# 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。

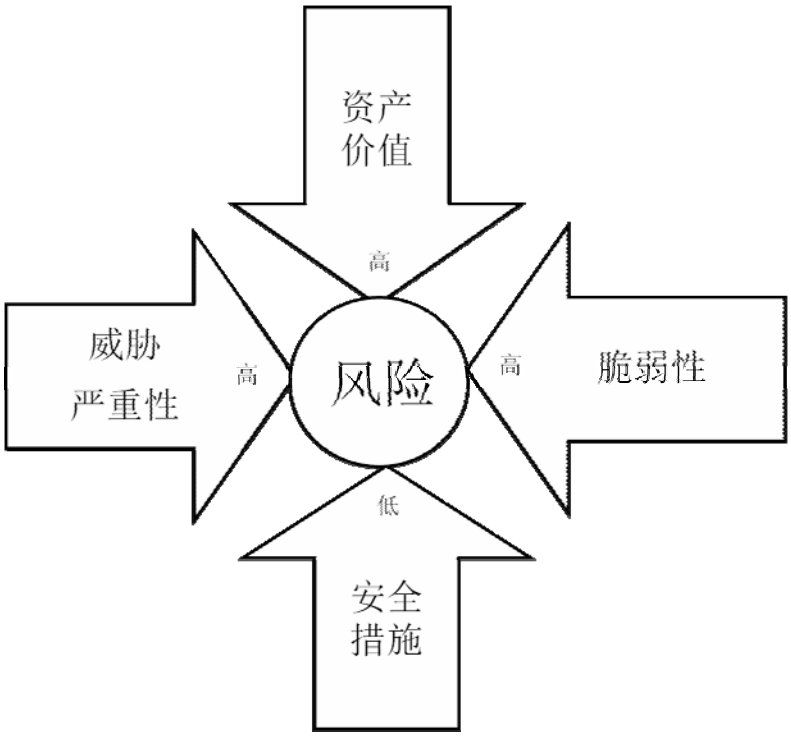


图 7-1　安全风险要素分析

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：

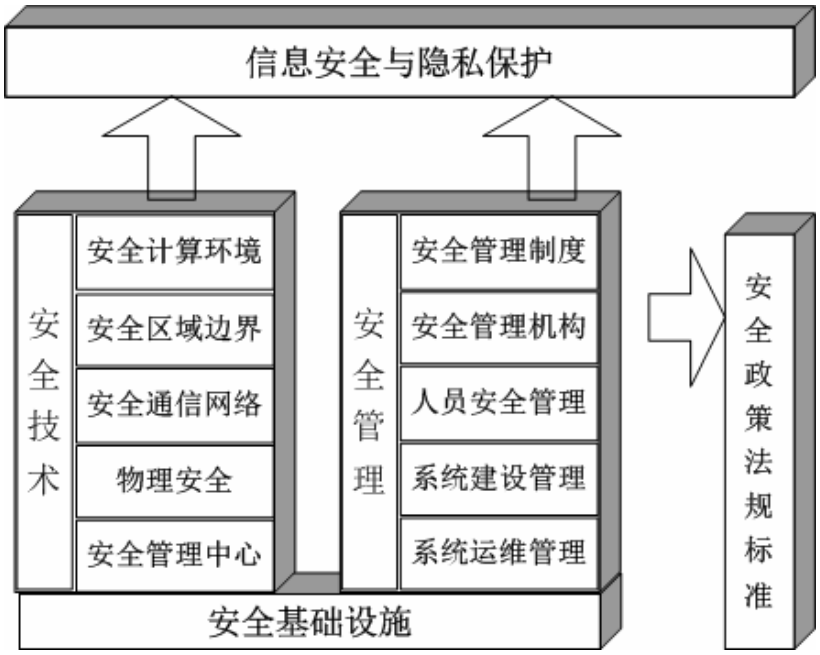


**图 7-2　安全体系总体框架**

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：

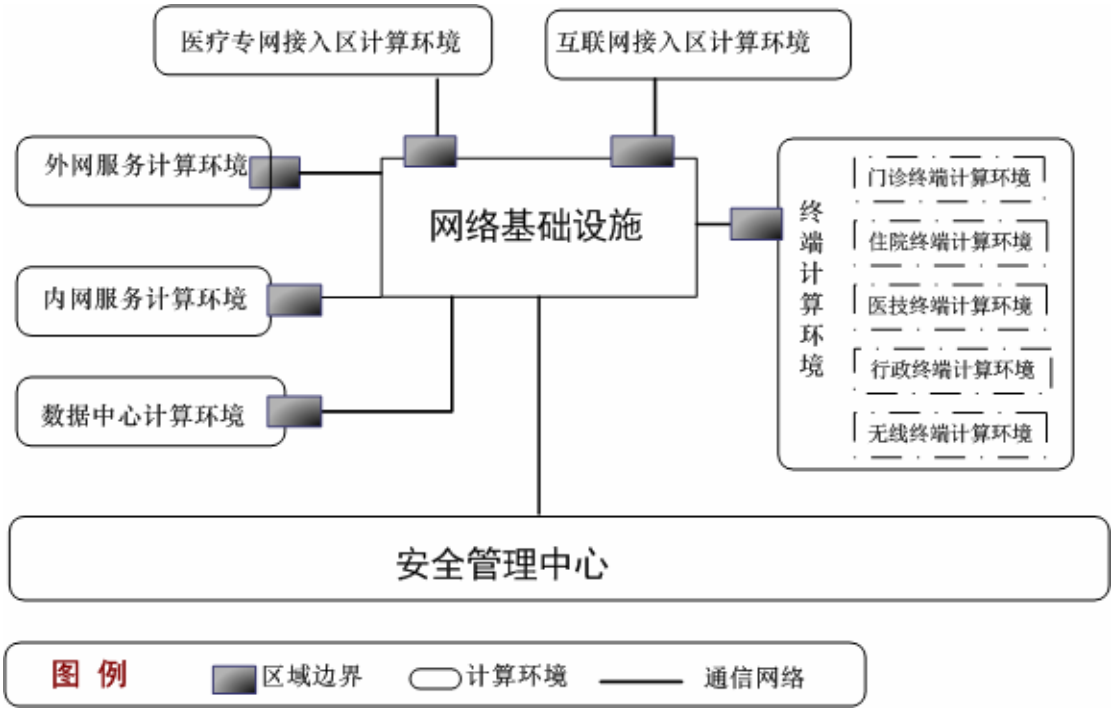


图 7-3　保护对象示意图

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：

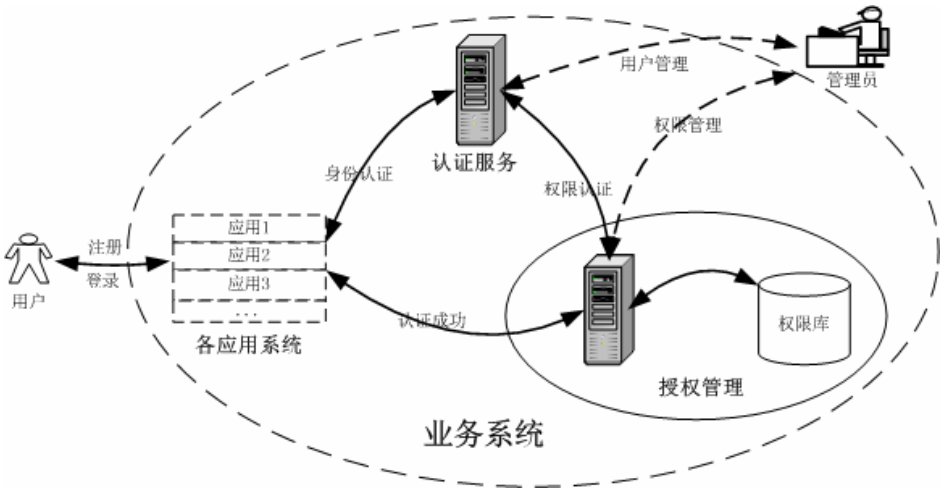

图 7-4　访问控制框架

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。

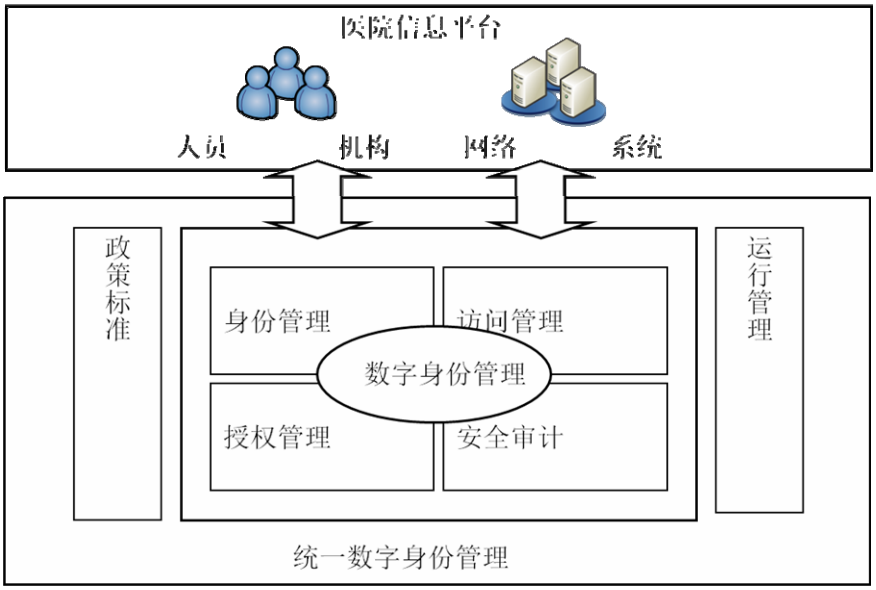


**图 7-5　统一数字身份管理**

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。

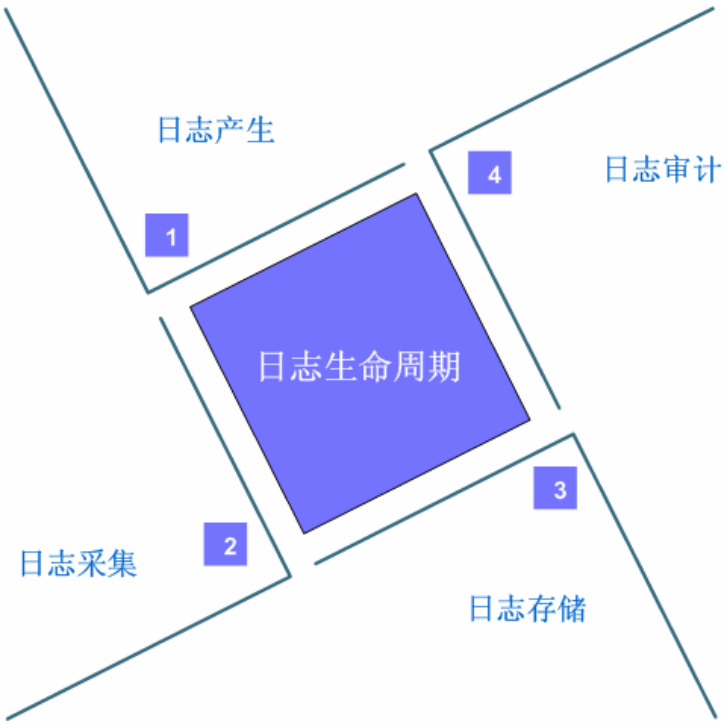


图 7-6 集中日志审计

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；<br>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；<br>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。<br>制定严格的制度制定与发布流程，方式，范围等；<br>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；<br>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；<br>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；<br>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；<br>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；<br>建立授权与审批制度；<br>建立内外部沟通合作渠道；<br>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；<br>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；<br>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；<br>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；<br>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；<br>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；<br>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；<br>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；<br>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；<br>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；<br>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；<br>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；<br>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；<br>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；<br>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；<br>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；<br>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；<br>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；<br>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；<br>b） 应确保提供软件设计的相关文档和使用指南；<br>c） 应在软件安装之前检测软件包中可能存在的恶意代码；<br>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；<br>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；<br>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；<br>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；<br>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；<br>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；<br>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；<br>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；<br>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；<br>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；<br>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；<br>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；<br>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；<br>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；<br>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；<br>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；<br>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；<br>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；<br>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；<br>e） 应对网络设备的配置文件进行定期备份；<br>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；<br>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；<br>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；<br>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；<br>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；<br>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；<br>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；<br>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；<br>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；<br>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；<br>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；<br>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；<br>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；<br>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。 | |