

团 体 标 准

T/GDWJ XXXX—XXXX

健康医疗信息 跨网数据交换安全技术要求

Health medical information-security technical requirements for data exchanging across
regional networks

(征求意见稿)

XXXX – XX – XX 发布

XXXX – XX – XX 实施

广东省卫生经济学会发布

目次

前言 II

引言 III

1 范围 1

2 规范性引用文件 1

3 术语和定义 1

4 缩略语 4

5 技术框架 4

 5.1 系统架构 4

 5.2 交换对象和交换方式 5

 5.3 系统组成 5

 5.4 功能结构 5

6 技术要求 6

 6.1 功能要求 6

 6.2 安全要求 7

附录 A（资料性）跨网数据安全交换综合评估表 10

参考文献 13

前 言

本文件按照GB/T 1.1—2020《标准化工作导则 第1部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利，本文件的发布机构不承担识别专利的责任。

本文件由广东省卫生经济学会提出并归口。

本文件起草单位：东莞市第六人民医院、广州市妇女儿童医疗中心、东莞市卫生统计信息中心、山东中网云安智能科技有限公司、广东网安科技有限公司、郑州立雪智能科技研究院、中山大学附属口腔医院、中山大学附属第一医院、暨南大学附属顺德医院、广东省妇幼保健院、广州医科大学附属第二医院、广东省卫生经济学会、清远市人民医院、连州市人民医院、江门市中心医院、佛山市第一人民医院、连州市医疗总院、河源市人民医院、东莞市第八人民医院、东莞市凤岗医院、广州市黄埔区人民医院、杭州数圭通科技有限公司、杭州美创科技股份有限公司、北京天融信科技有限公司、深圳昂楷科技有限公司、深圳君同云科技有限公司。

本文件主要起草人：熊劲光、曹晓均、陈惠城、黄春柳、郑金、魏书山、陈见、黄之怡、高峰、余俊蓉、吴庆斌、冯海燕、陆慧菁、李永强、邓意恒、邓联丙、潘遂壮、温明锋、林晓怡、贺锦堂、黄新萍、冯成志、单智宽、高先亮、叶桦、王景保、陈凯、谢泽康。

引 言

医疗卫生行业或机构的跨网数据交换场景多样、形式多样，是网络安全和数据安全风险突出之处，也是数据分类分级保护的关键安全域。主要涉及医疗卫生行业主管部门或机构与公众服务（基于互联网）、上级行业主管部门、其他相关行业主管部门（包括医保、社保、公安、民政、教育、工商、政数或大数据局等）、医疗卫生行业其他机构（包括医联体、医共体、健共体、专科联盟、医学检验/检查中心等）、非医疗行业相关机构（包括第三方检验/检查机构、银行及非银行支付机构、商业保险、药械、物流、科研、数据合规流通、新技术赋能等第三方机构）间的跨网数据交换场景。

为了满足医疗卫生行业或机构跨网数据安全交换的实际需求，特编制本标准，用以规范各类各级医疗卫生机构的健康医疗信息跨网数据安全交换系统的建设、运行和管理。本标准包括健康医疗信息跨网数据安全交换技术框架、技术要求、综合评估的主要内容，并详细阐述了跨网数据安全交换系统的系统架构、功能结构、功能要求和安全要求。

涉及国家秘密的信息系统和数据与非涉密信息系统和数据之间的跨网交换按国家主管部门的相关规定执行。

健康医疗信息 跨网数据交换安全技术要求

1 范围

本文件适用于指导医疗卫生行业主管部门或机构开展跨网数据安全交换系统的建设、运行和管理工
作，主要针对健康医疗信息的跨网数据同步与安全交换提出技术要求。

其他行业机构与卫生健康行业有数据安全交换需求的可参照使用，也可供卫生健康、网络安全相关
管理部门开展健康医疗数据的合规流通监管时作为参考。

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。

GB/T 25069 信息安全技术 术语
GB/T 20279 信息安全技术 网络和终端隔离产品技术规范
GB/T 39725 信息安全技术 健康医疗数据安全指南
GB/T 44792 健康管理 远程医疗平台信息接入与数据交换
WS 365 城乡居民健康档案基本数据集
WS 372 疾病管理基本数据集
WS 375 疾病控制基本数据集
WS 376 儿童保健基本数据集
WS 377 妇女保健基本数据集
WS 445 电子病历基本数据集
WS/T 447 基于电子病历的医院信息平台技术规范
WS/T 448 基于居民健康档案的区域卫生信息平台技术规范
WS/T 483 健康档案共享文档规范
WS/T 500 电子病历共享文档规范
WS 538 医学数字影像通信基本数据集
WS 539 远程医疗信息基本数据集
WS/T 544 医学数字影像中文封装与通信规范
WS/T 545 远程医疗信息系统技术规范
WS/T 546 远程医疗信息系统与统一通信平台交互规范
WS/T 790 区域卫生信息平台交互标准
WS/T 846 医院信息平台交互标准
T/GDWJ 013 广东省健康医疗数据安全分类分级管理技术规范
《医疗卫生机构网络安全管理办法》（国卫规划发〔2022〕29号）
《广东省远程医疗平台接口规范（试行）》
《广东省互联网医疗监管平台接入流程及接口规范》

3 术语和定义

GB/T 25069和GB/T 20279界定的以及下列术语和定义适用于本文件。

3.1

跨网 across regional networks

逻辑隔离且无协议通信的网络之间，或者是物理隔离的网络之间。

3.2

数据交换 data interchange

为满足不同系统间数据传送和处理需要，实现不同系统间数据交互的过程。

[来源：GB/T 25069—2022，3.570]

3.3

数据库数据 database data

按照数据结构来组织、存储在数据库系统中的数据信息。

注：如电子病历（EMR）、电子健康档案（EHR）、电子疾病档案（EDR）等数据集，以及国家医保局统一标准的病案首页、结算清单等，为关系型数据库数据，属于结构化数据或半结构化数据（XML）。

3.4

计算机文件数据 file data

存储在磁盘、光盘、磁带等长期储存设备上的数据。

注：如电子病历（EMR）、电子健康档案（EHR）、电子疾病档案（EDR）等的共享文档（XML）或版式文档（OFD），以及符合DICOM标准的影像文档，属于半结构化或非结构化数据，简称文件数据。

3.5

请求命令与响应数据 request and response data

基于服务器之间一方发送的请求数据和另一方返回的响应数据所形成的应用交互协议数据。

注：如应用服务器与数据库服务器之间、应用服务器与文件服务器之间、应用服务器与应用服务器之间、应用服务器与集成平台之间的请求命令与响应数据。

3.6

流媒体数据 streaming media data

采用流式传输的方式跨网传递或交换的媒体格式数据。

注：如远程医疗、互联网诊疗过程中的音视频数据

3.7

安全域 security domain

遵从共同安全策略的资产和资源的集合。

[来源：GB/T 25069—2022，3.38]

3.8

物理断开 physical disconnection

使用物理方法保证不同安全域之间无法以直接或间接的方式相连接的技术。

注：实施不同安全域的物理断开，包括在物理传导、物理存储上的断开。

[来源：GB/T 20279—2024，3.2]

3.9

协议转换 protocol conversion

把基于网络的公共协议中的应用数据剥离出来,封装为系统专用的私有协议进行数据传输的技术。

[来源: GB/T 20279—2024, 3.3]

3.10

信息摆渡 information ferry

信息由信息源所在安全域传输至中间缓存区域,再将中间缓存区域的信息传输至信息目的所在安全域的数据传输技术。

注: 在任一时刻,中间缓存区域只与一端安全域相连。

[来源: GB/T 20279—2024, 3.4]

3.11

网闸 gap

位于两个不同安全域之间,采用协议转换和信息摆渡技术实现网络隔离,并且保证只有安全策略允许传输的信息能够通过的产品。

[来源: GB/T 20279—2024, 3.9]

3.12

单向光闸 unilateral optical gap

结合网闸技术和光传输技术的一种信息安全隔离部件,其特性是利用光的单向传播特性进行信息传输,确保信息在物理传导上的单向性,同时具有网闸的协议转换手段和信息摆渡方式。

3.13

前置机 staging server

跨系统进行数据交换和传输的中间设备,其主要功能有网络通信、数字认证、格式转换、数据校验及数据缓冲等。

示例: 部署国家传染病智能监测预警前置软件的中间设备(服务器)。

3.14

跨网数据交换 data exchange across regional networks

逻辑隔离且无协议通信的网络之间,或物理隔离的网络之间进行的数据交换。

3.15

跨网数据交换区 data exchange area across regional networks

逻辑隔离且无协议通信的网络之间,或物理隔离的网络之间进行数据交换时,对各类交换业务进行注册、接入认证、操作监控与审计的区域。

3.16

跨网数据交换基础设施 data exchange infrastructure across regional networks

按需提供逻辑隔离且无协议通信的网络之间,或物理隔离的网络之间进行数据交换服务和管理的软硬件设备或系统及相关配套设施。

- 下列缩略语适用于本文件。
- EMR: 电子病历 (Electronic Medical Records)
 - EHR: 电子健康档案 (Electronic Health Records)
 - EDR: 电子疾病档案 (Electronic Disease Records)
 - CDA: 临床文档架构 (Clinical Document Architecture)
 - DICOM: 医学数字影像与通信 (Digital Imaging and Communications in Medicine)
 - OFD: 开放版式文档 (Open Fixed-layout Document)
 - PDF: 可移植文档格式 (Portable Document Format)
 - XML: 可扩展标记语言 (Extensible Markup Language)
 - API: 应用程序接口 (Application Programming Interface)
 - FTP: 文件传输协议 (File Transfer Protocol)
 - FTPS: 基于传输层安全的文件传输协议 (File Transfer Protocol over Transport Layer Security)
 - HTTP: 超文本传输协议 (Hyper Text Transfer Protocol)
 - HTTPS: 安全超文本传输协议 (Hyper Text Transfer Protocol over Transport Layer Security)
 - SYSLOG: 系统日志 (System Log)
 - SNMP: 简单网络管理协议 (Simple Network Management Protocol)
 - SMB: 服务器消息块 (Server Message Block)
 - IP: 网际协议 (Internet Protocol)
 - IPv4: 网际协议版本 4 (Internet Protocol Version 4)
 - IPv6: 网际协议版本 6 (Internet Protocol Version 6)

5 技术框架

5.1 系统架构

跨网数据交换业务采用跨网数据交换区作为统一的出入口,采取设备认证、格式检查等安全措施实现两个不同网络之间的数据交换,保证数据交换的保密性、完整性、可用性。系统架构如图1所示:

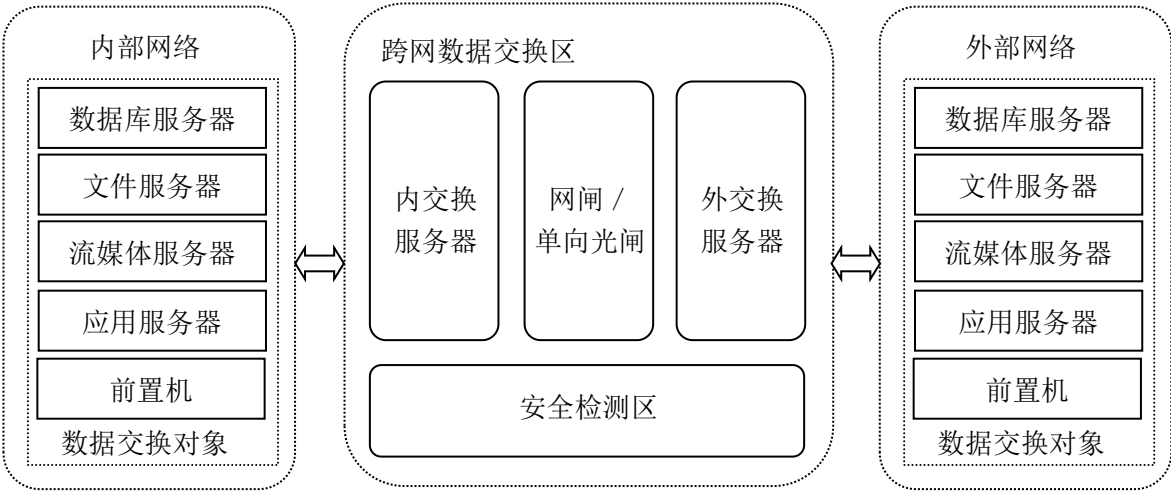


图 1 跨网数据安全交换系统架构示意图

5.2 数据交换对象和交换方式

交换对象包括数据库数据、文件数据、流媒体数据、请求命令与响应数据等。
交换方式包括单向数据传输、双向数据传输。

5.3 跨网数据安全交换系统组成

5.3.1 跨网数据交换区

实现不同网络之间的安全隔离与信息交换，根据安全策略实现网络之间的安全数据摆渡，对各种应用和操作进行监测、统计分析及安全审计，实现整个数据交换的安全监测和审计；

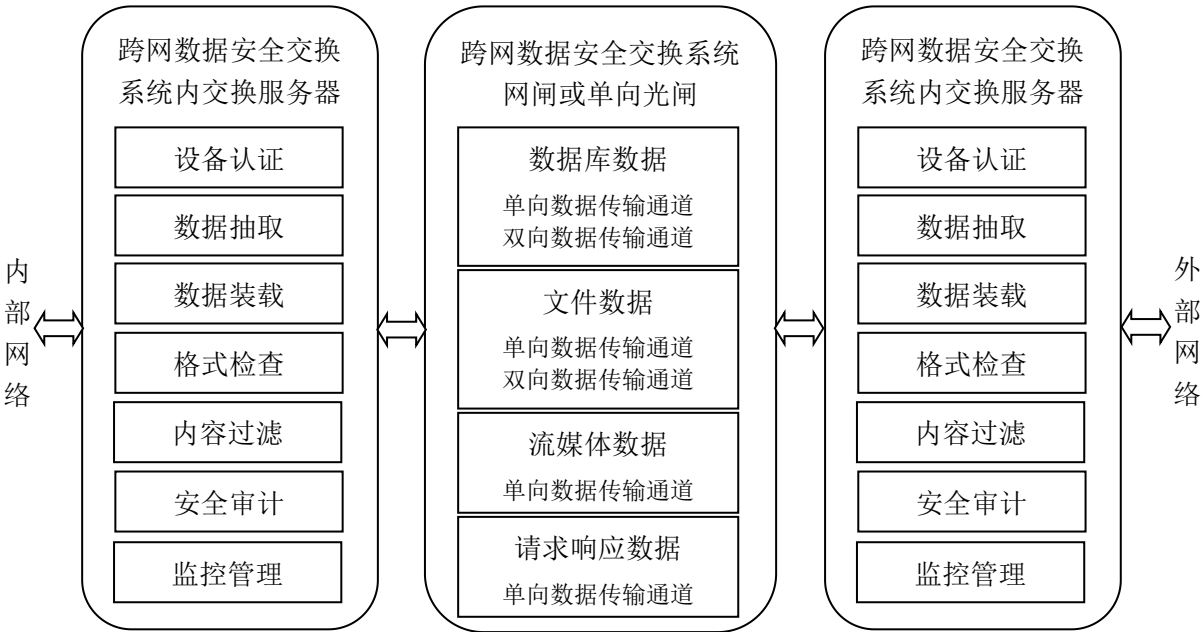
- a) 网闸：通过协议转换，以信息摆渡的方式实现双向数据传输；包括普通网闸和视频网闸，与内外服务器组成双向传输链路，适用于数据库数据、文件数据、请求命令与响应数据和流媒体数据的双向传输。
- b) 单向光闸：通过协议转换，以信息摆渡的方式实现单向数据传输；与内、外交换服务器组成单向传输链路，适用于数据库数据、文件数据交换的单向传输。
- c) 内 / 外交换服务器： 完成数据抽取、数据装载、设备认证、格式检查、内容过滤、安全审计等安全功能。

5.3.2 安全检测区

实现对数据交换系统的安全保护，包括网络级的身份认证、访问控制、权限管理、恶意代码防范等，实现应用级的身份认证、访问控制等功能，防止非法访问。

5.4 功能结构

跨网数据安全交换系统功能结构如图2所示：



网闸和单向光闸通过协议转换，以信息摆渡的方式实现各类数据的双向和单向传输。内、外交换服务器作数据源时完成数据抽取、格式检查、内容过滤、设备认证，作数据目标时完成数据装载、设备认证；外交换服务器应具备向内交换服务器发送监控、报警信息并接受内交换服务器配置指令的功能。

数据库数据、文件数据交换时内、外交换服务器应具备设备认证、数据抽取、数据装载、格式检查、内容过滤、安全审计、监控管理功能。

流媒体数据、请求命令与响应数据交换时内、外交换服务器应具备设备认证、格式检查、内容过滤、安全审计、监控管理功能。

各子模块应具备如下功能：

- a) 设备认证：基于数字证书、IP 地址绑定等技术对连接跨网数据安全交换系统的设备进行设备身份认证，禁止未认证设备上线；
- b) 数据抽取：从源端前置机或信息系统抽取待交换的数据库数据、文件数据到跨网数据安全交换系统；
- c) 数据装载：从跨网数据安全交换系统将数据库数据、文件数据装载到目标端前置机或信息系统；
- d) 格式检查：对交换对象的格式根据事先定义的规则进行关于范围、长度、类型等检查；
- e) 内容过滤：对交换对象的内容进行病毒检测、木马过滤；
- f) 安全审计：提供跨网数据安全交换行为审计、管理员配置管理审计等；
- g) 监控管理：提供跨网数据安全交换系统运行状态实时监控、交换业务配置管理、交换业务统计分析、安全事件实时报警等。

6 技术要求

6.1 功能要求

6.1.1 数据库数据交换

- a) 支持主流数据库系统，包括国产数据库；
- b) 支持主流操作系统，包括国产操作系统；
- c) 支持异构数据库之间的数据交换；
- d) 支持历史数据和增量数据的交换；
- e) 支持时间戳、视图、触发器、日志等数据抽取模式；
- f) 支持基于字段值、行、列等条件的数据交换；
- g) 支持实时、定时的数据交换；
- h) 支持数据库交换的断点续传；
- i) 具备数据传输完整性和一致性检查机制，支持 EMR、EHR、EDR 等相关数据集标准及要求。

6.1.2 文件数据交换

- a) 支持主流文件类型，包括 XML、CDA、DICOM、OFD、PDF 等；
- b) 支持主流操作系统，包括国产操作系统；
- c) 支持异构文件系统之间的数据交换；
- d) 支持历史文件、增量文件的数据交换；
- e) 支持 FTP、FTPS、SMB、共享文件夹等文件数据抽取模式；
- f) 支持基于特定条件的文件数据交换；
- g) 支持实时、定时的文件数据交换；

- h) 支持文件交换的断点续传；
- i) 具备数据传输完整性和一致性检查机制，支持 EMR、EHR、EDR、CDA、DICOM 等相关合规性要求。

6.1.3 流媒体数据交换

- a) 支持远程医疗、互联网诊疗常见的主流流媒体数据类型；
- b) 支持远程医疗、互联网诊疗常见的主流流媒体协议；
- c) 支持远程医疗、互联网诊疗常见的视频控制信令的数据交换；
- d) 支持视频流数据的双向或单向传输；
- e) 支持 DICOM 等相关医学影像标准及要求。

6.1.4 请求命令与响应数据交换

- a) 支持主流数据库（包括国产数据库）服务协议的认识和过滤；
- b) 支持 FTP、FTPS、SMB 等主流文件服务协议的认识和过滤；
- c) 支持 HTTP、HTTPS 及 API、集成平台相关的主流应用服务协议的认识和过滤；
- d) 支持实时请求命令与响应数据交换；
- e) 支持 WS/T 447、WS/T 448 以及 EMR、EHR 等相关共享文档、交互规范标准要求。

6.2 安全要求

6.2.1 隔离性要求

6.2.1.1 数据库数据交换

- a) 单向数据传输采用单向光闸或网闸作为唯一连接通道，通过协议转换，以信息摆渡的方式实现单向数据交换，同时必须确保数据无反向传输；
- b) 双向数据传输采用网闸作为唯一连接通道，通过协议转换，以信息摆渡的方式实现双向数据交换。

6.2.1.2 文件数据交换

- a) 单向数据传输采用单向光闸或网闸作为唯一连接通道，通过协议转换，以信息摆渡的方式实现单向数据交换，同时必须确保数据无反向传输；
- b) 双向数据传输采用网闸作为唯一连接通道，通过协议转换，以信息摆渡的方式实现双向数据交换。

6.2.1.3 流媒体数据交换

- a) 流媒体数据交换采用专用流媒体网闸作为唯一连接通道，通过协议转换，以信息摆渡的方式实现数据交换。
- b) 流媒体网闸应具备流媒体协议转换、流媒体控制信令的过滤和检查功能，并适应快速信息摆渡。

6.2.1.4 请求命令与响应数据交换

- a) 请求命令与响应数据交换采用网闸作为唯一连接通道，通过协议转换，以信息摆渡的方式实现数据交换，同时必须确保阻断传输层（含）以下的网络协议。
- b) 使用此类数据交换时，不建议采用前置机方式。

6.2.2 设备认证要求

- a) 应确保非法设备无法通过数据安全交换系统实现数据交换，交换对象应采用 IP 地址（支持 IPv4、IPv6）绑定、设备数字证书或 SNMP 等方式进行设备认证；
- b) 若采用设备数字证书认证方式，应支持商用密码数字证书。

6.2.3 访问控制要求

- a) 支持通过用户名口令、数字证书方式对系统管理员和操作员进行身份认证，认证支持商用密码数字证书，应通过商用密码现有认证体系进行认证，也可离线认证；
- b) 支持对系统管理员、系统安全员、系统审计员进行不同角色的授权管理。

6.2.4 内容安全要求

6.2.4.1 数据库数据交换

- a) 支持对数据库字段类型、长度等进行安全格式检查；
- b) 支持对数据库字段内容进行关键字过滤；
- c) 支持对数据库大字段内容进行病毒查杀；
- d) 支持不同数据库之间数据交换时格式转换。

6.2.4.2 文件数据交换

- a) 支持对文件类型、长度等进行安全格式检查；
- b) 支持对文件内容进行关键字过滤；
- c) 支持对文件内容进行病毒查杀。

6.2.4.3 流媒体数据交换

- a) 支持对不同视频系统的协议进行识别和过滤，支持白名单保护机制。

6.2.4.4 请求命令与响应数据交换

- a) 支持对请求命令与响应的参数类型、长度等进行安全格式检查；
- b) 支持对请求命令与响应内容进行关键字过滤；
- c) 支持对请求命令与响应内容进行病毒查杀。

6.2.5 可用性要求

- a) 单向数据传输系统支持链路冗余，应在一条链路故障时保证单向数据的传输；
- b) 双向数据交换系统支持热备，应在故障时自动切换交换任务到其他运行的双向数据交换系统；
- c) 双向数据交换系统支持负载均衡，应根据负载自动切换交换任务到其他运行的双向数据交换系统。

6.2.6 安全管理与审计要求

- a) 支持实时监控跨网数据安全交换系统业务状态、通道运行状态；
- b) 支持通过图、表等方式展现跨网数据安全交换系统业务相关统计信息，并应按不同时间粒度和区间汇总；
- c) 支持对跨网数据安全交换系统的行为、安全事件和交换内容等进行审计；
- d) 支持对系统管理员、系统安全员、系统审计员管理行为进行审计；
- e) 支持安全事件报警功能；
- f) 支持配置文件、审计日志的备份功能，并提供备份数据的导入、导出、查询功能；

- g) 支持接收符合标准 SYSLOG 或 SNMP 接口规范的审计日志；
- h) 支持对审计数据保存大小上限进行动态设置。

附 录 A
(资料性)

跨网数据安全交换综合评估表

参考T/GDWJ 013—2022相关数据安全分类分级的原则和方法，依据数据分类分级评估结果，对跨网跨域安全交换基础设施进行综合评估，得出综合评估结论，综合评估结论为：通过/不通过。

表1 跨网数据安全交换综合评估表

项目	检测内容	检测项	1 级	2 级	3 级	4 级
通用 要求	网络安全	网络拓扑架构	√	√	√	√
		网络传输加密	√	√	√	√
		运维网络隔离	√	√	√	√
	设备安全	产品认证	√	√	√	√
		自主可控	√	√	√	√
	系统安全	操作系统安全加固	√	√	√	√
		可信计算防护	√	√	√	√
		中间件及数据库安全加固	√	√	√	√
	应用安全	漏洞检测	√	√	√	√
		安全功能	√	√	√	√
	数据安全	访问控制	√	√	√	√
		恶意代码检测	√	√	√	√
		数据残留	√	√	√	√
	安全管理	安全管理检查	√	√	√	√
技术 能力 要求	接入控制	安全基线核查	√	√	√	√
		数据交换实体身份认证	—	√	√	√
	数据引接	数据标识	—	√	√	√
		数据加密	—	—	√	√
		数据完整性保护和数字签名保护	√	√	√	√
		传输加密	—	√	√	√

表2 （续）

项目	检测内容	检测项	1 级	2 级	3 级	4 级
技术能力要求	边界防护	网络通道隔离	—	—	√	√
		独立部署	—	—	√	√
		网络访问控制	√	√	√	√
		网络攻击监测	√	√	√	√
		恶意代码检测	√	√	√	√
		抗 DDoS 攻击	√	√	—	—
		应用防护	—	√	√	√
		网络诱捕	—	—	√	√
		网络拓扑隐藏	√	√	√	√
		安全缓冲	—	—	√	√
		流量回溯	—	—	√	√
		网络防追踪	—	—	√	√
	数据审核	数据管理功能	—	√	√	√
		协议与数据分离	—	—	√	√
		数据格式检查	√	√	√	√
		数据标识数字签名验证	—	—	√	√
		数据完整性检查	—	√	√	√
		降密脱敏情况检查	—	—	√	√
		数据安全清洗	—	—	—	√
		可信计算防护	—	—	√	√
	隔离交换	交换方式	√	√	√	√
		单向隔离	√	√	√	√
		受控转发	—	—	√	√
		链路扩展	—	—	—	√
		链路冗余	—	—	√	√

表3 （续）

项目	检测内容	检测项	1 级	2 级	3 级	4 级
技术能力要求	运维监管	实体管理	√	√	√	√
		策略管理	√	√	√	√
		状态监控	√	√	√	√
		行为审计	√	√	√	√
		行为分析	√	√	√	√
		统一监管	√	√	√	√
渗透测试	渗透测试	跨网跨域通道渗透测试	√	√	√	√
		运维管理网络渗透测试	√	√	√	√
判决条件		若基本项通过则评估结论为通过，否则为不通过。				

参 考 文 献

- [1] GB/T 37964—2019 信息安全技术 个人信息去标识化指南
 - [2] GB/T 35273—2020 信息安全技术 个人信息安全规范
 - [3] GB/T 39335—2020 信息安全技术 个人信息安全影响评估指南
 - [4] GB/T 37932—2019 信息安全技术 数据交易服务安全要求
 - [5] GB/T 37988—2019 信息安全技术 数据安全能力成熟度模型
 - [6] GB/T 39477—2020 信息安全技术 政务信息共享 数据安全技术要求
 - [7] GB/T 41479—2022 信息安全技术 网络数据处理安全要求
 - [8] GW 0205—2014 国家电子政务外网跨网数据安全交换技术要求与实施指南
 - [9] MH/T 0073—2020 中华人民共和国民用航空行业标准
 - [10] Q/CR 855—2021 中国国家铁路集团有限公司企业标准
 - [11] FYB/T 53001—2017 安全隔离与信息交换平台建设要求
-