ICS 35.240.01
CCS C 07

T/EJCCCSE

团　　体　　标　　准

T/EJCCCSE XXXX—XXXX

实验室信息管理及读取系统

Laboratory Information Management and Retrieval System

（征求意见稿）

在提交反馈意见时，请将您知道的相关专利连同支持性文件一并附上。

XXXX－XX－XX 发布　　XXXX－XX－XX 实施

中国商业股份制企业经济联合会　　发 布

目　　次

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。

本文件由新疆维吾尔自治区人民医院（新疆维吾尔自治区高血压病研究所、新疆维吾尔自治区急救医学研究所、新疆维吾尔自治区临床药学研究所、新疆维吾尔自治区临床营养研究所、新疆维吾尔自治区临床皮肤性病研究所、新疆维吾尔自治区普通外科微创研究所、新疆维吾尔自治区内分泌糖尿病研究所）提出。

本文件由中国商业股份制企业经济联合会归口。

本文件起草单位：新疆维吾尔自治区人民医院（新疆维吾尔自治区高血压病研究所、新疆维吾尔自治区急救医学研究所、新疆维吾尔自治区临床药学研究所、新疆维吾尔自治区临床营养研究所、新疆维吾尔自治区临床皮肤性病研究所、新疆维吾尔自治区普通外科微创研究所、新疆维吾尔自治区内分泌糖尿病研究所）。

本文件主要起草人：

实验室信息管理及读取系统

1 范围

本文件规定了实验室信息管理及读取系统的功能、性能要求、安全管理、数据管理、系统维护与更新要求。

本文件适用于实验室信息管理及读取系统。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；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 20269 信息安全技术 信息系统安全管理要求

3 术语和定义

本文件没有需要界定的术语和定义。

4 功能

4.1 样本管理

4.1.1 样本登记

4.1.1.1 支持多种方式录入样本信息，包括手工输入、条形码扫描、与医院信息系统（HIS）或其他相关系统的数据接口导入等。

4.1.1.2 登记信息应至少包括患者基本信息（姓名、性别、年龄、住院号/门诊号等）、样本类型（血液、尿液、组织等）、采集时间、采集部位、送检科室等。

4.1.2 样本追踪

4.1.2.1 实时监控样本在实验室内部的流转状态，包括样本接收、处理、检测、存储、销毁等环节，并能准确记录每个环节的时间和操作人员信息。

4.1.2.2 提供样本状态查询功能，可通过样本编号、患者信息或其他相关条件快速查询样本的当前位置和处理进度。

4.2 检验项目管理

4.2.1 项目定义

4.2.1.1 可灵活定义各种检验项目，包括项目名称、代码、参考范围、检测方法、收费标准等信息。

4.2.1.2 支持对检验项目进行分类管理，如生化检验、血液检验、微生物检验等。

4.2.2 项目申请与审核

4.2.2.1 接收来自临床科室的检验项目申请，可与 HIS 系统集成实现自动获取申请信息。

4.2.2.2 对申请的检验项目进行自动或人工审核，检查申请信息的完整性和合理性，对不符合要求的申请进行提示和退回。

4.3 检测结果管理

4.3.1 结果录入与编辑

4.3.1.1　提供多种结果录入方式，如手动输入、仪器自动传输（支持与各种实验室检测仪器的接口连接）等。对于异常结果，系统应能自动提示操作人员进行复核。
4.3.1.2　允许操作人员对录入的结果进行编辑，但需记录编辑历史，包括修改时间、修改人员和修改原因。

4.3.2　结果审核与发布

4.3.2.1　由具备相应资质的人员对检测结果进行审核，审核通过后的结果应及时、准确地发布给临床科室。
4.3.2.2　支持对审核流程进行自定义设置，可根据检验项目的重要性、风险程度等因素确定不同的审核级别和人员。

4.4　报告管理

4.4.1　报告生成

4.4.1.1　根据预设的报告模板自动生成检验报告，报告内容应包括患者基本信息、检验项目结果、参考范围、结果解释、报告日期、报告医生签名等。
4.4.1.2　可根据需要生成不同格式的报告，如纸质报告、电子报告（PDF、HTML 等格式），电子报告应具备防篡改功能。

4.4.2　报告查询与打印

4.4.2.1　提供方便快捷的报告查询功能，临床科室可通过患者信息、检验项目、报告日期等条件查询和浏览检验报告。
4.4.2.2　支持在授权范围内的报告打印功能,对于纸质报告的打印应记录打印时间、打印人员等信息。

4.5　数据查询与统计分析

4.5.1　数据查询

允许授权用户对实验室的各类数据进行灵活查询，包括样本信息、检验项目、检测结果、报告等。查询结果可进行导出，支持常见的数据格式（如 Excel、CSV 等）。

4.5.2　统计分析

4.5.2.1　具备强大的统计分析功能，可按日、周、月、年或自定义时间段对检验工作量、阳性率、检验项目分布、患者来源等进行统计分析，并以图表（柱状图、折线图、饼图等）形式直观展示统计结果。
4.5.2.2　支持对特定疾病或检验项目的数据分析，为临床诊断和治疗提供数据支持，同时也有助于实验室的质量控制和管理决策。

4.6　质量控制管理

4.6.1　质量控制计划制定

4.6.1.1　依据实验室的质量控制要求和相关标准，制定质量控制计划，包括质控品的选择、检测频率、靶值和控制限的设定等。
4.6.1.2　可对不同的检验项目分别设置质量控制方案，并能根据实际情况进行调整和更新。

4.6.2　质量控制数据采集与分析

4.6.2.1　自动采集质控品的检测数据，并与预设的靶值和控制限进行比较。对于超出控制限的数据，系统应及时发出警报，并提示可能存在的问题及相应的处理措施。
4.6.2.2　生成质量控制报告，记录质控数据的变化趋势、失控情况及处理结果，便于实验室管理人员对质量控制情况进行评估和持续改进。

4.7　仪器设备管理

4.7.1　设备登记与维护

4.7.1.1　对实验室的所有仪器设备进行详细登记，包括设备名称、型号、生产厂家、购买日期、安装位置、校准周期、维护记录等信息。
4.7.1.2　制定设备维护计划，系统自动提醒维护人员进行设备的定期维护、校准和保养，并记录维护操作的内容、时间和人员。

4.7.2　设备状态监控

4.7.2.1　实时监控仪器设备的运行状态，包括开机、关机、待机、故障等状态信息。对于故障设备，系统应及时发出警报，并记录故障发生的时间、现象等信息，以便维修人员快速响应和处理。
4.7.2.2　可查询设备的历史运行数据和故障记录，为设备的性能评估和更新换代提供依据。

4.8　人员管理

4.8.1　人员信息维护

4.8.1.1　建立实验室人员档案，包括姓名、性别、职称、岗位、权限、联系方式等信息。
4.8.1.2　支持对人员信息的添加、修改、删除等操作，同时记录操作历史。

4.8.2　权限管理

4.8.2.1　根据实验室人员的岗位和职责，对系统的不同功能模块和操作进行细粒度的权限划分，如样本登记员、检测人员、报告审核员、系统管理员等具有不同的权限。
4.8.2.2　权限设置应遵循最小授权原则，确保系统数据的安全性和保密性。

5　性能要求

5.1　响应时间

在正常网络环境下，系统对于用户操作的响应时间应满足以下要求：

a)　样本登记、结果录入等基本操作的响应时间不超过 1 s；
b)　复杂查询（如涉及多条件、大量数据的查询）和统计分析操作的响应时间不超过 2 s；
c)　报告生成和发布操作的响应时间不超过 3 s。

5.2　数据处理额能力

5.2.1　系统应能满足医院实验室日常业务的高峰数据处理需求，在业务高峰期（根据医院实际情况确定高峰时段），每小时处理样本登记数量不少于 1 个，检测结果录入数量不少于 2 条，报告生成数量不少于 3 份。
5.2.2　系统应具备良好的数据存储和管理能力，支持长期保存实验室数据（至少［具体年限］年），并保证数据的完整性和可恢复性。

5.3　系统可靠性

5.3.1　系统应具备高可靠性，确保 98 % 以上的正常运行时间，全年故障停机时间不超过 96 h。
5.3.2　具备数据备份和恢复功能，每天至少进行一次全量备份或增量备份，备份数据应存储在异地容灾中心或其他安全的存储介质上，以防止数据丢失或损坏。在发生故障时，能够在 24 h 内恢复系统正常运行，并保证数据的一致性。

6　安全管理

6.1　设立集中管理机构

应符合 GB/T 20269 的规定。应配备必要的领导和技术管理人员，应选用熟悉安全技术、网络技术、系统应用等方面技术人员，明确责任协同工作，统一管理信息系统的安全运行，进行安全机制的配置与管理，对与安全有关的信息进行汇集与分析，对与安全有关的事件进行响应与处置；应对分布在信息系统中有关的安全机制进行集中管理；应接受信息安全职能部门的直接领导。

6.2　集中管理机构职能

6.2.1 信息系统安全运行的统一管理：集中管理机构主要行使以下技术职能：

a) 防范与保护：建立物理、支撑系统、网络、应用、管理等五个层面的安全控制机制，构成系统有机整体安全控制机制；统一进行信息系统安全机制的配置与管理，确保各个安全机制按照设计要求运行。

b) 监控与检查：对服务器、路由器、防火墙等网络部件、系统安全运行性状态、信息（包括有害内容）的监控和检查；汇集各种安全机制所获取的与系统安全运行有关的信息，对所获取的信息进行综合分析，及时发现系统运行中的安全问题和隐患，提出解决的对策和方法。

c) 响应与处置：事件发现、响应、处置、应急恢复，根据应急处理预案，作出快速处理；应对各种事件和处理结果有详细的记载并进行档案化管理，作为对后续事件分析的参考和可查性的依据。

d) 安全机制集中管理控制完善管理信息系统安全运行的技术手段，进行信息系统安全的集中控制管理。

6.2.2 关键区域安全运行管理：在 6.2.1 的基础上，集中管理机构对关键区域的安全运行进行管理，控制知晓范围，对获取的有关信息进行相应安全等级的保护。

6.2.3 核心系统安全运行管理:在 6.2.2 的基础上,集中管理机构应与有关业务应用的主管部门协调，定制更高安全级别的管理方式。

6.3 人员

6.3.1 可配备兼职安全管理人员：安全管理人员可以由网络管理人员兼任。

6.3.2 安全管理人员的兼职限制：安全管理人员不能兼任网络管理人员、系统管理员、数据库管理员等。

6.3.3 配备专职安全管理人员：安全管理人员不可兼任，属于专职人员，应具有安全管理工作权限和能力。

6.3.4 关键部位的安全管理人员：在 6.3.3 的基础上，安全管理人员还应按照机要人员条件配备。

6.4 网络安全

6.4.1 系统应部署在医院内部安全的网络环境中，与外部网络之间应设置防火墙、入侵检测系统等网络安全防护设备，防止外部网络攻击和非法访问。

6.4.2 对网络通信进行加密处理，采用安全的通信协议（如 HTTPS），确保数据在传输过程中的保密性和完整性。

6.5 系统安全

6.5.1 系统应具备完善的身份认证机制，支持用户名/密码、数字证书、指纹识别等多种认证方式，确保用户身份的真实性。

6.5.2 定期对系统进行安全漏洞扫描和修复，及时更新系统补丁，防止系统被恶意攻击和利用。同时，对系统的关键配置文件和参数进行备份和保护，防止被篡改。

7 数据管理

7.1 数据标准化

7.1.1 系统中的所有数据应遵循统一的数据标准和规范，包括数据格式、编码规则、术语定义等。例如，检验项目代码应采用国际或国内通用的标准编码（如 LOINC 编码等），患者信息应与医院信息系统中的数据格式保持一致。

7.1.2 建立数据字典，对系统中的各类数据元素进行详细定义和解释，方便用户理解和使用数据，同时也有助于数据的一致性维护和系统的升级扩展。

7.2 数据完整性

7.2.1 系统应确保数据的完整性，在数据录入、存储、传输和处理过程中，通过数据校验、逻辑检查等手段防止数据丢失、错误或不一致。例如，在样本登记时，对必填信息进行检查，确保所有必要的样

本和患者信息都被准确录入。

7.2.2　对于数据的修改和删除操作，应进行严格的审核和记录，只有在符合规定的情况下才能进行，并且要保证修改或删除操作不会破坏数据的整体完整性。

8　系统维护与更新要求

8.1　系统维护

8.1.1　医院应配备专业的系统维护人员，负责系统的日常维护工作，包括服务器维护、网络维护、数据库维护、软件更新等。

8.1.2　建立系统维护日志，详细记录维护操作的内容、时间、人员以及系统运行状态的变化情况，以便对系统的维护历史进行查询和分析。

8.2　系统更新

8.2.1　系统开发商应定期对系统进行更新和升级，以修复系统漏洞、优化系统性能、增加新功能等。更新过程应确保系统数据的安全，尽量减少对医院实验室业务的影响。

8.2.2　在更新前，应提前通知医院相关部门和用户，并对更新内容进行详细说明和培训，确保用户能够熟悉和适应新的系统功能。