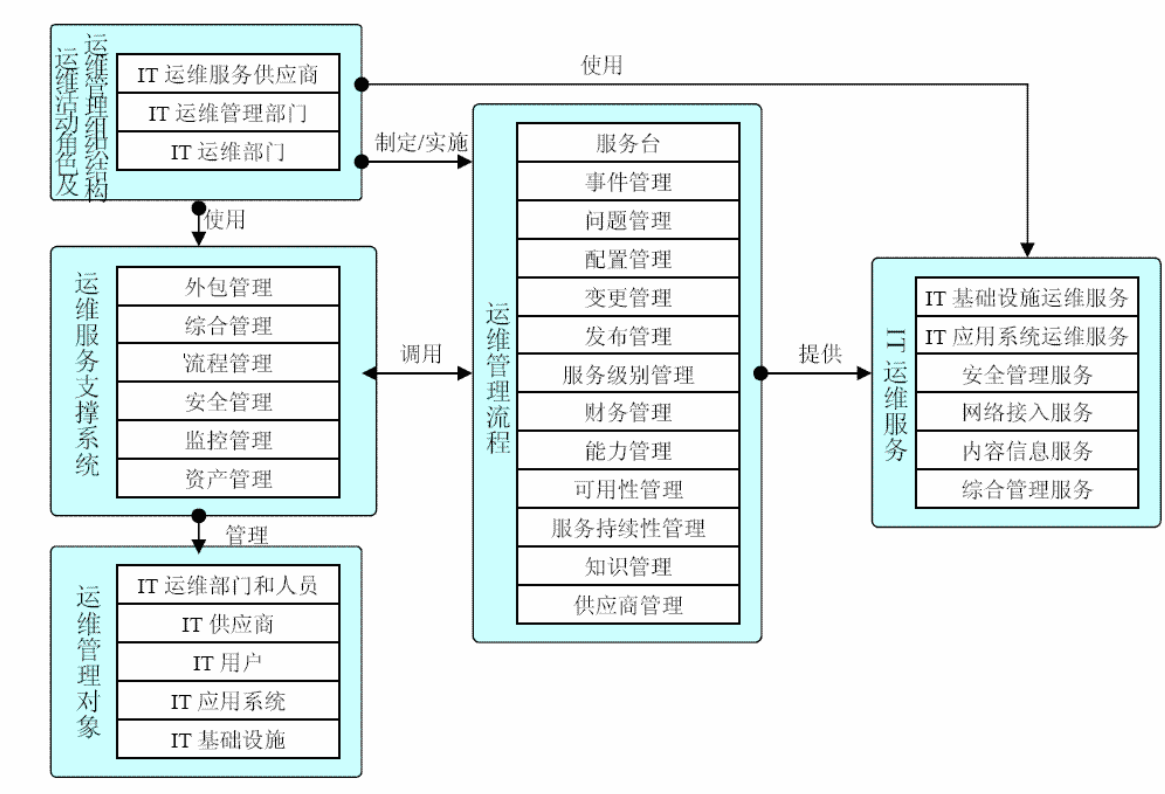


图 9-2 组成运维服务管理体系的 5 个要素的详细组成及其相互作用

9.2.3 医院信息平台的运维管理体系架构

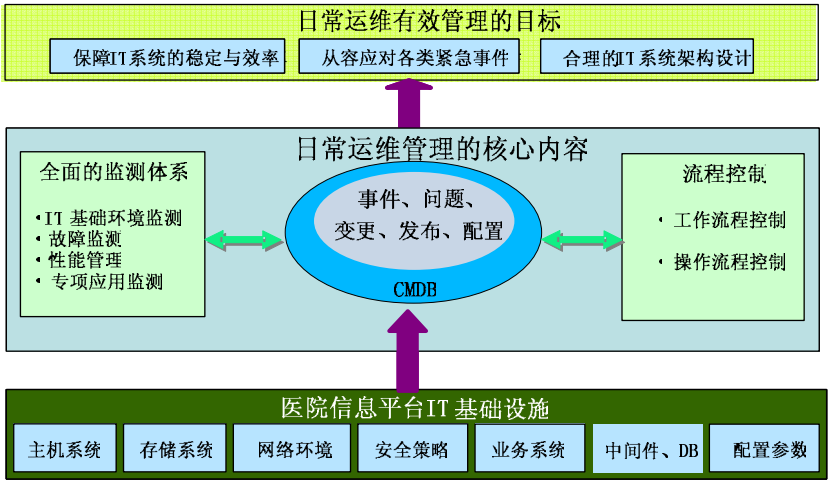


图 9-3 医院信息平台的运维管理体系架构

■ 医院信息平台 IT 基础设施

此部分为医院信息平台运维管理的最基础环节，同时也是所有 IT 服务的最核心对象。主要包括主机系统（终端、服务器、操作系统）、存储系统（DAS/NAS/SAN 等）、网络环境（基础网络，内外网环境、Internet 等）、安全环境（防火墙、IDS/IPS、流量控制、防毒防攻击等）、业务系统（HIS/LIS/PACS/EMR 等）中间件、数据库环境以及各种设备及系统的配置参数。

■ 日常运维管理的核心内容

主要是指基于 CMDB(配置管理数据库)进行 IT 环境的事件、问题、变更、发布、配置等服务行为进行统一的管理。为了能够保障上述服务行为的有效执行，必须从两个方面进行保障：全面的监测体系、流程控制。

■ 日常运维管理的目标

通过有效的运维管理实现医院信息化的三大目标：保障 IT 系统的稳定运行及效率、从容应对各类紧急事件、合理的 IT 系统架构设计。

9.2.4 医院信息平台的基础设施管理

随着信息化建设的推进，为了让凝聚了巨大人力物力投入的信息基础设施发挥出其效益，保障整个信息系统的平稳可靠运行，需要有一个可从整体上对包括服务器、网络，存储，安全等组件在内的 IT 基础设施环境进行综合管理的平台，并能够提供业务系统运行异常的实时告警和进行图形化问题定位，性能趋势分析和预警，能够基于关键业务系统的角度，以业务重要性为导向进行事件处理和通知。

医院信息平台是一个包括了众多软件，硬件技术，涉及多厂家产品，从网络、安全、存储、计算到中间件和应用的复杂异构环境。而且随着信息建设的深入和持续优化和发展，这个复杂庞大的基础设施，还会随之不断进行演进，在产品，技术和网络结构，业务关系上不断发生变化。因此，要求针对该环境进行管理的系统具有良好的可扩展性，能够将下层网络的复杂度有效的通过抽象屏蔽起来，向上层应用和运维流程开放稳定的接口。

9.2.4.1 医院信息平台的运维管理系统设计原则

从综合 IT 监控管理技术的发展来看，有以下几个关键的选择指标是在进行方案构建和产品选择的时候需要重点考虑的：

- **可视化能力**

建设 IT 运行监控中心的一个关键用途是与大屏幕监控中心配套，实现最佳的展示效果，体现信息化的建设水平和理念高度。因此可视化的效果如何，动态呈现的能力如何，就成为系统和方案选型中的一个核心考虑要素。

- **业务建模能力**

作为每个组织的 IT 维护工作，都有自己的核心业务。这些核心业务具有不同的重要性、组成结构，服务于特定的部门和用户。我们关注其不同的运行指标，这些个性化的管理需求，能否快速的，通过图形化的建模方式加以实施，并迅速在管理视图上得到反应，是非常重要的一个维度。

尤其需要避免的，是为了跟随组织的业务变化和 IT 系统演进，而大量的定制和重复开发，往往带来难以接受的实施周期和后续成本。

因此，系统可配置性如何，图形化的业务系统架构和监测体系建模功能如何，需要着重考虑。

- **实施周期**

目前有大量的 IT 运维流程管理产品，囊括了从综合监测到业务流程管理的所有方面，这些产品都集成了许多流程组件、工作台组件、知识库组件等。但是我们知道，流程是一个个性化非常强的东西。每个组织都有自己独特的 IT 管理体系和业务流程。简单的一次性照搬产品化流程系统，容易给我们带来削足适履的麻烦；长期而言可能带来很长的学习曲线和调整，并导致实施和维护成本的上升。

而我们实施运维管理系统的目的，无非是为了更好的提升核心业务的维护质量，围绕这个目标，能否有一个有效，清晰，简洁的管理机制，并可以与逐步建设的工作

流程通过 SOA 架构方便的集成，是从实际部署来看，成功率更高，更容易产生效果的建设思路。

- **设备兼容性**

要简化管理。首先，要能够全面的管理各种基于 IP 的信息化基础设施，这是一个基础。因此，系统要能够兼容国内各种主流的软硬件产品，包括网络设备，服务器，应用，中间件和环境等。要具有比较良好的网络层和链路层自动发现能力，具有自动发现主流应用和中间件的能力。从而最大化的降低管理人员对管理信息的维护工作量。

- **体系结构的开放性**

当前 IT 管理环境中，SSO 单点登录和与流程管理工作系统，门户等应用的集成，成为常见的需求，而当前最佳的集成方式，就是基于 SOAP 协议的 Web Service 接口，通过规范标准的接口定义，就可以实现与其他主流门户和流程系统的集成。在集成能力上，因此也是关注的一个重点。

9.2.4.2 医院信息资源统一监控平台系统架构及技术实现

9.2.4.2.1 系统逻辑架构

从软件体系结构角度看，系统可以分为以下四层：

数据采集与代理：本层由各种协议适配器构成，向上层提供统一的接口访问管理协议栈（SNMP/CMIP/TL1 等），获取管理信息（包括事件信息、日志信息、性能信息和拓扑信息等）,并在初始发现时作为驱动模块构建信息模型。

数据汇聚：对底层数据采集的数据进行统一的描述，组织为管理信息库。向上提供一个统一的管理语义和调用接口。使得各个业务模块面对统一的数据模型，使得对资源的管理方式一致并处于单一的可控路径下，方便对资源进行权限管理，互斥访问等操作，使得面向事务的并发管理成为可能。

数据处理层：专注于管理业务的实现，不再关心底层协议的差异性。响应前台应

用的请求，完成数据查询，处理等功能；

数据展现层：前台界面，从数据处理层得到数据加以显示。是管理员与网络管理系统的接口。

9.2.4.2.2 架构设计思路

按照功能需求规格来决定主要软件模块的划分。将整个软件系统分为四层：数据采集层，数据抽象层，数据处理层和数据表现层；每一层的功能依托于下一层的实现，一般不作跨越功能层次的调用。

利用分布式总线实现各个模块之间的通信。模块之间通过接口，利用消息总线进行互操作。

总体设计上先决定功能模块，然后按照功能模块设计其服务接口；按照功能模块特点和数据流量以及流向决定其部署方式和通信方式；按照性能需求和对移植性、开发强度的综合考虑决定中间件和对象服务的选型。

9.3 医院信息化平台的 IT 服务管理

信息技术基础设施库(ITIL®)作为 IT 服务管理(ITSM)最佳实践的事实标准，成为了解及衡量 IT 服务价值的重要渠道。在医疗行业中，尽管全球存在差异化的应用环境，但是许多医院的 IT 部门都在开始部署 ITIL，来提升 IT 部门服务医院内部各项业务的质量和性价比，并通过此途径来打造医院的核心竞争力、提升医院各方面收益。

ITIL 是在这样一个事实被普遍认可的情况下开发出来的，即组织正日益依赖于 IT 来实现其业务目标，这种目标在医院信息化过程中正在逐步展现。这种逐渐加深的对 IT 的依赖使得组织对与其目标相关的、可以满足客户需求和期望的高质量 IT 服务的需求也越来越强烈。在过去的几年中，人们关注的焦点已经从开发 IT 应用系统转换到对 IT 服务进行统一的管理上来了。在医院中，一个 IT 应用系统(有时是指信息系统)只有在满足以下两点时才会有助于实现医院的目标：第一，该系统可以被医院充分利用；第二，当系统产生故障或需要进行必要的修改时，可以得到维护和

运营管理的有力支持，即 IT 系统利用率以及系统运维及故障恢复时间。

现阶段，在整个 IT 产品的生命周期中，运营阶段占了整个时间和成本的约 70%至 80%，其余的时间和成本花费在产品开发(或采购)上面。医院也是如此，由于 IT 环境的复杂，有时甚至要高于这个比例。因此，具有良好效果和效率的 IT 服务管理流程对于 IT 的成功运用是至关重要的。这些 IT 服务管理流程适用于任何类型的医院，而不论其是大规模的还是小规模的，公立的还是私立的，使用集中的 IT 服务还是非集中的，以及使用内部供应的 IT 服务还是外包 IT 服务。在任何情况下，服务必须具有可靠性、一致性和高质量，并且其成本也应当是可接受的。

IT 服务管理主要涉及对为满足组织需求而定制的 IT 服务的交付和支持。ITIL 被开发出来也是为了系统和一贯地推广得到证明的 IT 服务管理最佳实践。这种方法主要基于服务质量理念和开发有效且高效的流程的理念之上。

基于 IT 基础设施，ITIL 为 IT 部门的所有活动提供了一个通用框架，这些活动是服务交付的一部分。这些活动被划分为不同的流程，当这些流程协同运作时，可以提供一个有效的框架从而可以使得组织的 IT 服务管理更加成熟。这些流程中的每一个都包括了一项或多项 IT 部门的任务，如服务开发、基础设施管理、服务交付和支持等。这种流程的方法使得有可能独立于组织架构而描述 IT 服务管理最佳实践。

医院信息平台的运维管理过程中，在 IT 基础设施统一管理基础之上，在日常的运维过程中需有一套完善的服务管理体系支撑，才能够保障医院 IT 信息平台的稳定、可靠、高效运行。为了便于理解和实施，后续将对 IT 服务管理的 6 大组件，包括服务台、事件管理、问题管理、变更管理、发布管理、配置管理等结合医院信息化平台进行简单描述。从而帮助医院建设一套完善的信息化运维服务的管理体系和流程。

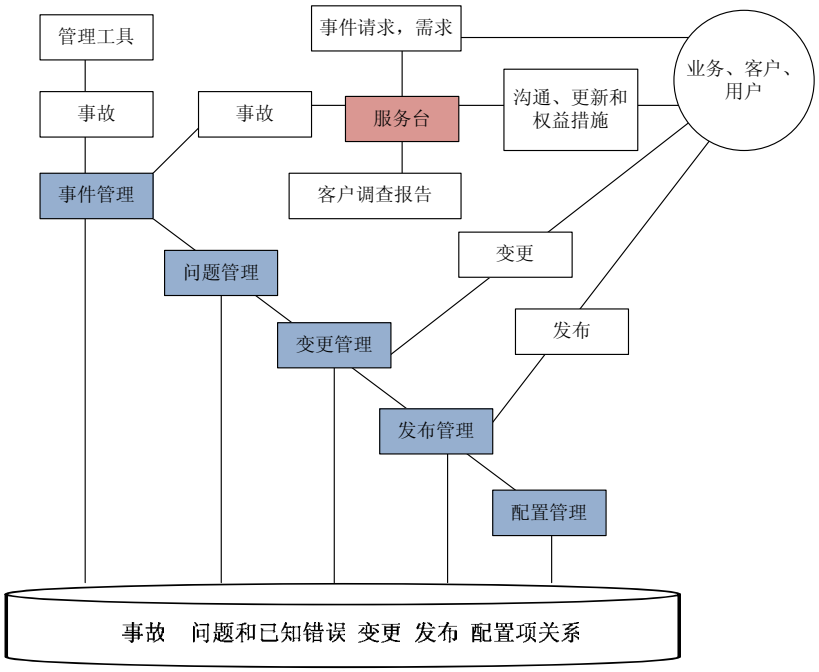


图 9-4 IT 服务管理体系

9.3.1 服务台

服务台是 IT 部门与业务部门的单一联系点，在运营层面上具体实现了 IT 与业务的融合。IT 与业务在运营层面上的融合具体体现为：IT 要支持业务的持续运作、按照服务级别协议规定排序用户的要求，最大化业务的需求（如同时发生用户不能打印和交换机出现问题影响计费系统时，服务台必须对二者根据影响程度和紧迫程度按优先级对用户反馈的意见进行排序，确定处理的优先级，以最大化业务的需求）。

9.3.1.1 服务台的主要职责

服务台（Service Desk）及事件管理（Incident Management），它的用意在于加重第一线支持的功能，并赋予它更广泛的角色——在使用者第一次通报的时候就实时把问题解决，增加事件解决的比例，让 IT 部门能更专注于医院业务目标的达成，提供高品质的支持，进而提高使用者满意度。服务台是一个功能（Function），它没有严格定义的执行流程，它与多个服务管理流程密切相关，为用户提供与问题、变更、服务级别、发布、配置、 IT 服务持续等管理的接口，它是提供高效率的 IT 营运服务所不可或缺的关键。

服务台的任务包括作为与使用者及顾客的单一联络窗口，接收并记录所有使用者的电话，处理使用者相关的事项及抱怨，解决事件或将事件升级请求二线支持，通知使用者及顾客事件状况，并制作相关管理报告。

具体而言，服务台的主要职责是：

1）接受客户请求（可以通过电话、电子邮件和传真等）；

2）记录并跟踪事故和客户意见；

3）及时通知客户其请求的当前状况和最新进展；

4）根据服务级别协议，初步评估客户请求，尽力解决它们或将其安排给有关人员解决；

5）根据服务级别协议的要求，监督规章制度的执行情况并在必要时对其进行修改；

6）对客户请求从提出直至终止和验证的整个过程进行管理；

7）在需要短期内调整服务级别时及时与客户沟通；

8）协调二线支持人员和第三方支持小组；

9）提供管理方面的信息和建议以改进服务品质；

10）根据用户的反馈发现 IT 服务运作中产生的问题；

11）发现客户培训和教育方面的需求；

12）终止事故并与客户一道确认事故的解决情况。

9.3.1.2 服务台的构建模式

1）集中式服务台

集中式服务台是指由一个物理上集中的服务中心统一处理所有的服务请求。这种

模式的优点是：降低总体运作成本；管理控制上得到了加强；提高了资源利用率。

该模式最适合于 IT 部门既负责提供服务，又负责为服务提供支持的情形，服务台负责接受、记录、监督和升级所有的服务请求，同时也起业务运作支持的作用。

2）虚拟式服务台

虚拟式服务台，能够不受时间和地点限制提供支持服务。

Web 技术是为实现虚拟服务台提供了很好的技术支持。提供的服务可以包括：服务推广、与使用者及顾客沟通的渠道、提供供货商修正程序下载、已知问题告知、通知注意事项、系统公告、使用手册、常问问题解答、每周每月管理报告，服务指南及知识库查询。目前的工具软件可以提供范例 Web 网站、常见问题解答、报告、通知使用者及顾客状况电子邮件这些功能，甚至能够个人化。

9.3.1.3 评价服务台的关键指标

（1）电话应答是否迅速（如 90 %的呼叫在 X 秒内被应答）；

（2）呼叫是否按时转送给二线支持；

（3）是否按时恢复服务；

（4）是否及时通知用户目正在实施的变更和将来需要实施的变更；

（5）首次修复率。

（6）服务台员工接电话是否有礼貌；

（7）用户是否得到预防事故发生的建议。

9.3.1.4 服务台的工作流程

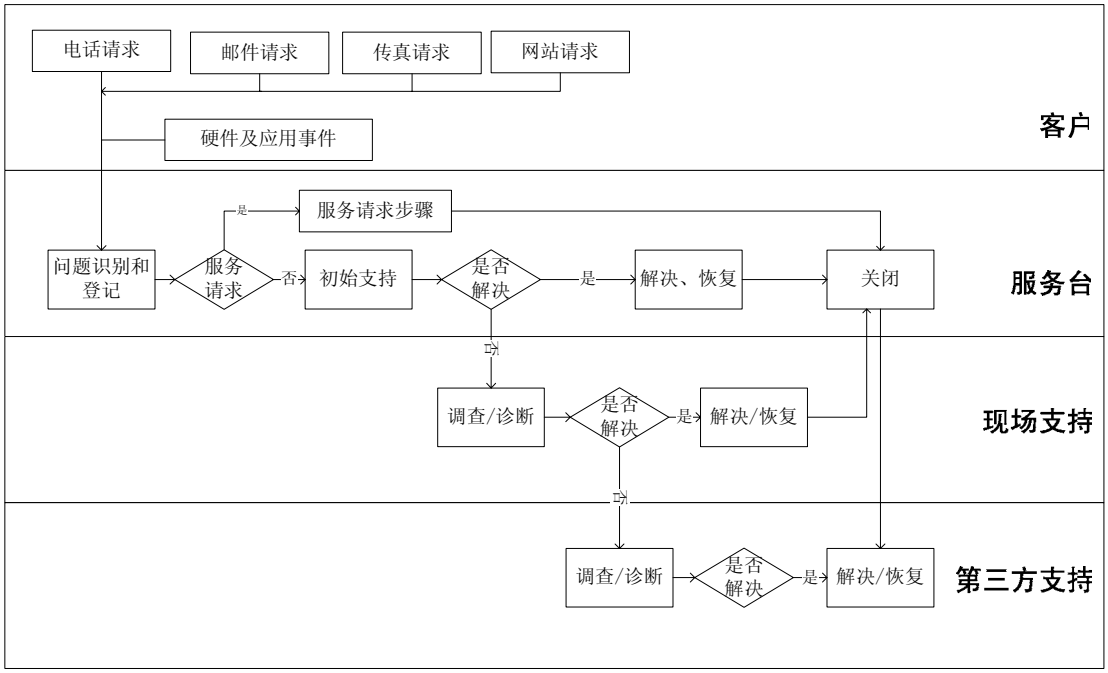


图 9-5 服务台流程

9.3.2 事件管理

事件管理（Incident Management）又称突发事件管理，是一个被动型的任务，也就是减少或消除存在或可能存在与 IT 服务中的干扰因素给 IT 服务带来的影响，以确保用户可以尽快回复自己的正常工作。因此，要将事件（Incidents）记录下来并分类，再分配给适当的专业人员去处理；监控事件的发展；并在事件得到解决后将其终止。

核心设备出现故障，应用系统受到攻击等等，这些突发事件如果发生，信息部门如何处理而不耽误医疗业务开展，这是需要迫切解决的问题。建立突发事件管理流程，如核心设备冗余系统，灾备系统、安全防护系统，灾难发生时的紧急起用备用系统等等，才能有效的处理突发事故，把损失和影响降到最低。

医院信息平台的事件管理目标是要在给医疗工作人员和医院正常的业务活动带来最小影响的情况下，尽快回复到正常服务级别。事件管理需要保留事件的有效记录以便能够权衡并改进处理流程，给其他的服务管理流程提供合适的信息以及正确报告

进展情况。

9.3.2.1 事件管理的流程

（1）事件检测与记录

事件检测与记录步骤是事件管理流程的起点。该步骤的目的是快速、准确地探测和捕捉所有在 IT 生产环境中发生的错误，并在将来的问题管理流程中帮助确定问题和解决问题。在本步骤中，将收集创建一个事件单所需要的信息，重点是准确、完整地记录必要的信息。

（2）事件分类与初步支持

该步骤包括：为了对医疗工作人员的请求进行分析而进一步收集信息。该步骤的目的是对每个事件进行正确的分类，随即在现存的知识库中查询与该事件相匹配的条目。

若没有找到合适的解决方案或变通方法，则该事件需要转派给一线组长，后者根据知识库判断该组员是否能够处理该事件，能够处理的返回该客服组员进行处理。对于不能处理的事件，客服组长判断是属于应用、系统还是设备方向的事件，提交二线组长，由二线组长再根据实际情况分配给一个具有合适技能的事件分析员。

在处理过程中，事件记录员需要根据处理的情况详细记录整个处理过程和结果，记录信息应与实际情况一致。若根据当前已有知识库条目能够解决事件，则在解决完事件后，在事件单中记录和填写故障根源和解决方案。若解决方案比较复杂，还需附上附件。

（3）事件调查和诊断

这个步骤阶段的目标是进行深入的调查，以解决事件。各个技术水平的事件分析员（二线人员）将会参与寻找一个解决方案或变通方案。若事件分析员（二线人员）认为该事件根据知识库条目或其他常规方式能够解决，则返回一线事件记录员进行解决与恢复。若通过调查和诊断还是不能解决事件，可能需要问题管理流程也参与进来进行更加深入的分析研究。

一线事件记录员应及时跟踪事件的整个处理过程，并适时向用户说明处理情况。

（4）解决和恢复

这个步骤尝试使用解决方案和变通方法来解决事件。某些情况下，需要引入变更管理来批准评估实施步骤。

事件解决完毕后，二线支持人员需要依据解决情况创建知识库条目，并进行等级划分，然后定期对一线人员进行新知识库条目的培训。

（5）事件关闭

这个步骤确保客户对事件的处理情况感到满意。这里分两种情况，若是用户提出的事件，则所有工单关闭前都需要征得用户同意；若是监控发现的事件，则在解决后直接关闭。

（6）监控事件

这个步骤监控目前尚未解决或正在解决的事件，它由事件单创建时开始，在事件单关闭时结束。这个步骤目前基本上是由一线组长人工来执行，只有触发升级策略才会由后台工具发出邮件通知。

9.3.2.2 事件管理的流程图

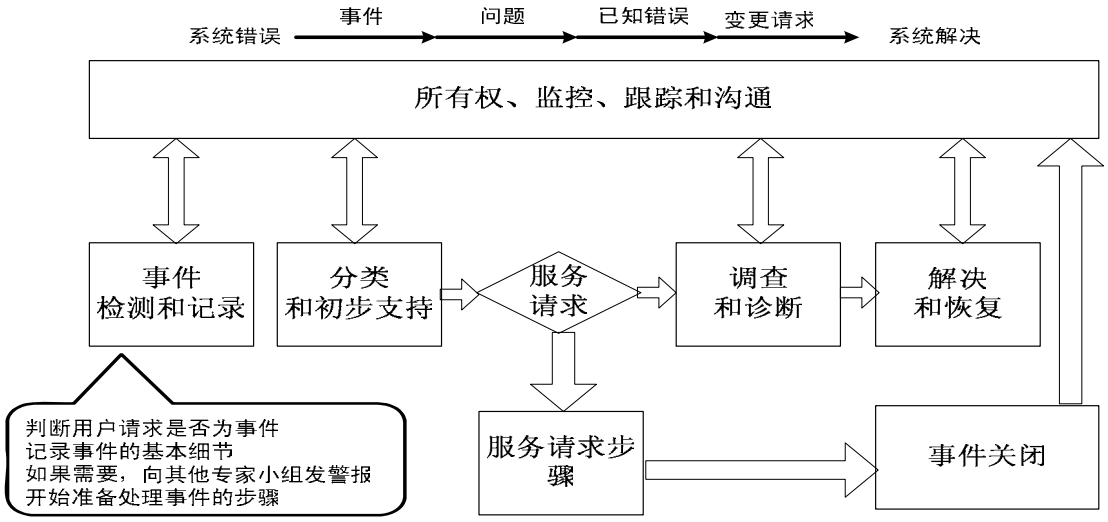


图 9-6 事件管理流程

9.3.3 问题管理

问题管理的责任是调查和分析 IT 基础架构和查找事故产生的根本原因。问题管理强调找出事故产生的根源，从而制定恰当的解决方案或防止其再次发生的预防措施。

建立问题管理流程，把存在的问题的现象、问题原因、解决方法记录下来，有利于从根本上解决问题，杜绝同样问题的再次发生。采取主动性问题预防措施，从而能消除或减少信息系统中故障的发生。

在记录问题时，必须对问题进行优先级/影响度分析，以对问题有效分配必要资源和解决时限。问题记录必须有规范的格式，从而在转派或解决过程中能得到有效更新和统一认识。提高解决问题的效率。

9.3.3.1 问题管理的流程

（1）问题检测与记录

本步骤的主要目的是识别问题（主动或是被动），创建问题单以及对问题进行严重等级的判断。

（2）问题分派

这个步骤首先将问题分派给 IT 部门中的分析员，然后这个问题分析员将开始收集数据判断这个问题是否可能解决，然后该问题分析员对应的业务岗位的支持组组长开始跟踪问题解决的整个流程。

（3）问题调查与诊断

该步骤确定了问题信息的来源，对数据进行分析，找出问题的根本原因。

（4）问题解决

本步骤的目的是为成为“已知错误”的问题提供一个最终的解决方案，或者临时的变通方法，并进行实施。并且需要引入变更管理流程来完成解决方案的实施。

（5）问题关闭

这个步骤确保问题的处理情况令人满意。问题单的信息是正确、完整的，处理过程中的经验能够得到记录以形成可重用的知识。

9.3.2.2 问题管理的流程图

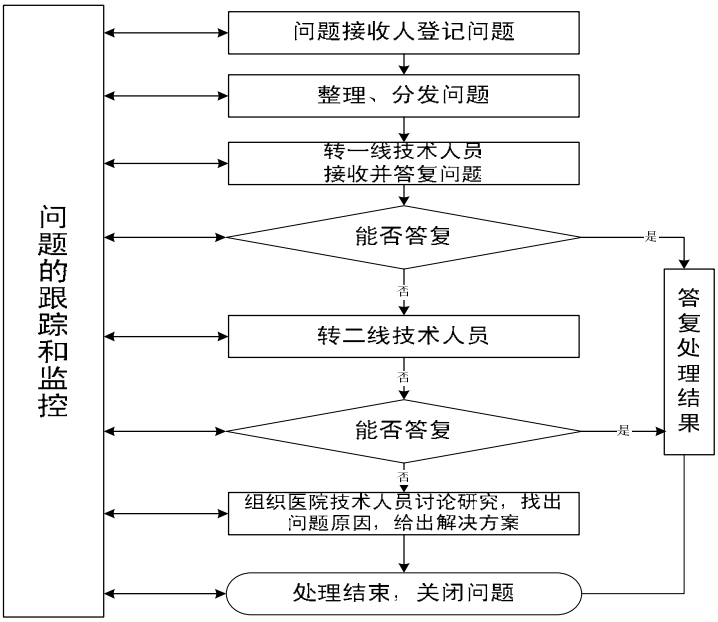


图 9-7 问题管理流程

9.3.4 变更管理

变更管理是在最短的中断时间内完成基础架构或服务的任一方面的变更而对其进行控制的服务流程。

医院的各种信息系统，由于外部政策的变化和内部发展的需要，各部门在应用过程中根据自身的需要提出各种需求。因此，不同时期，不同考核制度，不同核算方法，要求信息系统必须根据需要变更。网络的拓展、硬件的更新使网络配置系统发生变更。这些变更如果没有记录在案，将会影响下次问题的处理，甚至造成突发事件。因此，建立基于 ITIL 的变更管理和版本管理，可以确保系统更改后上线的可靠性和准确性。

变更管理流程设计主要考虑下面三方面：

1）变更原因、变更影响、变更紧急度。

2）设计以下主要角色:变更请求者、变更受理者、变更审批者、变更实施者、变更管理流程负责人。

3）确定变更的主要活动和流程，并建立变更实施管理档案。

9.3.4.1 变更管理的流程

（1）接受变更请求

- 所有变更请求，都需递交到医疗 IT 部门负责人手中，供评估和批准。
- 评估变更分类、变更级别等，确定与变更相关的人员，并对常规变更进行实施；

（2）变更请求分类和登录

通过分类，确定该变更请求的批准人和领导 / 执行人，并确定是否是紧急变更，紧急变更适用同一流程但将得到快速批准和实施。

（3）提交变更请求到变更顾问委员会（CAB）进行评估，确定影响度

医疗信息化部门负责人将根据特定的变更请求成立特定的 CAB，成员包括对该变更的评估和批准提供应有附加价值的技术人员和管理人员。评估工作包括技术可行性，对容量的影响，对现有服务的影响，资源需求等。

（4）批准变更请求

医疗信息化部门负责人确定对该变更请求有批准权的专家参加 CAB，必要时参与评估。评估后该负责人根据判断决定是否批准变更请求。

（5）检查变更计划 / 测试结果，并批准实施

医疗信息化部门负责人确定合适人员主管该变更并参与 CAB， 称为变更主管。变更请求得到评估和批准后，变更主管安排相应资源进行变更的构建 / 开发，然后需

要对将要实施到医疗业务环境的变更进行测试，并制定实施计划，随后提交测试结果和计划给负责人以获得实施。负责人必需要确保测试结果和计划都有文档记录和得到签署，并确认变更对医疗业务环境没有影响或影响可以得到控制。这一步骤为变更流程的关键质量检查点。

（6）规划变更请求

变更请求一旦获得批准，它必须根据资源和其他情况进行规划，确定实施日期，分配相应资源，并通知请求人。

（7）协调变更实施（Coordinating the change implementation）

一切就绪后，可以实施变更。建议医院的计算机中心运维组实施相应变更，变更经理监视实施过程，并在必要时进行协调。

（8）更新变更状态

在整个变更过程中，变更的状态从登记，评估，回顾到最后关闭是不同的。变更经理负责更新预先定义好的变更状态。

（9）回顾和关闭

实施变更后，负责人负责从技术和流程角度去回顾变更，该回顾在预先定义好的时间段针对变更单独进行，除确保变更请求得到了预期效果外，也寻找流程的改进机会，如资源计划和实际使用的一致性。确定是否满足了变更目的，有没有副面影响，否则需制定后续行动计划。随后，负责人负责利用预先定义好的结束状态关闭变更请求。

（10）总结汇报

向医院管理层提供流程报表，向医疗工作人员提供变更的相关执行信息。定期向相关小组 / 部门根据流程衡量标准汇报很重要，只有如此，才可以基于现有环境的最新信息，作出进一步的改进建议。

（11）变更会议

负责人负责定期或不定期召开变更会议，以在 IT 内部以及与医疗工作人员就变更管理有一个好的沟通。在会上，可以传递如，最近变更规划，将要实施变更的信息，也包括对变更流程的反馈和建议等。

（12）变更流程回顾

建议定期回顾变更管理流程以提高效率和效能，在实施变更流程不久之后，可以进行第一次回顾，以确保流程得到正确实施并起到预期目的，发现的问题必须追根溯源并尽快解决。之后，可以定期举行正式的回顾——如每三个月。

9.3.4.1 变更管理的流程图

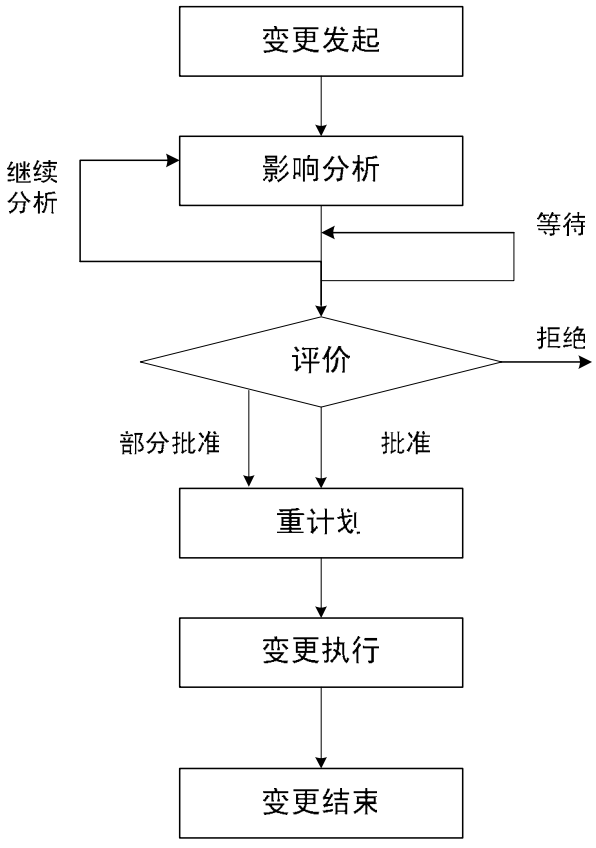


图 9-8 变更管理流程

9.3.5 发布管理

发布管理是对经测试后的新增或修改的配置项导入实际运行环境所进行的分发和上线的管理过程；它采用一种项目规划的方法来实施变更，处理变更所涉及的所有技术和费技术方面的是想，即关注变更的实施，而且主要应用于软件方面的发布。

9.3.5.1 发布管理的目标

发布管理的目标如下：

1）要通过正式的过程来确保医疗业务环境的质量

2）确保软硬件组件的发布经过计划和协调；

3）确保与变更相关的硬件和软件是可追溯的和安全的；只有正确的、经过批准和测试的软硬件版本才能导入实际运作环境；

4）确保每项发布都更新到了配置管理数据库中，并在最终软件库中也得到更新。

9.3.5.2 发布管理的流程图

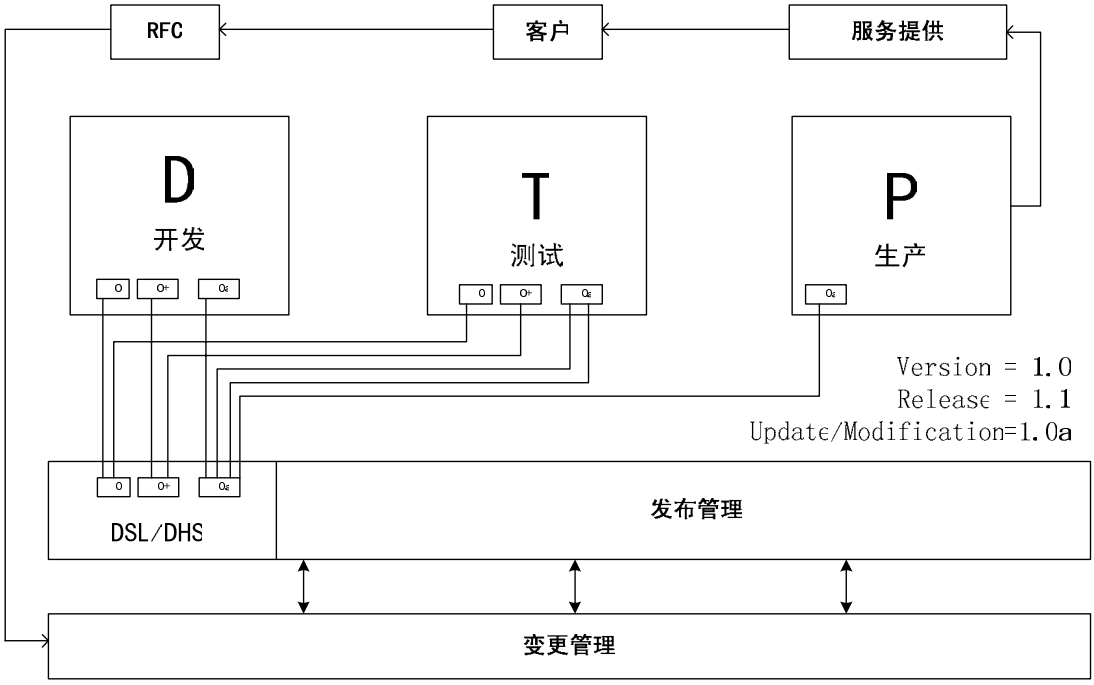


图 9-9 发布管理流程

9.3.6 配置管理

配置管理是网络系统基础架构控制中心。也是医院信息系统稳定运行的保障。建立统一完整的配置管理流程及管理范围，使配置管理流程成为医院信息部门的唯一进行配置管理的功能流程。

建立网络主服务器、网络系统、存储、IT 设备的基础配置信息库。建立相应的流程机制来更新和保持配置信息的完整性和正确性。

配置管理可以为信息系统运行过程中可能产生的突发事件、疑难问题等提供准确的网络基础架构配置信息，可以帮助技术人员迅速对问题原因进行分析，并确定解决方案。 同时，通过建立配置管理流程，使维护人员能够对系统所有硬件及软件资源实现动态管理，从而提高了 IT 资源的利用率，降低医院信息建设的投资成本。

配置管理数据库包括配置项及各配置项相互关系信息

9.3.6.1 配置管理的目标

1）对医院内部的所有 IT 资产和配置及其服务作出说明；

2）提供有关配置及其记录的准确信息以支持所有其他的“服务管理”流程；

3）为“事故管理”、“问题管理”、“变更管理”和“发布管理”提供坚实的基础；

4）对照基础设施验证配置记录并纠正任何异常情况

9.3.6.2 配置管理的主要活动

（1）规划

确定配置管理的战略和目标，分析现有的信息，确定所需的工具和资源，协调与其他过程、相关方的接口等。

（2）控制

确认只有经过授权的配置项及其更新纳入配置管理数据库（CMDB）。确保对配置项的增加、变更、替换或移除只有在获得必要的文档（RFC）和审批的前提下才能进行。

（3）验证和审核

通过对 IT 基础设施进行审计来检验配置管理数据库，以确认已记录配置项的存在性和验证记录的准确性。

9.3.6.3 配置管理与其他管理的相互关系图

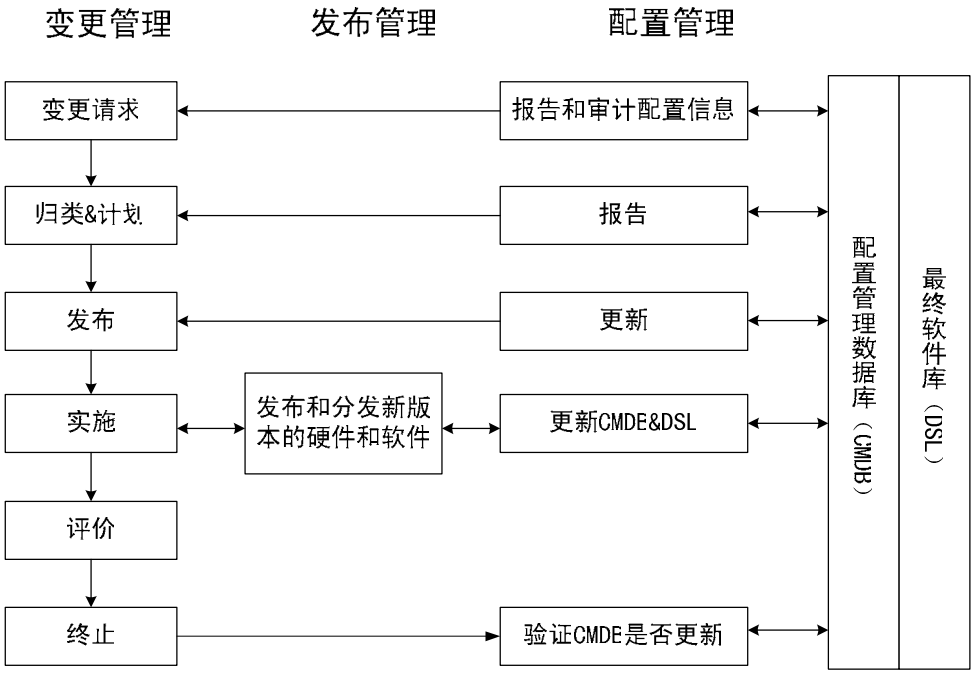


图 9-10 配置管理与其他管理的相互关系图

9.4 本章小结

随着网络技术的飞速发展和医疗行业信息化建设的深入，医疗信息化在医疗行业的应用越来越多，应用越来越复杂。医疗业务对信息化的依赖性越来越高。医院信息部门的压力也越来越大。“管好网络、管好机房、管好应用”，这看起来似乎是信息服务部门最基本任务，做起来却越来越棘手。一方面信息部门的员工疲于奔命；另一方面，业务部门并不满意。这对矛盾在医疗行业信息服务中越来越突出。医院信息平

台的运维管理就是把医疗信息化与业务相结合。

在其他行业，如电信、银行业用户和部分已经做了核心应用系统集中工作的政府部门，在完成数据中心大集中的过程中，已经逐步完善了 IT 服务管理体系。此类用户已经基本完善了对运维管理的主要流程的建设，正在将对流程本身的关注，逐步转变到对如何管控和流程执行效果的关注上来。但由于我国的医疗与卫生行业的信息化起步较晚，与国外先进国家还存在一定差距，尤其在建设信息系统之后的 IT 系统维护的水平更是有待提高。到目前为止，建立医院信息平台的运维管理体系还处于一个摸索阶段，医院信息运维管理模型还没有完全建立。

因此，在今后的医疗信息化发展过程中，医院信息运维管理要结合我国医院业务的实际情况，建立医院信息服务管理流程，将医院信息服务管理流程化，使信息部门在处理问题时，变被动为主动。从而确保信息服务流程能为医院的业务运作提供更好的技术和服务支持，提高信息部门的服务效率。

基于电子病历的医院信息平台

建设技术解决方案

（1.0 版）

技术部分

卫生部信息化工作领导小组办公室

卫 生 部 统 计 信 息 中 心

二 O 一一年三月

目　录

基于电子病历的医院信息平台

建设技术解决方案

（1.0 版）

业务部分

卫生部信息化工作领导小组办公室

卫 生 部 统 计 信 息 中 心

二〇一一年三月

目　录

致　谢

《基于电子病历的医院信息平台建设技术解决方案》研制是一项十分复杂且具挑战性和创造性的工作，得到了有关单位和企业的大力支持与协助，在此一并表示感谢！

项目主持单位： 卫生部信息化工作领导小组办公室
卫生部统计信息中心

项目参与单位：（排名不分先后）

中国卫生信息学会
中国医院协会信息管理专业委员会
中国人民解放军总医院
中国疾病预防控制中心妇幼保健中心
中国医学科学院肿瘤医院
中国医科大学附属盛京医院
华中科技大学同济医学院
华中科技大学同济医学院附属同济医院
英特尔（中国）有限公司
万达信息股份有限公司
用友医疗卫生信息系统有限公司
湖南长城医疗科技有限公司
福建弘扬软件有限公司
海思林科(北京)信息技术有限公司
杭州创业软件股份有限公司
浙江和仁(浙大中控)科技有限公司
方正众邦数字医疗有限公司
东华软件股份公司
无锡曼荼罗软件有限公司
广州市慧通计算机有限公司
北京蓝海联盟科技有限公司
北京嘉和美康信息技术有限公司
东软集团股份有限公司
北京数字证书认证中心有限公司
锐捷网络有限公司
杭州华三通信技术有限公司
浪潮集团有限公司
国投安信数字证书认证有限公司
中科软科技股份有限公司