ICS
C 07

WS

WS/T XXXXX—XXXX

中 华 人 民 共 和 国 卫 生 行 业 标 准

居民健康卡注册管理信息系统技术规范

Technical specifications for information system of residents' health card register management

（征求意见稿）

-XX-XX 发布　　XXXX-XX-XX 实施

中华人民共和国国家卫生和计划生育委员会　发布

目录

前　言

本标准按照GB/T 1.1—2009给出的规则起草。

本标准负责起草单位：

本标准主要起草人：

居民健康卡注册管理信息系统技术规范

1 范围

本规范规定了居民健康卡国家、省、市（县）注册管理信息系统的整体架构、基础功能、IT基础设施规范、安全规范与性能要求。

本规范适用于指导省、市（县）居民健康卡注册管理中心开展本级居民健康卡注册管理信息系统的规范化建设。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅所注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

居民健康卡管理办法（卫办发〔2011〕94号）

居民健康卡技术规范（卫办发〔2011〕60号）

居民健康卡技术规范第二次修订说明（卫统中心便函〔2012〕26号）

居民健康卡生命周期管理办法(v1.0)（卫办综发〔2012〕26号）

居民健康卡个人化管理办法(v1.0)（卫办综发〔2012〕26号）

居民健康卡生产单位及产品备案管理办法(v1.1)（卫统中心便函〔2012〕26号）

居民健康卡安全存取模块（SAM）卡生命周期管理办法(v1.1)（卫统中心便函〔2012〕26号）

3 术语

下列术语适用于本文件。

3.1 居民健康卡 （Residents Health Card）

居民健康卡是中华人民共和国居民拥有的，在医疗卫生服务活动中用于身份识别，满足健康信息存储，实现跨地区和跨机构就医、数据交换和费用结算的基础载体，是计算机可识别的CPU卡。

3.2 居民健康卡注册管理中心（Center of Residents Health Card Registration and Management）

居民健康卡注册管理中心是负责居民健康卡的发行与使用监管、生命周期管理、密钥、SAM卡的分级下发管理、生产企业及产品备案管理的单位，按照居民健康卡的发行和管理模式，分为国家、省、市（县）注册管理中心。

3.3 居民健康卡SAM卡（Residents Health Card SecurityAccess Module Card）

居民健康卡安全存取模块（SAM）卡。SAM卡是一种具有特殊性能的CPU卡，用于存放密钥和加密算法，可完成交易中的相互认证、密码验证和加密、解密运算。居民健康卡SAM卡用作居民健康卡读/写卡设备的身份认证。

3.4 信息资源中心 （information resource center）

省级信息资源中心，汇聚省内医疗卫生机构产生的业务、管理、服务等信息资源，供居民健康卡注册管理信息系统及区域内医疗卫生机构使用。

3.5 居民健康卡注册管理信息系统（Information system of residents’ health card register management）

居民健康卡注册管理信息系统（以下简称卡管系统），是对居民健康卡业务进行分级管理的应用系统，为各级注册管理中心提供全面的居民健康卡注册管理功能，涵盖居民健康卡相关机构管理、居民健康卡管理、居民健康卡SAM卡管理、产品应用登记管理、统计分析、系统管理、接口管理等方面。

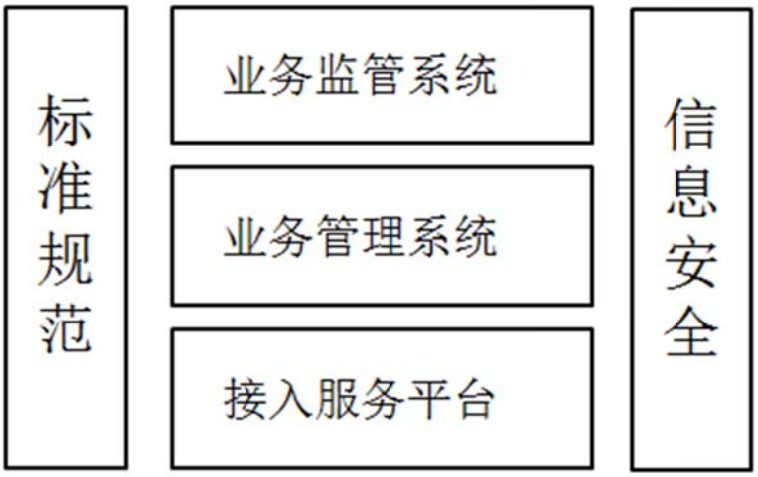
3.6 信息安全 （Information security）

信息安全是指信息网络的硬件、软件及其系统中的数据受到保护，不受偶然的或者恶意的原因而遭 到破坏、更改、泄露，系统连续可靠正常地运行，信息服务不中断。网络环境下的信息安全体系是保证 信息安全的关键，包括计算机安全操作系统、各种安全协议、安全机制（数字签名，信息认证，数据加 密等），直至安全系统，其中任何一个安全漏洞便可以威胁全局安全。信息安全服务至少应该包括支持 信息网络安全服务的基本理论，以及基于新一代信息网络体系结构的网络安全服务体系结构。

4 居民健康卡注册管理信息系统框架和技术要求

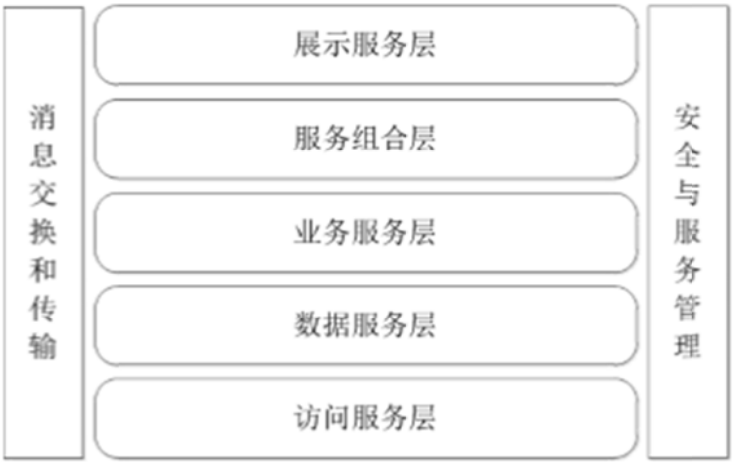
4.1 总体框架

居民健康卡注册管理系统按照功能主要分为业务监管系统和业务管理系统。业务监管系统主要部署在国家级，其核心职能是监管居民健康卡制卡、发卡、用卡各项业务流程的开展进行情况，同时负责多个业务管理系统间的数据交互；业务管理系统通常部署在省市级，主要承担具体业务。实际应用中，有时还会在医院端部署接入服务系统。不同层级之间通过数据交互实现连接，其总体框架如下图所示。



4.2 符合面向服务的体系结构的技术框架

居民健康卡注册管理系统采用面向服务的体系结构（SOA）的技术路线。在 SOA 体系结构中， 服务既可以是传统的基于 Web Service 的服务，也可以是目前面向互联网的基于 REST 的轻量级服务。



a）展现服务层 展现服务层定义企业信息门户（EIP）中可配置、可重用的门户组件（Portlets），用于支持门户 应用的开发；以及人机交互组件、网页组件、报表组件实现对不同客户接入方式的支持，并提供丰富的 客户端展现方式。在各级居民健康卡注册管理系统的应用中，卡信息查询、监管、报表等主要在展现服务层体现。同时，随着大量移动终端设备的出现，移动客户端应用同样可以用于健康卡信息的展现。

b）服务组合层服务组合层通过对下层的访问服务、数据服务、业务服务的编排来实现，流程编排的规则在该层内 定义，通过服务的编排组合就可以快速搭建出新的业务应用系统。在居民健康卡注册管理系统中，SAM卡申领报批、跨地区制卡查重等服务主要在服务组合层体现。

c）业务服务层 业务服务层定义那些可重用的业务处理过程，用于支持复合的业务处理需求。这层定义的业务处理 过程服务可能是单个原子事务的无状态处理操作服务，也可能是多个业务应用或异步服务之间交互的 有状态处理操作服务。业务服务层之上的开发者无需知道具体某项业务的逻辑处理过程。在居民健康卡注册管理系统中，注册服务、卡数据存储服务、制卡信息、居民信息管理服务等服务主要在业务服务层体现。

d）数据服务层 数据服务层定义的服务支持把异构的、孤立的企业数据转变成集成的、双向的、可重复使用的信息 资源。数据服务通过访问服务层以统一的方式访问企业的所有数据，数据服务层之上的开发者可以集中 精力处理数据的加工问题，而不必关注访问不同来源的数据的实现细节。在居民健康卡注册管理系统中，卡索引抽取、数据仓库等主要在数据服务层体现。

e）访问服务层 访问服务层实现与底层数据资源、应用资源的通信功能，使用通用标准接口，定义整合企业信息资 源（数据资源与应用资源）的各种访问服务，例如：不同类型的适配器以及专用的API等等。访问服务 屏蔽了企业信息资源（现在的或未来的）的技术和实现方式，访问服务层之上的开发者无需知道数据的位置、类型以及应用程序的编程语言等。在居民健康卡注册管理系统中，各级卡管系统数据交换层主要在访问服务层体现。

f）消息交换和传输 服务间的消息交换和消息传输贯穿的各个服务层。消息交换和传输可以采用企业服务总线ESB。服 务间的消息交换需要基于通用的交换标准和行业的交换标准。消息传输层可以提供通用的传输协议支 持，如HTTP、HTTPS、SMTP、JMS、FTP等。

g) 安全与服务管理 安全管、理和服务管理贯穿各个服务层。在居民健康卡注册管理系统中，信息安全与隐私保护主要在安全与服务管理层体现。服务安全管理支持认证和授权、不可否认和机密性、安全标准等。基于WS的服务的安全管理遵 循WS服务规范中WS-Security规范，其他形式的服务也需要提供安全保障 服务管理包括服务注册、服务发现、服务监控、服务治理等多方面的内容，本规范暂不对这些功能提出具体要求。

4.3 指导原则

a) 以 Web Service 技术作为 SOA 服务开发技术的首选技术，并要求遵循WS-I Basic Profile的有关指引；

b) 在选择 SOA 技术标准规范时，应重点定义“服务接口”和消息协议标准或规范，对服务内部功 能实现所采用的技术标准规范可不加限制；

c) 凡与 SOA 重用性密切相关的组件，如服务接口，必须采用成熟的技术标准规范；

d) 确保在居民健康卡注册管理系统上的业务数据是正确的，符合技术规范的要求。

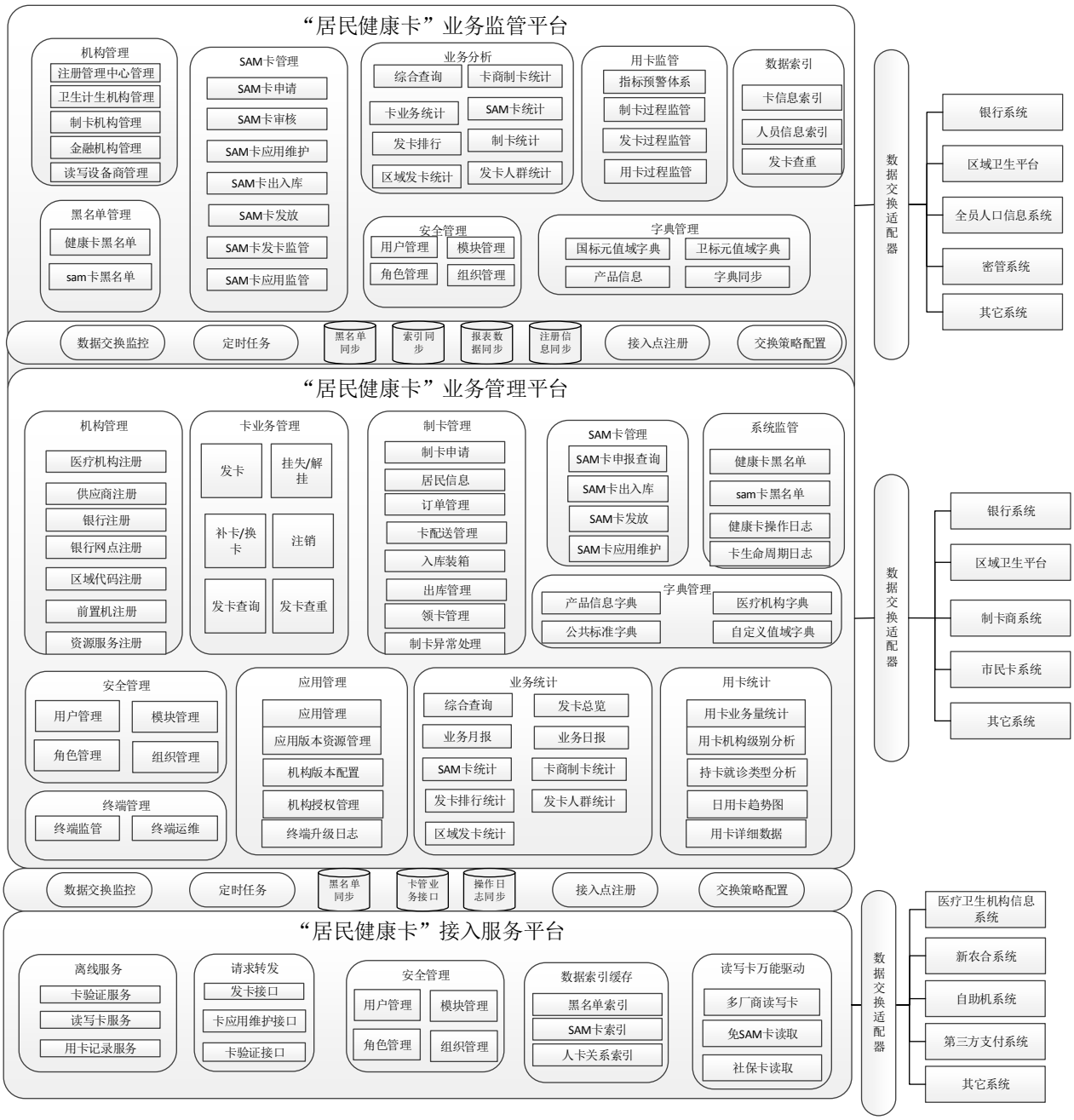
e) 居民健康卡注册管理系统的架构及功能满足卫生部制定的居民健康卡相关管理办法。

f) 对还没有最后定案的事实标准或规范，作为可选技术参考使用。

5 居民健康卡注册管理系统参考模型架构

5.1 系统技术架构

本规范中的系统技术架构在如图所示：



5.2 系统关键功能说明

系统功能设计应参照《居民健康卡注册管理系统基本功能规范》与《居民健康卡注册管理基本数据集》进行设计，本规范中只对系统关键功能进行简要描述。

5.2.1 机构管理

对居民健康卡相关机构信息进行注册及管理，包括卡注册管理中心、卫生计生机构、制卡机构、金融机构、卡读写设备生产机构信息的管理。系统使用组织机构代码对上述机构进行统一编码，并提供统一的注册、修改、注销、查询、打印及导出功能，

5.2.2 制卡管理

居民健康卡制卡管理主要由业务管理平台完成，包含居民健康卡注册管理信息系统对制卡过程的监督及居民健康卡申领登记、居民健康卡数据管理、居民健康卡制卡计划、居民健康卡制卡管理。

制卡过程中需要对制卡数据进行正确性及重复性校验，确保制卡数据正确及“一人一卡”。正确性校验主要通过与银行、公安等外部系统之间对接来完成，重复性校验则需要由各个业务管理系统定时上传所有卡注册信息到业务监管系统汇总，形成全国的卡片注册信息库，并在发卡前由业务监管系统进行批量或零星的查重验证;对于已经注册的重复卡信息由业务监管系统下发业务管理系统进行处理。

5.2.3 居民健康卡应用维护

系统提供居民健康卡进行挂失、解挂、补换卡、注销等管理操作，同时对居民健康卡的生命周期状态信息进行监控，对每个区域居民健康卡的挂失数、补换卡数以及注销数量进行统计分析，对卡片的数据进行监测、统计。

居民健康卡的挂失、注销操作会产生居民健康卡的黑名单。居民健康卡业务监管系统收集各业务管理系统及外部系统提交的黑名单数据，形成全国的健康卡黑名单信息库并下发到各业务管理系统，由业务管理系统提供居民健康卡黑名单核查服务或下发黑名单信息至卡应用受理机构进行黑名单核查。

5.2.4 SAM卡管理

居民健康卡SAM卡管理主要由国家居民健康卡注册管理信息系统完成，用于对SAM卡的制作、入出库进行监管，主要包含SAM卡制卡管理、 SAM卡贮存与流通管理、SAM卡应用维护、SAM卡黑名单管理、SAM卡应用监管功能。

SAM卡的冻结、注销操作会产生SAM卡的黑名单。居民健康卡业务监管系统收集各业务管理系统及外部系统提交的SAM卡黑名单数据，形成全国的SAM卡黑名单信息库并下发到各业务管理系统，由业务管理系统提供SAM卡黑名单核查服务或下发SAM卡黑名单信息至卡应用受理机构进行黑名单核查。

5.2.5 业务监管

居民健康卡注册管理系统对居民健康卡在制卡、发卡、应用过程中产生的业务数据，按照多条件、多维 度进行数据统计分析，并以多种展现形式（包括表格、线图、直方图、饼图等）进行展示。对于偏离阈值业务指标，系统提供报警机制，实现对整个业务情况的主动监管。

5.2.6 系统管理

提供统一的字典管理（含行政区划字典）、用户管理、权限管理、操作日志管理功能，并包含系统安全认证及鉴权体系。

5.2.7 接口管理

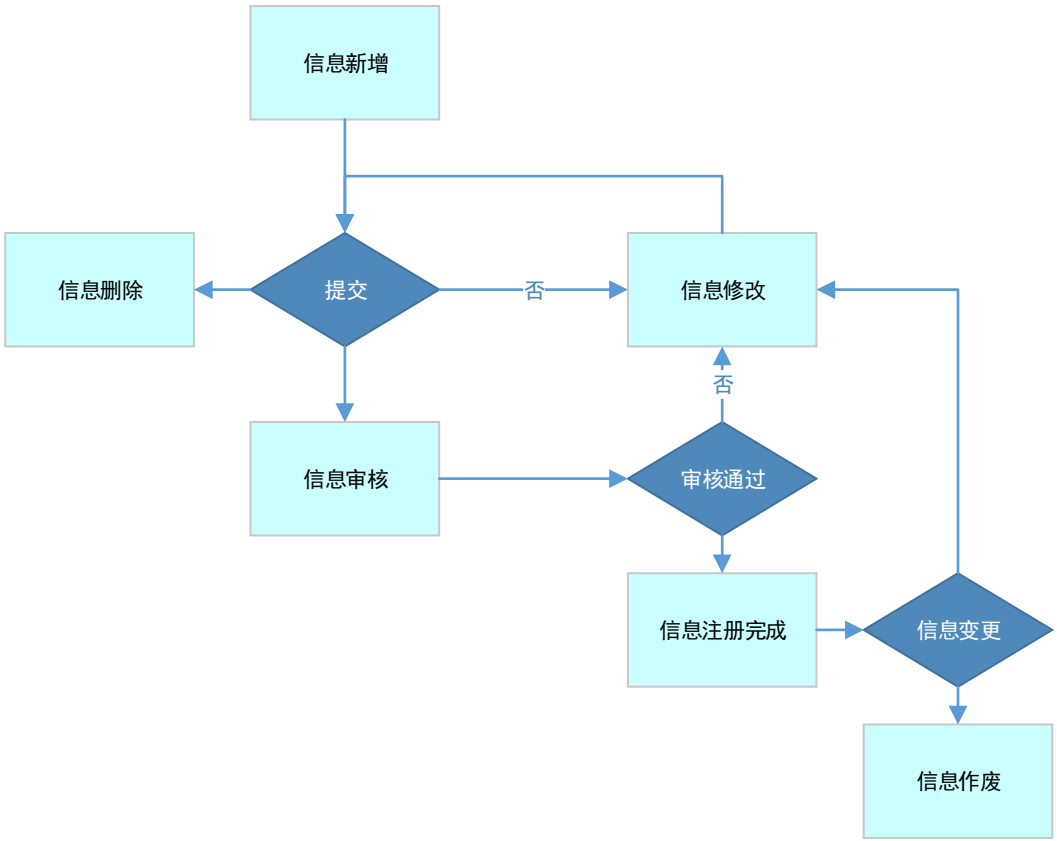
居民健康卡注册管理系统接口分为内部接口和外部接口。内部接口主要用于不同层级的注册管理系统间交换卡注册信息、黑名单信息、卡操作日志信息等数据，或提供查重校验、黑名单校验等服务；外部接口主要用于与外部系统的对接，如与金融机构系统、公安系统及区域人口健康信息平台等系统进行数据交换，或向卫生计生机构提供服务。

5.3 系统推荐工作流

系统中采用统一的工作流管理可实现对业务流程及数据交易的规范，可参考如下关键工作流进行设计：

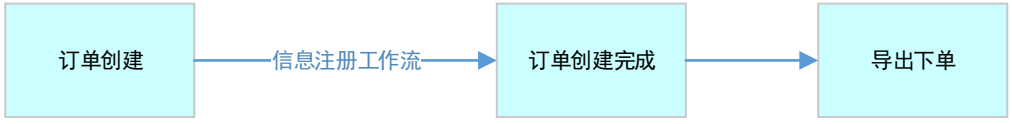
5.3.1 信息注册工作流

对系统中所有信息的注册，都应通过统一的注册管理工作流进行实现，如下图所示：



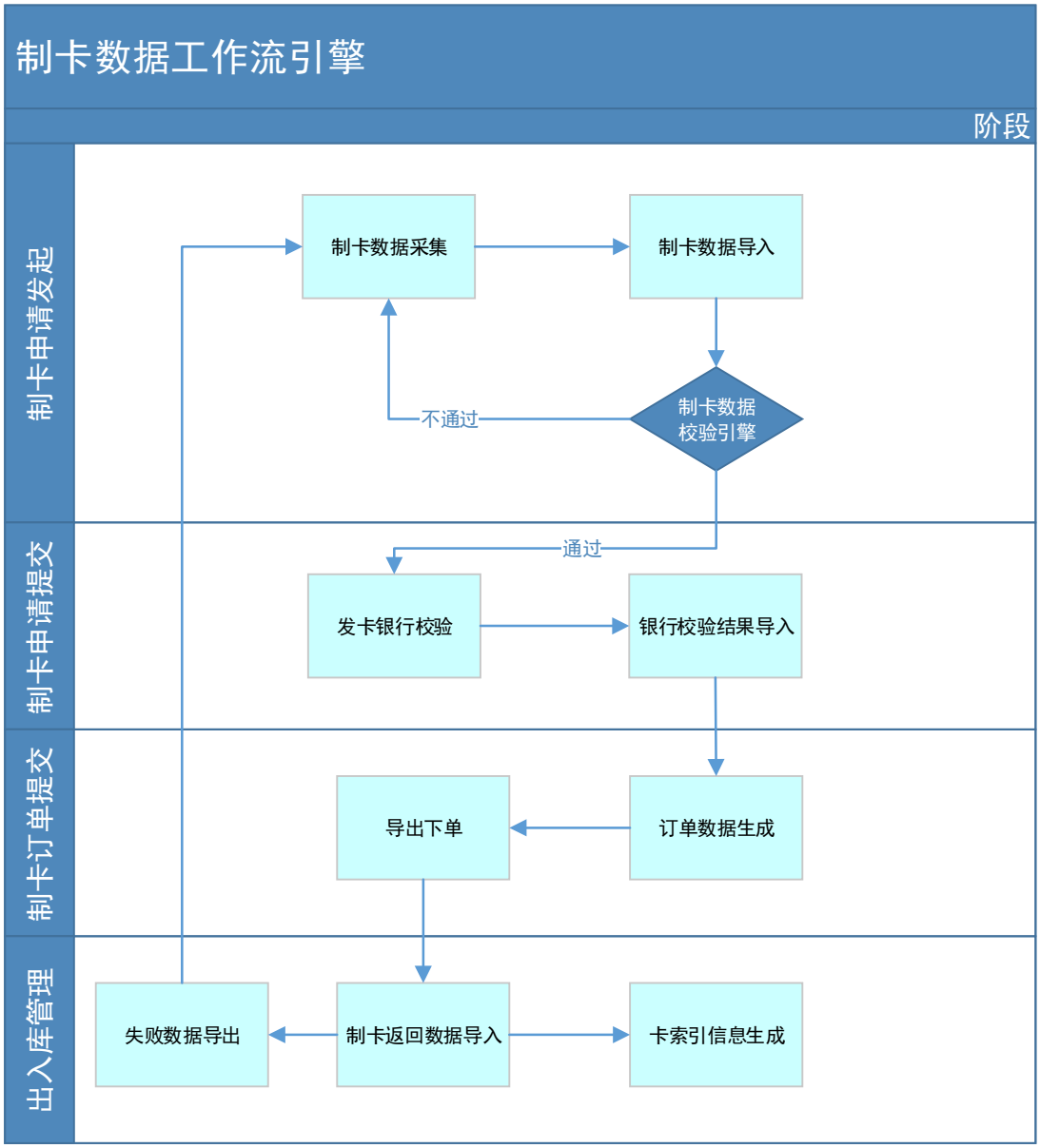
例如，对于一个制卡申请，应遵循：

而同样对于一个制卡订单，有：



5.3.2 制卡数据处理工作流

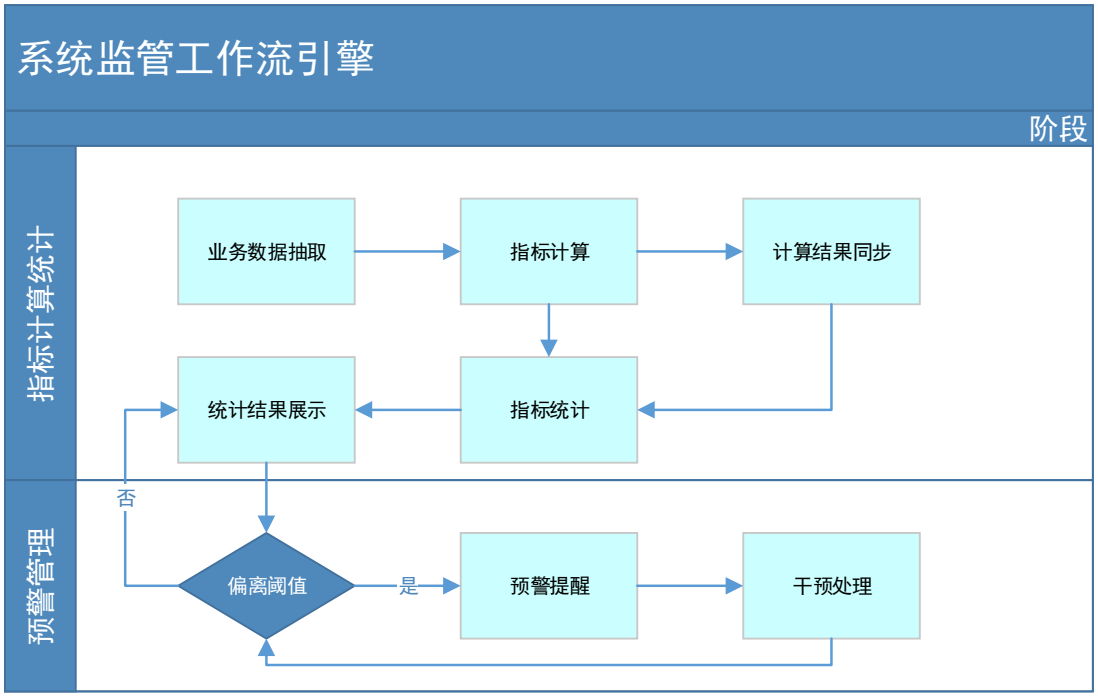
对于制卡数据的处理，应遵循统一的居民健康卡制卡数据处理工作流，如下图所示：



5.3.3 系统监管工作流

对于系统监管功能，应首先定义需要监管的指标，如下图：

指标定义应包含指标的定义、指标的的计算公式、指标的阈值等信息。完成指标定义后，应按照统一的系统监管工作流，完成各项指标的监管，如下图：

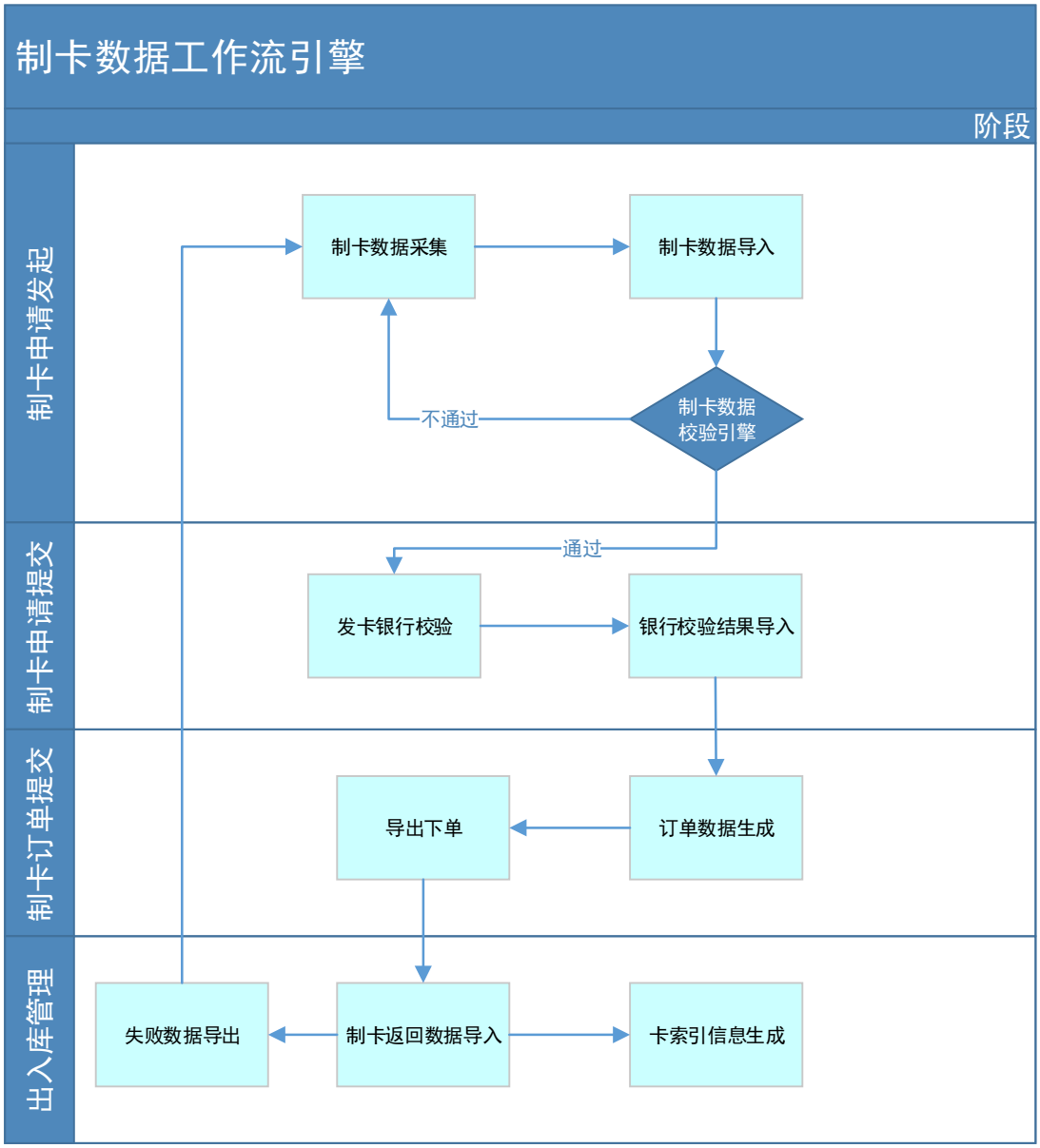


通过工作流中的预警体系，最终实现了系统主动监管。

5.3.4 数据交换工作流

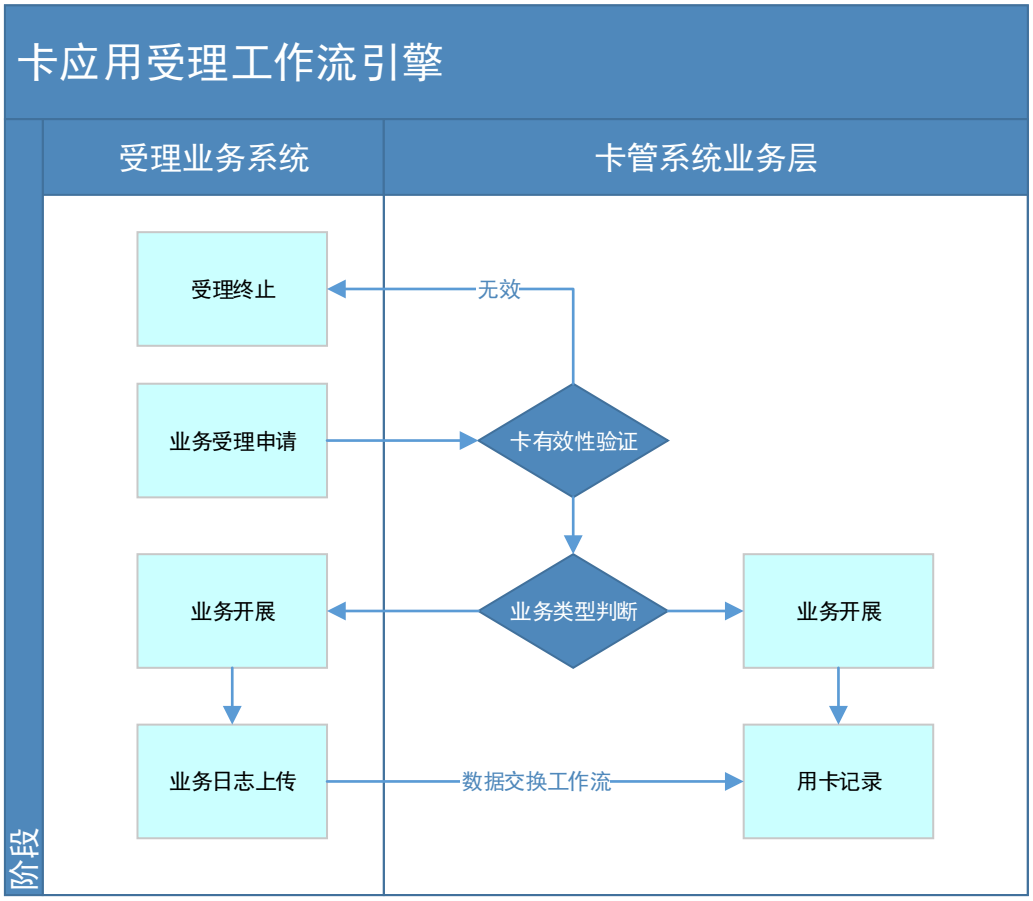
多级卡注册管理系统间存在数据交换，如卡索引信息、黑名单信息、注册信息、业务监管信息等。数据交换应当首先进行数据交换策略配置，如下图：

数据交换策略定义应按照具体业务需求进行定义，包括数据交换接口信息（如接口定义、接口地址等）、数据交换安全信息（如用户名、密码、加密信息等）、数据交换策略信息（实时交换、T+1定时交换等）、交换数据项等。各级卡管系统间的数据交换应遵循统一的数据交换工作流，如下图：



5.3.5 卡应用受理工作流

居民健康卡的应用通常在各个应用业务系统中完成，因此每拓展一项居民健康卡的新应用，都需要相应的业务系统与卡管系统进行对接，以完成卡生命周期及普通业务应用的管理。该对接过程应遵循统一的卡应用受理工作流，如下图：



5.4 外部系统对接

5.4.1 总体要求

在居民健康卡的制卡、发卡、用卡过程中，居民健康卡注册管理系统需要与大量的外部系统进行对接，提供相应的数据支撑或业务支撑，满足相关业务需求。与外部系统的对接，不仅需要卡注册管理系统具有良好的可扩展性，同时也应当遵循一定的原则：

a）同级对接：外部系统应当与同级卡注册管理系统对接，如省级全员人口库对接省级卡注册管理系统。

b）避免重复对接：外部系统不应同时对接多级卡注册管理系统，多级系统间的数据交互应在系统内部实现。

c）统一管理：卡注册管理系统应对接入的外部系统进行统一管理，能够完成接入情况的监管及控制

d）安全和性能：与外部系统对接的安全性及性能应满足相关规范或具体业务的要求。

5.4.2 外部业务系统对接要求

居民健康卡注册管理系统与外部业务系统的对接应通过专门的接入服务平台来实现，由接入服务平台对接各个外部业务系统，再统一接入居民健康卡注册管理系统业务层。居民健康卡接入服务平台应包括以下功能：

a）请求转发：对外部业务系统的请求，可转发至居民健康卡注册管理系统业务层进行处理。

b）数据缓存：缓存居民健康卡注册管理系统下发的数据，为外部业务系统提供离线数据支撑

c）离线处理：对外部业务系统的请求可进行一定程度的离线处理，避免与居民健康卡注册管理系统连接中断而导致业务无法正常开展

d）数据交换：能够按照数据交换工作流与居民健康卡注册管理系统间进行离线数据的交换。

e）读写卡驱动：提供多厂商的读写卡驱动封装服务，实现卡应用系统一键调用完成读写卡。

根据业务需求，居民健康卡接入服务平台也可以提供部分定制化的业务服务，如接入点用卡监管、终端签到签退功能等。

5.4.3 对接技术实现

居民健康卡注册管理系统与外部系统的对接应遵循居民健康卡注册管理系统技术指导原则，按照SOA技术框架要求提供对外的接口服务。系统应以 Web Service 技术作为实现接口服务的首选技术，也可根据具体业务、性能、安全需求采用离线文件、中间库等其它方式实现对接。

居民健康卡注册管理系统对外接口应充分考虑数据安全性，遵循相应的安全规范，采用接口身份认证、关键数据加密传输等技术手段，保障信息安全。

6 IT 基础设施规范

6.1 基本要求

用于搭建居民健康卡注册管理系统的IT基础设施（包括基础软件、数据库、服务器、存储、网络等），应满足以下基本技术要求：

a）可扩展性要求：应具有良好的横向可扩展性，满足业务系统的处理能力需求；

b）可靠性要求：应实现 IT 基础设施各环节的高可靠性，以保障系统稳定可靠运行；

c）管理自动化：需要提供标准化的接口以支持监控和管理功能，包括对状态、故障的监控，远程 维护等；

d）安全性要求：应遵循国内现有标准和规范要求，具体要求参照 9 安全规范。

6.2 基础软件

6.2.1 应用服务器软件

a）系统基本要求

1）支持主流操作系统；

2）支持主流数据库系统；

3）支持主流服务器虚拟化软件系统；

4）支持主流消息中间件；

5）提供对应用开发的主流框架的支持；

6）支持 Web Service 最新标准和规范；

7）兼容主流硬件服务器。

b）可扩展性要求

1）具有良好的横向扩展能力，实现应用级负载均衡；

2）在应用系统不停机的情况下，支持动态增加硬件服务器和应用服务器节点。

c）可靠性要求

1）应具有容错性，单个应用的部署和故障，不应影响其他应用的部署和运行，不应导致整个系统失效；

2）应通过冗余、集群等方式实现高可用性，单节点失效的情况下，可以持续提供服务；

3）应实现 HTTP 会话级别的故障恢复；

4）在数据库出现故障并恢复情况下，应用服务器应自动恢复数据连接，无需重新启动。

6.2.2 企业服务总线（ESB）软件

a）系统基本要求

1）支持主流操作系统；

2）支持主流数据库系统；

3）支持主流服务器虚拟化软件系统；

4）支持 Web Service 最新标准和规范；

5）支持主流消息中间件；

6）提供对应用开发的主流框架的支持，提供主流编程语言的实现接口；

7）兼容主流硬件服务器。

b）可扩展性要求

1）具有良好的横向扩展能力，实现负载均衡；

2）在企业服务总线不停止服务的情况下，支持动态增加硬件服务器和 ESB 节点。

c）可用性要求

1）应采用技术来保证平台 7*24 小时的运行；

2）应保证在数据量或应用连接数高峰运行时的系统运行正常，保障持久化的系统运行。

d）功能要求

1）应遵循 SOA 设计原则和技术标准,提供松耦合模式,实现业务逻辑和应用逻辑、数据逻辑 等分离；

2）支持智能路由支持，采用灵活的消息路由方式，支持基于消息内容的处理和路由；

3）支持标准 XML 数据的格式转换，可以通过多种方式实现转换功能；

4）提供发布/订阅功能，支持队列和主题两种订阅模式；

5）提供可靠的数据或消息传输,支持主流消息中间件，支持开放的通讯协议。

6.3 数据库管理系统

用于搭建居民健康卡注册管理系统的数据库，应满足以下基本技术要求：

a）系统基本要求

1）支持主流操作系统；

2）兼容主流硬件服务器，兼容主流存储架构；

3）支持主流的备份软件和数据同步软件；

4）兼容主流的应用服务器架构；

5）提供对应用开发的主流框架的支持，提供主流编程语言的实现接口。

b）可扩展性要求

应具有横向可扩展性，支持多节点集群或分布式部署，满足业务系统的处理能力需求。

c）可用性要求

数据库管理系统应支持以下方式实现系统的高可用性：

●故障恢复
●多种备份与还原方式
●基于时间点还原
●备份压缩
●数据复制
●数据库集群或分布式数据库

d）功能要求

1）关系型数据库和对象型数据库应提供对 SQL92 的完全支持以及 SQL99 的核心级别支持；

2）应满足数据库事务执行四要素（ACID）：原子性、一致性、隔离性及持久性；

3）可选支持以压缩的形式存储数据；

4）应支持 Unicode、GBK/GB2312 等多种字符集。

6.4 硬件服务器

6.4.1 基本要求

居民健康卡注册管理系统采用传统技术架构或云计算技术架构搭建,硬件服务器应满足如下技术 要求：

a）配置合理：服务器的资源配置应该尽量与业务需求相匹配，实现资源的均衡使用；

b）可扩展性要求:服务器应具有横向和纵向可扩展性,满足业务系统的处理能力需求；

c）管理自动化：服务器需要提供标准化的接口以支持监控和管理功能，包括对状态、故障、能耗、 温度的监控，远程启动、访问和维护等；

d）高能效：服务器自身应该具有较高的性能/功耗比，具有良好的散热设计，具有良好的环境适 应能力（较宽的温度、湿度范围等），应遵循《HJ 2507-2011 环境标志产品技术要求 网络服 务器》的要求。

6.4.2 系统要求

a）支持主流操作系统；

b）采用开放式架构和处理器；

c）支持主流的内存型号,内存支持 ECC 纠错；

d）支持普通硬盘或固态硬盘，并支持热插拔技术；

e）支持磁盘阵列技术；

f）支持多种主流存储架构，包括 FC SAN、IP SAN、NAS，可选支持 FCoE 技术；

g）系统 I/O 插槽数量及集成网络端口数量可扩展；

h）网络接口要求

●支持千兆以太网技术，可选支持万兆以太网技术；
●支持网络端口聚合功能；
●支持网络端口故障切换功能；
●可选支持硬件虚拟化辅助技术；
●可选支持网络加速功能。

i）供电：提供单电源/冗余电源可选。

6.4.3 可扩展性要求

服务器系统应满足可扩展性要求，建议采用开放式架构服务器系统，满足平台及应用处理能力需求。

a) 横向扩展要求

1) 服务器系统应具备组成一定规模的多结点计算系统的能力，提供便利的软硬件部署及管理模式。

2) 如果采用云计算技术架构部署，服务器系统应支持动态资源分配和自动化管理。

b) 纵向扩展要求

●CPU 扩展能力：在同一主板上支持多个 CPU 插槽，且在提供多个 CPU 插槽的同时支持用户选配 CPU 个数。

●内存扩展能力:在同一主板上支持多个内存插槽,可以通过内存扩展板进行扩展。

●硬盘扩展能力:在一个机箱内支持多块硬盘槽位。支持 SATA/SAS/SSD 类型硬盘。

●网卡扩展能力：提供 2 个或多个千兆以太网卡，可选支持 10Gb 的网络接口。

●电源扩展能力：一个机箱支持多个电源模块，为主机提供供电保障。

6.4.4 可靠性要求

居民健康卡注册管理系统选择主机系统应具备多种高可靠性保护措施，例如，内存ECC保护，硬盘RAID，冗余电源、可调频风扇等。具体包含：

a) 内存可靠性要求 主机系统应提供内存保护功能,为需要更高等级可用性的应用提供了增强的容错能力。用户将能够 按照自己的意愿来选择系统内存保护级别：

1) 服务器内存提供 ECC 功能

2) 根据内存可靠度要求，可选支持高级 ECC 内存保护技术或内存镜像

b) 硬盘可靠性要求

1) 应支持 RAID 技术，保证磁盘系统的高可靠性，提高持续工作而不发生故障的能力，宜包 含但不限于：RAID0、1、0+1、5 等级别

2) RAID 卡宜支持缓存电池保护

c) 整机可靠性要求

1) 热插拔：用户在不需要切断电源的情况下，对部件进行更换，保证主机正常运行。用户可 以按照需求选择不同部件热插拔功能，内存热插拔、硬盘热插拔、PCI-E 热插拔、电源模 块热插拔、风扇热插拔等。

2) 冗余部件：关键部件（内存、硬盘、电源、风扇等）应提供冗余部件，当一个部件出现故 障，另外的部件能支撑主机系统正常运行，故障部件可以进行维护和更换。

3) 故障诊断：当主机出现故障时，能够快速定位故障部件，并向管理人员发出报警指令，例如：短信报警、邮件报警、蜂鸣报警等。

6.4.5 虚拟化技术支持

a) 虚拟化软件要求

1) 虚拟化软件可以支持资源分拆，从逻辑角度而不是物理角度来对资源进行分配和使用，即 从单一的逻辑角度来看待不同的物理资源。

2) 兼容市场上主流的服务器设备，兼容市场主流操作系统和主流的应用软件。

3) 虚拟机之间应实现相互独立，每个虚拟机之间做到完全隔离，其中某个虚拟机的故障不会 影响同一个服务器上其他的虚拟机的运行。

4) 支持存储虚拟化和网络虚拟化。网络虚拟化需要支持虚拟网络隔离，不同的虚拟机可以处 于不同的网络，保证即使位于同一物理服务器上的虚拟机也可以互相隔离。
5) 支持虚拟机的生命周期管理，包括虚拟机的创建、启动、暂停、恢复、重启、关闭等。
6) 支持虚拟机状态的监控，包括虚拟机存储信息监控，虚拟网络信息监控和虚拟机的图形化 控制台的查看。
7) 具备快速部署能力，可以在短时间内完成虚拟系统的搭建，并支持批量创建虚拟机。
8) 支持动态调度能力。当需要系统节能时，可以通过调度集中虚拟机，并且休眠部分服务器。当某个服务器负载过重时，可以通过调度将虚拟机进行动态迁移，满足负载均衡的需要。 上述调度必须保证虚拟机内的服务不能停止。
9) 支持灵活的管理方式。支持对虚拟化系统的远程集中管理，支持基于 web 方式的平台管 理。
10) 支持在主流分布式文件系统上创建虚拟机。

b) 主机对虚拟化支持要求
1) 主机能够支持主流的虚拟化软件；
2) 所有主机系统应支持同一个虚拟化引擎；
3) 处理器、I/O 和网络接口应支持虚拟化硬件辅助功能。

6.4.6 服务器可管理性要求

服务器的管理体系应满足对居民健康卡注册管理系统中数量较多的服务器管理要求，便于系统管理员对硬件层面的管理和控制。管理人员应能通过统一接口来管理和监控资产信息、能耗状况、健康状况、性能状况等一系列信息。

a) 管理功能要求。服务器应支持独立于操作系统的带外管理功能，包括：
1) 资产管理，可以获取服务器资产状况，包括型号及序列号、配置信息、固件版本管理。
2) 配置管理
- 支持将服务器所需软件（操作系统、补丁、应用等）自动分发给该服务器；
- 支持自动执行部署服务器软件，包括自动部署操作系统或者专有的应用。

3) 远程控制，应支持管理员通过远程的方式来管理和控制，提供健康状况监测和日志查询。 可选支持 KVM Over IP，可选支持虚拟介质（如光驱重定向）。
4) 故障管理，应在服务器前后面板、服务器内部分别提供工作状况指示灯，指示服务器各个 部件的工作情况，包括电源、整机健康状况、内部部件（CPU、内存、电源模块、硬盘灯）。 刀片服务器应提供刀片机箱及刀片机箱关键部件工作及健康状况指示灯。

b) 管理接口。应提供独立的管理网口，并支持 IPMI 管理协议、SNMP 管理协议和 SNMP TRAP 机制 以及基于 HTTP 的远程管理。

6.5 存储系统

6.5.1 基本要求

存储系统应满足居民健康卡注册管理系统目前建设需求及未来发展需求。在满足平台建设需求 的前提下，尽量采用优化设计，使数据存储系统能够满足用户需求的高可稳定性、高扩展性、异构性、 兼容性、易维护性等需求。 存储系统应具备以下特点：

a) 高可靠性： 在系统整体设计中应选用高可靠性存储产品，设备充分考虑冗余、容错能力和备 份，同时合理设计存储网络架构，最大限度保障系统正常运行。
b) 可扩展性：存储网络支持平滑扩充和升级，避免在系统扩展时对存储网络架构的大幅度调整。
c) 易管理性：支持集中监控、分权管理，以便统一分配网络存储资源。支持故障自动报警。
d) 高性能：应保障存储设备的高吞吐能力，保证数据的高质量传输，满足性能要求，避免存储瓶 颈影响整体的系统应用。
e) 先进性和成熟性：存储设备应采用先进的技术和制造工艺；在容量扩展支持、数据空间分配， 抵御病毒攻击、高性能方面应保持技术领先；网络结构和协议应采用成熟的、普遍应用的并被 证明是可靠的结构模型和技术。
f) 标准开放性：支持国际上通用标准的存储协议、国际标准的应用的开放协议，保证与其它主流 服务器之间的平滑连接互通和兼容性，以及将来网络的扩展性。
g) 环保节能：应满足环保与节能的要求，噪声低、耗电低、无污染。

6.5.2 存储可用性要求

存储系统需提供全年不断电无停止服务，确保高可靠性：全年不下电，不停机，不闪断。

a) 出现故障及时进行告警（声音、灯闪），告警分等级，界面可见，具有详细说明和修复手段提 示；
b) 要求存储设备有 RAID 保护机制，在用户数据写单份的情况下，要求数据访问的可靠性达到 99.999%；
c) 要求支持存储断电保护功能，并提供永久缓存数据保护；
d) 要求用户数据可靠性可灵活配置，支持设置用户数据的副本数、是否异地存放，向用户提供不 同级别的可靠性保护；
e) 要求任意两块磁盘或单个存储节点损坏，不会导致用户数据丢失；
f) 要求任意磁盘或存储节点故障，不影响云存储平台其他设备的正常使用和用户访问；
g) 产品电位接地，防止触电事故；
h) 尺寸、规格、形状合理，以免倾斜倒伏，碰撞； i) 产品材质耐温，散热；
j) 明确警示触电、有毒害、或其它危险发生的可能。

6.5.3 存储易管理性要求

a) 配有存储管理软件，应实现 FCSAN、IPSAN、NAS 一体化统一管理，提供全中文管理界面；
b) 支持包括 RS232 串口、10/100M 以太网口、Telnet 方式、图形界面、CLI 命令行等多种管理方 式；
c) 软件内置于存储系统内部，提供的存储管理软件可以在本地或远程设置，管理，监测和调整盘 阵的运行；
d) 支持故障预警功能，提供包括 LED 指示灯报警、蜂鸣报警、Email 报警、日志报警、SNMP 报警 等多种报警方式。

6.5.4 存储配置要求

由于各级平台业务量差异巨大，本规范定义了国家、省、市三个级别的存储配置要求。

地市级别存储配置要求

平台在线存储系统容量估算：采取集中式存储系统，注册系统、索引系统、HER 交易缓存（HIAL） 和 HER 数据系统约为 80-100GB/年。影像数据的存储配置应单独计算。

存储配置要求：

a) 在线存储要求：

●关键部件（控制器、电源、风扇等）采用热拔插模块化设计，内部连接无线缆；

●应支持 IPSAN/FCSAN 存储网络架构，可支持 NAS 异构统一平台，兼容异构存储。

●支持 iSCSI、NFS、CIFS 等多种文件共享协议，可安装部署于多种操作系统并存的复杂网络环境中；

●应支持 iSCSI 主机接口，可支持 FC 主机连接。

●应 SAS/SATA 硬盘，可支持 SSD/FC/硬盘。支持 300/450/600GB 高转速 SAS 磁盘，支持 500/1000/2000GB 高转速 SATA II 磁盘，实配容量≥1TB；最大扩展容量≥80TB。

●大缓存，缓存≥8GB，最大缓存≥24GB；

b) 灾备系统要求：

●支持本地的连续数据保护功能，存储应具有连续数据保护功能，可以满足数据恢复要求苛刻的 RTO/RPO 指标，快速准确的恢复故障前数据。

●可支持数据卷隔离映射功能、重复数据删除、自动精简配置、数据快照功能、快照回滚、远程卷复制（同步/异步）、基于快照的远程数据复制远程数据恢复、逻辑分区动态扩容。

●应支持远程容灾功能，结合本地连续数据保护功能，可实现数据级及应用级的容灾。

c) 离线存储要求：

●可选用虚拟带库或物理带库设备，支持 LT03\LT04\LT05 驱动器 支持 IP 主机接口，可支持 FC 主机接口

●配置容量≥2TB，最多支持存储容量≥200TB 支持 LT03\LT04\LT05 驱动器

省级级别存储配置要求

平台在线存储系统容量估算：采取集中式存储系统，注册系统、索引系统、EHR交易缓存（HIAL）和EHR数据系统约为200-500GB/年。影像数据的存储配置应单独计算。

存储配置要求：

d) 在线存储要求：

●关键部件（控制器、电源、风扇等）采用热拔插模块化设计，内部连接无线缆；

●支持 IPSAN/FCSAN 存储网络架构和 NAS 异构统一平台，兼容异构存储，支持存储虚拟化，实现存储资源的整合再利用，提高用户的投资回报率；

●支持 iSCSI、NFS、CIFS 等多种文件共享协议，可安装部署于多种操作系统并存的复杂网络环境中；

●支持 iSCSI、FC 主机连接，无缝接入用户现有应用环境，满足不同客户不同应用对数据存储系统的差异化需求；

●全面支持SSD/FC/SAS/SATA硬盘，支持300/450/600GB高转速FC磁盘；支持300/450/600GB 高转速 SAS 磁盘，支持 500/1000/2000GB 高转速 SATA II 磁盘，支持 100GB SSD 硬盘，实配容量≥3TB；最大扩展容量≥100TB，灵活配置满足不同层级数据存储需求；

●高缓存，缓存≥16GB，最大缓存≥32GB；

●异构整合、集中部署，统一管理，降低整体拥有成本（TCO）。

e）灾备系统要求：

●支持本地的连续数据保护功能，存储应具有连续数据保护功能，可以满足数据恢复要求苛刻的 RTO/RPO 指标，快速准确的恢复故障前数据。

●支持数据卷隔离映射功能、重复数据删除、自动精简配置、数据快照功能、快照回滚、远程卷复制（同步/异步）、基于快照的远程数据复制远程数据恢复、逻辑分区动态扩容。

●支持远程容灾功能，结合本地连续数据保护功能，可实现数据级及应用级的容灾。

f）离线存储要求：

●可选用虚拟带库或物理带库设备，支持 LT03\LT04\LT05 驱动器

●支持 FC 或 IP 主机接口

●配置容量≥6TB，最多支持存储容量≥200TB

●支持 LT03\LT04\LT05 驱动器

国家级别存储配置要求

在线存储系统容量估算:采取集中式存储系统,注册系统、索引系统、EHR交易缓存(HIAL)和EHR 数据系统约为600GB-1TB/年。各地市可结合实际情况增配存储容量。影像数据的存储配置应单独计算。存储配置要求：

a）在线存储要求：

●关键部件（控制器、电源、风扇等）采用热拔插模块化设计，内部连接无线缆；

●支持 IPSAN/FCSAN 存储网络架构和 NAS 异构统一平台，兼容异构存储，支持存储虚拟化，实现存储资源的整合再利用，提高用户的投资回报率；

●支持 iSCSI、NFS、CIFS 等多种文件共享协议，可安装部署于多种操作系统并存的复杂网络环境中；

●支持 iSCSI、FC 主机连接，无缝接入用户现有应用环境，满足不同客户不同应用对数据存储系统的差异化需求；

●宜全面支持 SSD/FC/SAS/SATA 硬盘，支持 300/450/600GB 高转速 FC 磁盘；支持 300/450/600GB 高转速 SAS 磁盘，支持 500/1000/2000GB 高转速 SATA II 磁盘，宜支持100GB SSD 硬盘，实配容量宜≥6TB；最大扩展容量宜≥200TB，灵活配置满足不同层级数据存储需求；

●高缓存，缓存宜≥32GB，最大缓存宜≥64GB；

●异构整合、集中部署，统一管理，降低整体拥有成本（TCO）。

b）灾备系统要求：

●支持本地的连续数据保护功能，存储需要具有连续数据保护功能，可以满足数据恢复要求苛刻的 RTO/RPO 指标，快速准确的恢复故障前数据。

●支持数据卷隔离映射功能、重复数据删除、自动精简配置、数据快照功能、快照回滚、远程卷复制（同步/异步）、基于快照的远程数据复制远程数据恢复、逻辑分区动态扩容，支持远程容灾功能，结合本地连续数据保护功能，可实现数据级及应用级的容灾。

c）离线存储要求：

●可选用虚拟带库或物理带库设备，支持 LT03\LT04\LT05 驱动器

●支持 FC 或 IP 主机接口

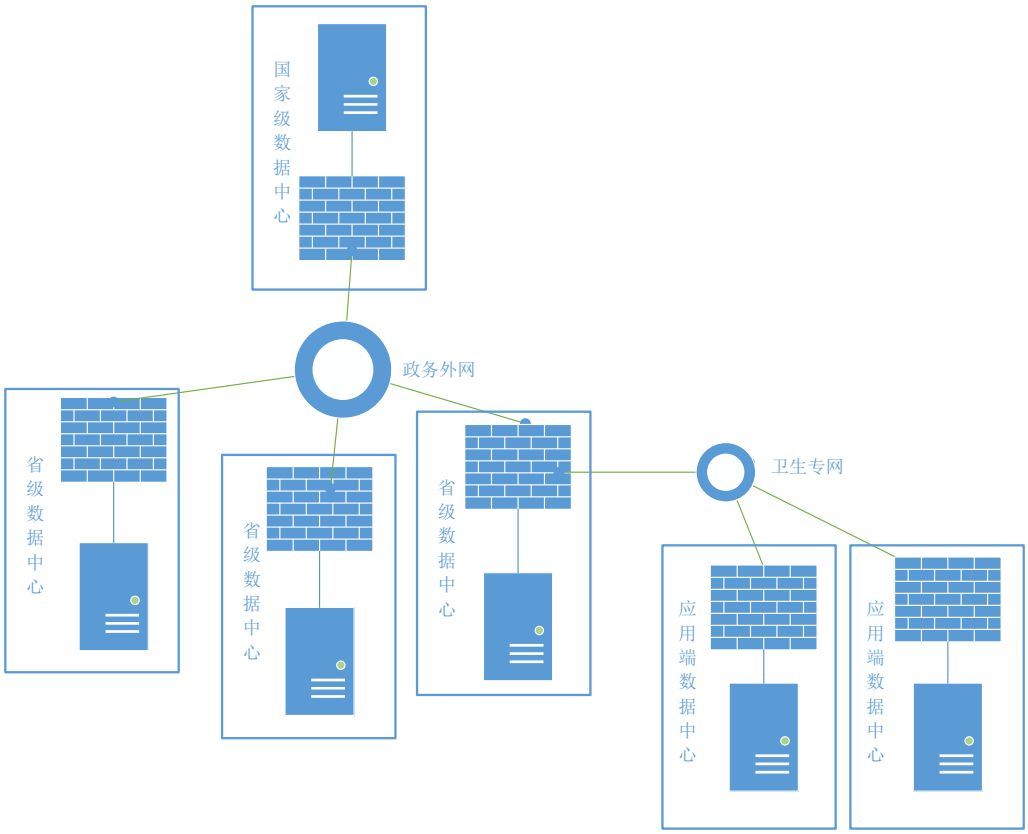
●配置容量宜≥12TB，最多支持存储容量宜≥400TB

●支持 LT03\LT04\LT05 驱动器

6.6 网络系统

6.6.1 居民健康卡注册管理系统网络参考架构

本技术规范中的系统网络参考架构如下图所示：



整体网络应由两大部分组成：国家电子政务外网及地方卫生专网。

a) 地方卫生专网主要负责支撑省市级居民健康卡注册管理系统的运行和管理，以及与外部系统的连接。

b) 国家政务外网连接国家级与省级居民健康卡注册管理系统，实现各省间的互联互通。

6.6.2 居民健康卡注册管理系统区域划分

居民健康卡注册管理系统网络按照功能从逻辑上划分，应至少包括以下区域，各区域间需通过防火墙进行安全隔离。

a) 骨干网络区域　　该区域主要实现以下功能

1) 对各接入点远程接入链路进行汇聚

2) 连接各级居民健康卡注册管理平台

3) 对各级居民健康卡注册管理平台数据进行高速转发处理

b) 业务系统区域　　该区域主要包括以下业务相关设备

1) 应用服务器

2) 数据库服务器

3）中间件服务器
4）数据存储设备

c）安全管理区域　　该区域主要实现以下功能
1）证书服务器
2）身份认证
3）漏洞扫描
4）入侵检测
5）网络管理

d）数据灾备区域　　该区域主要实现以下功能
1）作为远程灾备
2）实现业务系统与灾备区域数据的同步
3）通过高速链路直接与核心交换机

e）外联出口区　　该区域主要实现以下功能
1）负责连接外联单位
2）将来实现域间互连互通时提供开放接口

f）管理接入区　　该区域主机负责将居民健康卡注册管理系统的行政管理部门接入数据中心

6.6.3 网络带宽要求

接入带宽要求

a）三级医院接入带宽宜≥1000M b）二级医院接入带宽宜≥100M c）社区服务中心接入带宽宜≥8M d）社区服务站接入带宽宜≥4M e）行政管理接入带宽宜≥100M f）其他医疗卫生机构应结合业务要求进行配置

居民健康卡注册管理系统骨干区域带宽要求

a）对于 100 万人口以下规模的区域，核心交换设备宜达到千兆接入速率；

b）对于 100 万人口以上规模的区域，核心交换设备宜达到万兆接入速率。

6.6.4 骨干网络设计要求

网络可靠性

a）设备级别可靠性要求　网络设备支持风扇冗余　网络设备支持电源冗余　核心设备应提供关键部件的冗余备份，关键组件支持热插拔与热备份　核心设备应支持引擎冗余，引擎自动切换　核心设备应支持主流保护技术提高业务恢复能力，实现无中断业务运行

b）网络级别可靠性要求

●汇聚设备通过两条以上链路与核心设备相连
●服务区接入交换机通过两条以上链路与核心设备相连
●安全管理区设备通过两条以上链路与核心设备相连
●核心设备采用两台或以上进行冗余
●核心设备应支持 IP、LDP、VPN、TE 快速重路由
●核心设备应支持 Hot-Standby，IGP、BGP 以及组播路由快速收敛
●核心设备应支持虚拟路由冗余协议（VRRP，Virtual Router Redundancy Protocol）
●核心设备应支持快速环网保护协议（RRPP，Rapid Ring Protection Protocol）
●核心设备应支持 TRUNK 链路分担备份　核心设备应支持 BFD 链路快速检测

6.6.5 服务点系统接入设计要求

网络可靠性

a) 支持双出口备份，选择两家不同的运营商提供的物理链路接入作为互备

b) 支持接入设备双机备份

c) 支持快速切换 1) 网关异常时，包括网关瘫痪、重启等需要网关能快速切换 自动侦测特性能够保证在 1～2 秒内发现故障 VRRP 在 3～4 秒内完成主备网关的切换 网关内外都设置 VRRP 组，并将这一对 VRRP 组关联起来 2) 网关链路异常时，需要 VPN 隧道能快速切换

6.6.6 网络规划要求

IP 地址规划

a) 居民健康卡注册管理系统 IP 地址规划要求 IP 地址的分配必须采用 VLSM(Variable Length Subnet Mask，变长掩码)技术，保证 IP 地址的利用效率 需采用 CIDR(Classless Inter-Domain Routing，无类别域间路由)技术，这样可以减小路由器路由表的大小

b) 在规划 IP 地址时，应结合本地电子政务外网或其他资源网络（如新农合网，社保网）的部署，综合考虑 IP 地址资源分配。

c) IP 地址规划需参照的标准和规范

●RFC 1366 《Guidelines For Management of IP Address Space》

●RFC 1466 《Guidelines For Management of IP Address Space》

●RFC 1597 《Address Allocation for Private Internets》

●RFC 1918 《Address Allocation for Private Internets》

●RFC 0793 《Transmission Control Protocol》

●RFC 0791 《Internet Protocol》

6.6.7 网络管理要求

拓扑管理

系统应提供物理拓扑树、IP视图、时钟视图、隧道视图、自定义视图，用户从可以从不同的角度浏 览视图，实时了解和监控整个网络的运行情况。

拓扑管理需支持以下功能：

a) 拓扑图基础功能

●鸟瞰图：可方便定位拓扑窗口显示的区域

●全网网元统计：可统计全网网元类型和各种类型网元的数量

●拓扑缩放：视图支持缩小和放大

●过滤树：可快速过滤出用户关注网元

●拓扑视图：需反映网络中的各种物理和逻辑实体，并提供了各种操作的入口

b) 支持拓扑告警显示：使用不同的颜色或图标表示子网和网元状态的方式

c) 支持拓扑自动发现：系统应提供拓扑自动发现，无需人工干预。

性能管理

需要对网络的关键性能指标进行监控，并对采集到的性能数据进行统计，为用户对网络性能进行管理。性能管理需支持以下几部分功能：

a) 监控实例管理

●用户可以按照预先设置的模板和定时策略对指定设备的资源进行性能数据收集。

●监控实例包括数据监控实例和阈值告警监控实例。

b) 监控模板管理

●数据监控模板：可对性能指标进行采集，并收集网络资源的性能数据。可以为指标或指标组建立数据监控模板。

●阈值告警监控模板：可用于采集指定阈值的指标。通过为指定的资源设置阈值告警监控模板，可以监控指定资源的告警。

c）历史性能数据浏览：

●网络历史性能数据可以通过折线图、柱图、图表的方式显示。

●以多种格式对性能数据进行保存。

安全管理

需要对网管系统本身的安全控制，通过对用户、用户组、权限和操作集等管理，保证网管系统的安全。网管安全管理须支持以下几部分功能：

a）登录和会话管理

b）用户和用户组管理：

●新建用户帐号和用户组管理；

●修改用户和用户组信息；

●删除用户帐号和用户组。

c）权限管理：

●用户权限包括管理权限和操作权限

●管理权限是指用户可以管理的设备范围及其配置数据范围，或者用户所属用户组可以管理的指定区域。在拓扑视图上用户不可管理的设备是不可见的，用户所属用户组不可管理的区域也是不可见的。

●操作权限是指用户可以执行的具体操作。如果一个用户对某一设备没有管理权限，也就不具有该设备的操作权限。

d）安全策略管理：

●设置密码策略用来设置用户密码规则和密码安全策略。

●密码规则包括普通用户密码长度最小值、超级用户密码长度最小值和密码长度最大值。

●密码安全策包括密码不能与历史密码重复次数、密码最长存留天数、密码最短存留天数和密码到期前提前提示天数。

●设置帐户策略用来设置用户名最小长度、自动解锁时间、用户登录时的最大登录尝试次数、登录或解锁失败延时时间等。

e）地址访问控制：限制用户只能从特定IP地址的客户端登录服务器。如果客户端需要通过远程方式登录服务器，必须 先配置地址访问控制列表。

告警管理

告警管理需要对网络中的异常运行情况进行实时监视，通过告警统计、定位、提示、重定义、相关性分析、告警远程通知等手段，便于网络管理员及时采取措施，恢复网络正常运行告警管理包括需支持以下功能：

全网告警监视

●告警统计

●告警屏蔽和相关性分析

●告警转储和确认

●告警同步

●告警重定义：通过告警重定义功能，用户可以根据实际需要重新设置某些告警的级别

●告警抑制：某个告警为抑制状态后，后续不再上报该告警

●告警跳转：告警定位功能，从告警跳转到产生该条告警的拓扑对象
●告警维护经验库
●告警时间本地化：所有告警的产生、确认、清除，到达网管时间均显示为网管本地时间
●多种告警通知手段：支持电子邮件、短消息等告警远程通知

故障管理

a) 故障采集应支持如下类型：

●硬件类问题
●系统类问题
●二层网络问题
●三层网络及路由问题
●组播问题
●接口对接问题

QOS 问题

b) 故障采集应支持以下几种方式：

●支持直连方式采集：管理终端与待采集设备可通过网线或者串口线直接相连，通过Telnet、 SSH 或串口方式连接设备
●支持自动代理方式采集：能够确定代理的设备类型时，选用自动代理
●支持手工代理方式支持：不能确定代理的设备类型时，选用手工代理
●支持“VPN 实例”方式支持：设备位于 VPN 私网中，选用VPN 实例方式

报表管理

网络管理系统需要能针对IT资源的监控参数,根据管理人员的要求制定周期性的参数监控并产生相应的报表。系统需产生以下基础类型报表：

a) 告警和日志类报表

●设备告警级别分布明细报表
●设备告警级别分布报表
●设备通断统计报表
●通用告警信息报表
●历史变更记录报表

b) 资源类报表

●端口资源统计报表
●以太网端口资源统计报表
●以太网网元间业务资源统计报表
●组网图

日志分析

系统需支持通过对设备日志进行分析，实现对日志的结构化显示，并支持对重要信息的过滤搜索等功能。日志分析需要支持的功能包括：

●文件操作：日志文件的打开、保存
●配置管理：为选择的日志文件配置解释库，以便在解释库栏输出选中的日志对应的解释信息
●日志记录列显示、列隐藏
●日志记录排序：使当前页中的日志记录按照指定的方式进行排序
●日志记录批注：提供批注的插入、编辑、浏览和删除功能

●搜索功能：包括对当前页、当前文件、所有文件进行搜索；用户可以根据关键字进行搜索

●过滤功能：只显示带有用户所选指定项的日志记录，其他日志记录被隐藏

●输入日志的解析：解析用户手工输入的日志，并且可以选择解释库，对解析后的日志进行解释

网络巡检

系统需依据网络IT设备的巡检检查列表、相关预警及专家的经验，对设备配置和日常运行情况进行 定期巡检和维护。对于设备中不符合规范的配置和出现的问题，巡检工具应给出相应的报告和提示信息， 同时提供处理意见和措施。

a) 巡检应包含以下项目：

●设备单板版本的预警信息

●版本及补丁是否规范使用

●设备基本配置

●设备单板运行状况

●业务模块运行是否正常

●接口状态检查

●路由配置及状态

●系统异常情况

●芯片级协议级的状态检查

b) 巡检安排：

●例行巡检；

●重大节日巡检，在春节、国庆节等重要节日前应有针对性地对重点网络进行巡检，并给出详细分析和整改建议；

●升级后健康检查，在升级观察期内，应定期使用巡检工具登录设备进行巡检和观察，监控设备和版本的运行情况，防止新问题出现。

备件管理

a) 基础数据管理：

●替换关系管理：管理最新的产品单板替代关系

●统计数据管理：管理最新的备件统计基础数据

●整机清单数据管理：管理最新的整机清单数据

b) 备件管理

●备件查询：进行备件信息查询

●单项备件统计：根据现网的单项备件数量，统计需要的单项备件数量

●批量备件统计：根据现网的备件数量，需要批量统计备件数量

●数据导出：查询统计任务的数据结果导出并保存

6.7 灾备要求

应在生产系统外创建生产系统数据的副本，以满足灾难备份的要求。从技术实现生产系统和灾备系 统之间的数据镜像或复制。灾备系统的建设应遵循《GB/T 20988-2007 信息系统灾难恢复规范》的要 求。 灾备建设的指标主要为RPO和RTO两种： RPO：（Recovery Point Object）恢复点目标。指一个过去的时间点，当灾难或紧急事件发生 时，数据可以恢复到的时间点。 RTO：（Recovery Time Object）恢复时间目标，是指灾难发生后，从IT系统当机导致业务停 顿之刻开始，到IT系统恢复至可以支持各部门运作，业务恢复运营之时，此两点之间的时间段成 为RTO。

表29 RTO/RPO 与灾难恢复能力等级的关系

灾难恢复能力等级	RTO	RPO
1	2 天以上	1 天至 7 天
2	24 小时以后	1 天至 7 天
3	12 小时以上	数小时至 1 天
4	数小时至 2 天	数小时至 1 天
5	数分钟至 2 小时	0 至 30 分钟
6	数分钟	0

居民健康卡注册管理系统作为区域医疗的重要信息平台，不论规模大小，都应该规划实现4级及 以上灾备等级。 对于基本规模居民健康卡注册管理系统，灾难备份系统的建设目标是RPO为数小时至1天，RTO 为数小时至2天。 对于中级规模居民健康卡注册管理系统，灾难备份系统的建设目标是RPO≤30分钟，RTO为数 分钟至2小时。 对于高级规模居民健康卡注册管理系统，灾难备份系统的建设目标是RPO，灾难备份系统的建 设目标，灾难发生后数据不容丢失，即RPO=0，RTO为数分钟。

6.8 可管理性要求

6.8.1 基本要求

居民健康卡注册管理系统提供的IT基础设施各个组件（服务器、存储、网络等）应满足可管理性 要求；居民健康卡注册管理系统做为服务平台，也应满足可管理型的要求。

6.8.2 服务级别协议

居民健康卡注册管理系统的服务提供者将为区域内相关医疗卫生机构以及行政管理机构提供从硬件到软件的服务。服务提供者应该和服务使用者约定服务级别协议(SLA)。SLA需要规范的内容如下（包括且不限于） 分配给客户的最小带宽； 客户带宽极限； 能同时服务的客户数目；

●在可能影响用户行为的网络变化之前的通知安排；

●系统可用性；

●收费依据。

6.8.3 服务申请及变更

平台服务的使用者可以透过平台申请所需的服务，具有要求如下：

●用户可以通过交互接口来请求服务。平台的所有服务目录存放在服务目录里，用户可以通过门户方式或接口方式请求相关服务。

●系统能够对不同渠道提交的事件进行记录、转发、配置、部署、跟踪和反馈等工作。

●使用者所需服务内容和范围发生变更，或者服务的提供方所提供的服务发生变化，平台能够提供服务变更流程，记录，审批并实施服务的变更。

6.8.4 配置/部署管理

实现自动化部署。平台按照业务的要求，能够对虚拟资源、应用系统、配置变更等内容实施自动化部署。最大程度减少人工干预带来的不确定性和低效率。

配置相对充足的虚拟化资源，保证资源的弹性及动态扩展。平台应随时报告资源的可用情况，并保持一定的可用资源，以便增添新的业务及应对业务高峰。

通过定制的工作流自动完成需要手工完成的配置和部署的过程。

6.8.5 监控

对于任何环境而言，监控资源和应用程序性能都是非常重要的环节。在虚拟化的环境中，监控任务更为困难，也更为关键。系统能够：

●采集服务器，服务器集合，网络，存储等实时数据，反应资源使用情况
●校验服务级别协议（SLA）的符合性
●自动生成系统资源警告及详细数据，方便快速检测和解决应用程序问题
●报告应用程序的资源使用情况数据
●提供一站式门户网站查看每个受监控资源的详细信息

6.8.6 容量规划

居民健康卡注册管理系统内的系统、软件和数据容量将不断增长。应该可以监控现有资源使用情 况，并追溯历史数据来预测未来容量需求趋势。

6.8.7 事件管理

平台服务的提供者，应提供相应的事件管理功能，记录事件发生事件，内容，及处理过程。包括：

●事件的时间
●事件的级别
●事件的内容
●事件的状态

6.8.8 资产管理

应提供IT基础设施资产管理功能，满足资产审计，折旧，变更，淘汰等管理要求。

6.8.9 机房建设

居民健康卡注册管理系统机房建设应遵循国内标准和规范，并参考国际上现有的标准和规范。

7 安全规范

7.1 安全设计原则

a）规范性原则 安全设计应遵循已颁布的相关国家标准。

b）先进性和适用性原则 安全设计应采用先进的设计思想和方法，尽量采用国内外先进的安全技术。所采用的先进技术应符 合实际情况；应合理设置系统功能、恰当进行系统配置和设备选型，保障其具有较高的性价比，满足业 务管理的需要。

c）可扩展性原则 安全设计应考虑通用性、灵活性，以便利用现有资源及应用升级。

d）开放性和兼容性原则 对安全子系统的升级、扩充、更新以及功能变化应有较强的适应能力。即当这些因素发生变化时， 安全子系统可以不作修改或少量修改就能在新环境下运行。

e）可靠性原则 安全设计应确保系统的正常运行和数据传输的正确性，防止由内在因素和硬件环境造成的错误和 灾难性故障，确保系统可靠性。在保证关键技术实现的前提下，尽可能采用成熟安全产品和技术，保证 系统的可用性、工程实施的简便快捷。

f) 系统性原则 应综合考虑安全体系的整体性、相关性、目的性、实用性和适应性。另外，与业务系统的结合相对 简单且独立。

g) 技术和管理相结合原则 安全体系应遵循技术和管理相结合的原则进行设计和实施，各种安全技术应该与运行管理机制、人 员思想教育与技术培训、安全规章制度建设相结合。从社会系统工程的角度综合考虑，最大限度发挥人防、物防、技防相结合的作用。

7.2 总体框架

a) 应从安全技术、安全管理为要素进行框架设计；

b) 应从网络安全（基础网络安全和边界安全）、主机安全（终端系统安全、服务端系统安全）、应 用安全、数据安全几个层面实现安全技术类要求；

c) 应从安全管理制度、安全管理机构、人员安全管理、系统建设管理和系统运维管理几个层面实 现安全管理类要求。

7.3 技术要求

7.3.1 物理安全

物理安全主要是指居民健康卡注册管理系统所在机房和办公场地的安全性，主要应考虑以下几个方面内容。

a) 物理位置的选择 应满足 GB/T 22239-2008 中 7.1.1.1 的要求

b) 物理访问控制 应满足 GB/T 22239-2008 中 7.1.1.2 的要求

c) 防盗窃和防破坏 应满足 GB/T 22239-2008 中 7.1.1.3 的要求

d) 防雷击 应满足 GB/T 22239-2008 中 7.1.1.4 的要求

e) 防火 应满足 GB/T 22239-2008 中 7.1.1.5 的要求

f) 防水和防潮 应满足 GB/T 22239-2008 中 7.1.1.6 的要求

g) 防静电 应满足 GB/T 22239-2008 中 7.1.1.7 的要求

h) 温湿度控制 应满足 GB/T 22239-2008 中 7.1.1.8 的要求

i) 电力供应 应满足 GB/T 22239-2008 中 7.1.1.9 的要求

j) 电磁防护 应满足 GB/T 22239-2008 中 7.1.1.10 的要求

7.3.2 网络安全

基础网络安全

a) 结构安全

●应保证主要网络设备的业务处理能力具备冗余空间，满足业务高峰期需要；关键网络设备的业务处理能力至少为历史峰值的 3 倍；

●应保证网络各个部分的带宽满足业务高峰期需要；

●应绘制与当前运行情况相符完整的网络拓扑结构图，有相应的网络配置表，包含设备 IP 地址等主要信息，与当前运行情况相符，并及时更新；

●网络系统建设应符合本规范 8.5 要求。

b) 网络设备防护

●应对登录网络设备的用户进行身份鉴别；

●应删除默认用户或修改默认用户的口令，根据管理需要开设用户，不得使用缺省口令、空口令、弱口令；

●应对网络设备的管理员登录地址进行限制；

●网络设备用户的标识应唯一；

●身份鉴别信息应具有不易被冒用的特点，口令应有复杂度要求并定期更换；

●应具有登录失败处理功能，可采取结束会话、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；

当对网络设备进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。

安全区域边界安全

a) 在居民健康卡注册管理系统和外部网络边界处应部署防火墙设备或其他访问控制设备，访问控制设备需具备以下功能：

●实现基于源/目的 IP 地址、源 MAC 地址、服务/端口、用户、时间、组（网络，服务，用户，时间）的精细粒度的访问控制；

●应设定过滤规则集。规则集应涵盖对所有出入边界的数据包的处理方式；

●能对连接、攻击、认证和配置等行为进行审计，并且可以对审计事件提供的告警；

●实现日志的本地存储、远端存储、备份等存储方式；

●应对进出网络的信息内容进行过滤，实现对应用层 HTTP、FTP、TELNET、SMTP、POP3 等协议命令级的控制；

●应在会话处于非活跃一定时间或会话结束后终止网络连接；

●重要网段应采取技术手段防止地址欺骗；应禁用网络设备的闲置端口，采用对非虚拟 IP 进行设备地址绑定等方式防止地址欺骗。

b) 在平台和外部网络边界部署检测设备实现探测网络入侵和非法外联行为，检测控制设备需具备以下功能：

●能够监测以下攻击行为：端口扫描、强力攻击、木马后门攻击、拒绝服务攻击、缓冲区溢出攻击、IP 碎片攻击和网络蠕虫攻击等；

●当检测到攻击行为时，记录攻击源 IP、攻击类型、攻击目的、攻击时间，在发生严重入侵事件时应提供报警；

●应能够对内部网络用户私自联到外部网络的行为进行检查，准确定出位置，并对其进行有效阻断；

●能够检查网络用户终端采用双网卡跨接外部网络，或采用电话拨号、ADSL 拨号、手机、无线上网卡等无线拨号方式连接其他外部网络。

c) 应在在平台和外部网络边界处对恶意代码进行检测和清除：

●在不严重影响网络性能和业务的情况下，应在网络边界部署恶意代码检测系统;

●如果部署了主机恶意代码检测系统，可选择安装部署网络边界部署恶意代码检测系统。

安全审计

在平台和外部网络边界处部署审计系统，收集、记录边界的相关安全事件，并将审计记录转换为标准格式，上报审计管理中心。边界审计系统需具备以下功能：

●收集、记录网络系统中的网络设备运行状况、网络流量、用户行为的日志信息；

●审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；

●支持使用标准通讯协议将探测到的各种审计信息上报审计管理中心；

●应能够根据记录数据进行分析，并生成审计报表；

●应对审计记录进行保护，避免受到未预期的删除、修改或覆盖等。

7.3.3 服务端系统安全

身份鉴别

通过使用安全操作系统或相应的系统加固软件实现用户身份鉴别、用户身份标识唯一性检查、用户身份鉴别信息复杂度检查以及登录失败处理功能，并根据安全策略配置相关参数，安全操作系统或系统加固软件需具备以下功能：

a) 在每次用户登录系统时，采用强化管理的口令或具有相应安全强度的其他机制进行用户身份鉴别，并对鉴别数据进行保密性和完整性保护。

●宜支持数字证书+USB KEY 的认证方式实现强身份鉴别

●配置用户名/口令认证方式时，口令设置必须具备一定的复杂度，不合格的口令被拒绝；口令必须具备采用 3 种以上字符、长度不少于 8 位，并设置定期更换要求

b) 应提供用户身份标识唯一和鉴别信息复杂度检查功能，保证系统中不存在重复用户身份标识，身份鉴别信息不易被冒用；

c) 应提供登录失败处理功能，可采取结束会话、限制非法登录次数和自动退出等措施；

d) 当对服务器进行远程管理时，应采取必要措施，防止鉴别信息在网络传输过程中被窃听；

e) 应采用两种或两种以上组合的鉴别技术对管理用户进行身份鉴别： 通过本地控制台管理主机设备时，应采用一种或一种以上身份鉴别技术 以远程方式登录主机设备，应采用两种或两种以上组合的鉴别技术进行身份鉴别

访问控制

通过使用安全操作系统或相应的系统加固软件进行系统加固实现自主访问控制安全要求。安全操 作系统或系统加固软件需具备以下功能：

a) 策略控制：能接收到管理中心下发的安全策略，并能依据此策略对登录用户的操作权限进行控 制；

b) 客体创建：用户可以在管理中心下发的安全策略控制范围内创建客体，并拥有对客体的各种访 问操作（读、写、修改和删除等）权限；

c) 授权管理：用户可以将自己创建的客体的访问权限（读、写、修改和删除等）的部分或全部授 予其他用户；

d) 访问控制主体的粒度为用户级，客体的粒度为文件或数据库表级；

e) 应对重要信息资源设置敏感标记；

f) 应依据安全策略严格控制用户对有敏感标记重要信息资源的操作；

g) 应对重要服务器进行监视，包括监视服务器的 CPU、硬盘、内存、网络等资源的使用情况；

h) 应能够对系统的服务水平降低到预先规定的最小值进行检测和报警。重要服务器的 CPU 利用 率、内存、磁盘存储空间等指标超过预先规定的阈值后应进行报警。

安全审计

在管理区域部署审计系统，对区域卫生平台范围内的主机探测、记录、相关安全事件，实现系统安 全审计。审计系统需具备以下功能：

a) 审计范围应覆盖到服务器上的每个操作系统用户和数据库用户；

b) 审计内容应包括重要用户行为、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；审计内容至少包括：用户的添加和删除、审计功能的启动和关闭、审计策略的调整、权限变更、系统资源的异常使用、重要的系统操作（如用户登录、退出）等

c) 审计记录应包括事件的日期、时间、类型、主体标识、客体标识和结果等；

d) 应保护审计记录，避免受到未预期的删除、修改或覆盖等； 审计记录应至少保存 6 个月；

e) 应能够根据记录数据进行分析，并生成审计报表；

f) 应保护审计进程，避免受到未预期的中断。

恶意代码防范

通过部署病毒防护系统或配置具有相应功能的安全操作系统，实现主机计算环境的病毒防护以及 恶意代码防范。病毒防护系统需具备以下功能：

a) 远程控制与管理

b) 保持操作系统补丁及时得到更新

c) 全网查杀毒

d) 防毒策略的定制与分发实时监控

e) 客户端防毒状况

f) 病毒与事件报警

g) 病毒日志查询与统计

h) 集中式授权管理

i) 全面监控邮件客户端

剩余信息保护

a) 应保证操作系统和数据库系统用户的鉴别信息所在的存储空间，被释放或再分配给其他用户 前得到完全清除，无论这些信息是存放在硬盘上还是在内存中；

b) 应确保系统内的文件、目录和数据库记录等资源所在的存储空间，被释放或重新分配给其 他用户前得到完全清除。

入侵防范

a) 操作系统应遵循最小安装的原则，仅安装需要的组件和应用程序，并通过设置升级服务器等方 式保持系统补丁及时得到更新；

b) 应能够检测到对重要服务器进行入侵的行为，能够记录入侵的源 IP、攻击的类型、攻击的目 的、攻击的时间，并在发生严重入侵事件时提供报警；

c) 应能够对重要程序的完整性进行检测，并在检测到完整性受到破坏后具有恢复的措施，如不能 正常恢复，应停止有关服务，并提供报警。

7.3.4 终端系统安全

通过使用安全操作系统或相应的系统加固软件进行系统加固实现终端系统安全加固。安全操作系统或系统加固软件或硬件需具备以下功能：

a) 应对登录终端操作系统的用户进行身份标识和鉴别；

●宜支持数字证书进行身份认证

●使用口令进行身份认证时，口令应有复杂度要求并定期更换

b) 应依据安全策略控制用户对资源的访问，禁止通过 USB、光驱等外设进行数据交换，关闭不必 要的服务和端口等。

c) 应对系统中的重要终端进行审计，审计粒度为用户级；

d) 审计内容应包括重要用户行为、系统资源的异常使用和重要系统命令的使用及其它与审计相 关的信息；

e) 审计记录至少应包括事件的日期、时间、类型、用户名、访问对象、结果等；

f) 应保护审计进程，避免受到未预期的中断；

g) 应保护审计记录，避免受到未预期的删除、修改或覆盖等，审计记录至少保存 3 个月；

h) 应定期对审计记录进行分析，以便及时发现异常行为；

i) 操作系统应遵循最小安装的原则，仅安装需要的组件和应用程序，并保持系统补丁及时得到更 新；

j) 宜支持多操作系统，分离不同类型的应用场景；

k）可以采用硬件加固的方式实现终端系统安全加固，隔离异常终端，并且实现数字内容版权保护。

7.3.5 应用安全

a）用户管理和权限控制 应符合功能 6.7.1（用户管理和权限控制）
b）信息安全 应符合功能 6.7.2（信息安全）
c）隐私保护 应符合功能 6.7.3（隐私保护）
d）审计追踪 应符合功能 6.7.4（审计追踪）
e）剩余信息保护
●应保证用户鉴别信息所在的存储空间被释放或再分配给其他用户前得到完全清除，无论这些信息是存放在硬盘上还是在内存中；
●应保证系统内的文件、目录和数据库记录等资源所在的存储空间被释放或重新分配给其他用户前得到完全清除。
f）软件容错
●应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的数据格式或长度符合系统设定要求；
●在故障发生时，应用系统应能够继续提供一部分功能，确保能够实施必要的措施。

7.3.6 数据安全及备份恢复

a）应能检测到系统管理数据、身份鉴别信息、卡索引信息和卡使用信息等重要业务数据在传输和存储过程中完整性受到破坏，并能够采取必要的恢复措施 宜采用数字摘要技术保障数据的完整性； 宜采用数字签名/验签技术、时间戳技术保障数据的真实性及不可抵赖性； 能对发现的数据破坏事件进行记录。

b）应对身份鉴别信息、电子健康档案和电子病历等重要业务数据等重要业务数据在传输和存储过程中对敏感信息字段进行加密，系统应支持基于标准的加密机制： 宜采用 PKI 密码技术或采用具有相当安全性的其他安全机制实现

c）应建立数据备份措施，建立备份管理制度，制定数据备份策略，对重要信息进行备份以及对依据备份记录进行数据恢复：
●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；
●关键存储部件宜采用冗余磁盘阵列技术并支持失效部件的在线更换；对重要设备应进行冗余配置，以实现双机热备或冷备；
●数据库服务器宜采用双机冗余热备方式。进行定期在线维护，以缩短恢复所需时间；
●用户可以通过备份记录进行数据恢复；
●在条件具备的情况下，应在异地建立和维护重要数据的备份存储系统，利用地理上的分离保障系统和数据对灾难性事件的抵御能力；
●故障恢复前应制定合理的恢复工作计划以及故障恢复方案，数据恢复完成后应检测数据的完整性。

7.4 管理要求

基本管理要求从安全管理制度、安全管理机构、人员安全管理、系统建设管理和系统运维管理几个方面提出。

a）安全管理制度 应满足 GB/T 22239-2008 中 7.2.1 的要求
b）安全管理机构 应满足 GB/T 22239-2008 中 7.2.2 的要求

c) 人员安全管理 应满足 GB/T 22239-2008 中 7.2.3 的要求
d) 系统建设管理 应满足 GB/T 22239-2008 中 7.2.4 的要求
e) 系统运维管理 应满足 GB/T 22239-2008 中 7.2.5 的要求