



团 体 标 准

T/XXX XXXX—XXXX

保健食品安全性评价人工智能辅助系统建设规范

Construction specification for AI-assisted system of safety
evaluation of health food

（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

发 布

目次

前言 III

1 范围 4

2 规范性引用文件 4

3 术语和定义 4

4 缩略语 5

5 总体要求 5

 5.1 安全性要求 5

 5.2 可靠性要求 5

 5.3 科学性要求 5

 5.4 可追溯性要求 5

 5.5 互操作性要求 5

 5.6 可扩展性要求 5

6 系统架构要求 5

 6.1 总体设计 5

 6.2 中央知识库 6

 6.3 规则库 6

 6.4 流程引擎 6

7 功能模块要求 7

 7.1 合规预审模块 7

 7.2 电子实验记录模块 7

 7.3 数据分析模块 7

 7.4 报告生成模块 7

 7.5 知识检索模块 7

 7.6 模型迭代与知识优化模块 7

8 数据接口要求 8

 8.1 接口类型 8

 8.2 接口规范 8

 8.3 数据格式要求 8

9 安全隐私保护 8

 9.1 访问控制 8

 9.2 数据安全 8

 9.3 隐私保护 8

 9.4 合规审计 8

10 性能要求 8

 10.1 响应时间 9

 10.2 并发能力 9

 10.3 可用性 9

10.4 数据处理能力 9

11 验证与确认 9

11.1 验证要求 9

11.2 确认要求 9

11.3 记录要求 9

12 运维与持续改进 9

12.1 变更管理 10

12.2 持续优化 10

12.3 版本管理 10

参考文献 10

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××××提出。

本文件由吉林省检验检测协会归口。

本文件起草单位：吉林省产品质量监督检验院，吉林大学，吉林大学第一医院，佛山海关综合技术服务中心

本文件主要起草人：盛秋双，王潇，刘斌，李沐阳，王建锋，郑宏儒，沈雪，初晓，徐蕾，刘峻搏，邵秋荣，何蕾

保健食品安全性评价人工智能辅助系统建设规范

1 范围

本文件确立了保健食品安全性评价的指标体系，规定了保健食品安全性评价人工智能辅助系统（以下称“系统”）建设的总体要求、安全性评价指标体系、系统架构、功能模块、数据接口、安全隐私保护、性能要求、验证确认及运维管理等技术要求。

本文件适用于保健食品安全性评价AI辅助系统的规划、设计、开发、部署与运维。

本文件旨在通过智能化手段，提升评价工作的科学性、一致性与效率，构建“数据驱动-智能验证-持续优化”的闭环体系。

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 16740-2014 食品安全国家标准 保健食品

GB/T 22239—2019 信息安全技术 网络安全等级保护基本要求

GB/T 35273—2020 信息安全技术 个人信息安全规范

《保健食品及其原料安全性毒理学检验与评价技术指导原则（2020年版）》

《保健食品注册与备案管理办法》

3 术语和定义

下列术语和定义适用于本文件。

3.1

保健食品 health food

声称具有特定保健功能或者以补充维生素、矿物质为目的的食品，适宜于特定人群食用，具有调节机体功能，不以治疗疾病为目的，并且对人体不产生任何急性、亚急性或者慢性危害的食品。

3.2

安全性评价 safety assessment

通过毒理学检验、原料安全性分析及功能性实验，结合长期食用风险评估和法规要求进行综合判定。

3.3

人工智能辅助系统 AI-assisted system

基于人工智能技术（如机器学习，自然语言处理，知识图谱等），辅助完成保健食品安全性评价任务的信息系统。

3.4

流程智能体 workflow agent

能够自主执行特定业务流程任务的人工智能组件，具备任务理解、决策推理、工具调用等能力。

3.5

知识库 knowledge base

结构化存储保健食品领域文献、著作、法规、标准、毒理学数据的数据库，支持智能检索与推理。

3.6

规则引擎 rule engine

将保健食品安全性评价相关的判定规则编码为机器可执行逻辑的引擎，用于自动判定与决策。

3.7

预测-验证闭环 prediction-validation closed loop

一种系统持续优化的机制，指系统基于现有知识库与规则库生成预测或评价结论后，通过与后续实际实验数据或专家评审结果进行比对，将差异与验证结果反馈至知识库与AI模型，驱动其进行再学习与迭代优化的过程。

4 缩略语

下列缩略语适用于本文件。

AI: 人工智能 (Artificial Intelligence)

API: 应用程序接口 (Application Programming Interface)

LIMS: 实验室信息管理系统 (Laboratory Information Management System)

HTTPS/TLS: 超文本传输安全协议/传输层安全协议 (Hypertext Transfer Protocol Secure/Transport Layer Security)

ERP: 企业资源规划 (Enterprise Resource Planning)

JSON: 一种轻量级、易读易写、跨语言的数据交换格式 (JavaScript Object Notation)

SDK: 软件开发工具包 (Software Development Kit)

5 总体要求

系统建设应遵循国家相关法律法规和标准规范的要求，结合保健食品安全性评价的实际需求，确保系统的安全性、可靠性、科学性、可追溯性、互操作性和可扩展性。

5.1 安全性要求

系统建设应符合国家网络安全等级保护要求，采取必要的技术和管理措施，确保系统运行安全、数据安全及用户隐私安全。

5.2 可靠性要求

系统应具备高可用性设计，关键功能模块应实现冗余备份，确保评价服务连续稳定。

5.3 科学性要求

系统嵌入的评价逻辑、判定规则应符合现行法规标准要求，确保评价结论的科学性与合规性。

5.4 可追溯性要求

系统应完整记录评价全流程数据，支持审计追踪，满足监管合规要求。

5.5 互操作性要求

系统应遵循开放标准，支持与LIMS、企业信息系统、监管平台等外部系统的数据交换。

5.6 可扩展性要求

系统架构应具备良好的可扩展性，支持功能模块的灵活配置与升级迭代。

6 系统架构要求

6.1 总体设计

系统应采用分层架构设计，至少包含以下层次：

- (1) 交互层：提供用户交互界面，支持人机协同；
- (2) 智能服务层：提供 AI 能力支持，包括知识检索、规则推理、报告生成等；
- (3) 业务逻辑层：核心由流程智能体驱动，负责评价业务流程的解析、分解、自动化编排、执行监控与异常处理；
- (4) 数据层：负责评价数据的存储、管理与访问控制。

系统架构层次关系见图1。各层次之间通过标准化接口实现数据交互与功能调用，中央知识库（6.2）和规则库（6.3）为智能服务层提供知识支撑与判定依据，流程智能体（6.4）驱动业务逻辑层完成评价流程的自动化编排与执行监控。



系统架构层次关系图

6.2 中央知识库

应建立覆盖保健食品领域的结构化知识库，包括：

- (1) 国家法规文件（保健食品相关法律、行政法规、部门规章）；
- (2) 国家标准与行业标准（保健食品毒理学评价标准）；
- (3) 《保健食品及其原料安全性毒理学检验与评价技术指导原则》等指南；
- (4) 历史评价案例与典型毒理学数据。

6.3 规则库

应将保健食品安全性评价的关键判定规则编码为机器可执行逻辑，包括：

- (1) 实验设计与方案合规性判定规则（参照《保健食品毒理学评价程序》）；
- (2) 数据采集与录入规范校验规则；
- (3) 结果判定与阈值比对规则；
- (4) 报告格式与内容完整性校验规则；
- (5) 系统内嵌的安全性评价项目、判定阈值与结果形成规则应符合《保健食品及其原料安全性毒理学检验与评价技术指导原则（2020 年版）》的规定，并应可追溯、可配置、可审计。

6.4 流程引擎

应配置工作流引擎，用于评价业务流程的解析、分解、编排、执行监控与异常处理。流程智能体应具备下列能力：

- (1) 任务理解：应能解析评价任务的目标、输入条件与约束条件，并生成可执行的流程实例；

(2) 决策推理：应能基于知识库与规则库的判定结果确定后续流程路径，路径发生变更时应记录判定依据；

(3) 工具调用：应能调用数据分析、报告生成等系统功能模块及外部接口，调用过程应留痕；

(4) 执行监控：应实时监控流程实例状态，出现异常时应中止流程、发出告警并转入人工处置；

(5) 异常处理：应支持重试、回退与断点续跑，异常处置过程应完整记录。

7 功能模块要求

7.1 合规预审模块

7.1.1 功能要求

功能要求包括：

(1) 依据内嵌保健食品法规知识库，对实验方案进行自动化合规性审查；

(2) 识别关键参数合规范围（如动物种属、剂量设计、观察周期等），生成合规性报告；

(3) 对不符合项提出修改建议。

7.1.2 性能要求

单次方案审查响应时间不超过30秒。

7.2 电子实验记录模块

功能要求包括：

(1) 提供标准化电子实验记录模板（涵盖急性毒性、遗传毒性、亚慢性毒性等试验类型）；

(2) 支持动物分组、给药记录、体重变化、病理观察等关键数据的结构化录入；

(3) 实现实时数据校验与逻辑检查；

(4) 自动生成符合资质认定要求的原始记录。

7.3 数据分析模块

功能要求包括：

(1) 自动调用标准分析模型（如剂量-反应关系、半数致死量计算等）进行统计计算；

(2) 支持图表自动生成（如体重曲线、脏器系数图等）与导出；

(3) 依据安全性评价阈值进行自动化结果比对与判定；

(4) 支持趋势分析与异常检测（如历史数据对比、批次间差异）；

(5) 应提供 AI 模型预测结果与实验验证结果的比对分析功能，生成一致性/差异性验证报告。

7.4 报告生成模块

功能要求包括：

(1) 辅助生成符合《保健食品注册与备案管理办法》及资质认定要求的评价报告；

(2) 支持报告模板的自定义配置；

(3) 实现报告内容的自动校验与完整性检查；

(4) 支持报告的电子签名与版本管。

7.5 知识检索模块

功能要求包括：

(1) 支持多维度法规标准智能检索（如按毒理学终点、原料名称检索等）；

(2) 提供相似案例推荐功能（如类似原料的毒理学数据）；

(3) 支持问答式知识查询。

7.6 模型迭代与知识优化模块

功能要求包括：

(1) 应支持基于验证报告（7.3 (5)）和用户反馈，触发对 AI 评价模型的再训练或微调；

- (2) 应支持对知识库中新增法规、标准、案例的结构化导入与一致性检查；
- (3) 应记录每次模型迭代和知识更新的版本、内容及验证依据，确保可追溯。

8 数据接口要求

8.1 接口类型

系统应提供以下类型接口：

- (1) 数据交换接口：支持与 LIMS、企业 ERP 等系统数据交换；
- (2) 监管上报接口：支持向监管部门数据上报；
- (3) 第三方服务接口：支持调用外部 AI 服务或数据库。

8.2 接口规范

接口规范包括：

- (1) 优先采用 RESTful API 架构；
- (2) 接口文档应符合 OpenAPI 规范要求；
- (3) 数据传输应采用 JSON 格式；
- (4) 应提供接口调用示例与 SDK。

8.3 数据格式要求

数据格式要求包括：

- (1) 实验数据格式应符合相关领域数据标准；
- (2) 应支持主流数据格式（CSV、JSON、XML 等）的导入导出；
- (3) 数据编码应统一采用 UTF-8。

9 安全与隐私保护要求

9.1 访问控制

访问控制要求应包括：

- (1) 应建立基于角色的访问控制机制；
- (2) 应实现多因素身份认证；
- (3) 敏感操作应记录操作日志。

9.2 数据安全

数据安全应包括：

- (1) 应采取数据加密传输（HTTPS/TLS）；
- (2) 应实施数据分类分级管理；
- (3) 应建立数据备份与灾难恢复机制。

9.3 隐私保护

隐私保护应包括：

- (1) 涉及个人信息的数据处理应符合 GB/T 35273 要求；
- (2) 应建立数据脱敏规则；
- (3) 应提供数据删除与匿名化功能。

9.4 合规审计

- (1) 应支持安全审计日志的完整记录；
- (2) 审计日志保存期限不少于 3 年；
- (3) 应支持审计报告的自动生成。

10 性能要求

10.1 响应时间

响应时间要求包括：

- (1) 用户界面响应时间：单次操作响应不超过 3 秒；
- (2) 数据查询响应时间：常规查询不超过 5 秒；
- (3) 复杂分析任务：不超过 30 秒（除特别说明外）。

10.2 并发能力

并发能力要求包括：

- (1) 系统应支持不少于 100 个并发用户；
- (2) 核心评价功能应支持不少于 20 个并发任务。

10.3 可用性

可用性要求包括：

- (1) 系统可用率应不低于 99.5%；
- (2) 核心功能故障恢复时间不超过 4 小时。

10.4 数据处理能力

数据处理能力包括：

- (1) 应支持单批次不少于 1000 条记录的批量处理；
- (2) 应支持图像、文本、表格等多类型数据处理。

11 验证与确认

11.1 验证与确认要求

系统建设完成后，应进行以下验证：

- a) 功能验证：确认各功能模块满足设计要求；
- b) 性能验证：确认系统性能指标符合规定；
- c) 安全验证：确认安全措施有效运行；
- d) 兼容性验证：确认与外部系统对接正常。

确认要求包括：

- (1) AI 模型的预测结果应与实际毒理学实验数据进行比对验证，毒性分类预测准确率应不低于 85%，定量预测结果与实验值的相关系数 (R^2) 应不低于 0.80；
- (2) 规则库的判定逻辑应与保健食品领域专家判断保持一致，一致率应不低于 85%；
- (3) 系统输出报告应通过具有资质的保健食品评价机构专家评审，专家评审通过率应不低于 90%；
- (4) 应验证系统具备完整的“预测-验证-反馈-优化”闭环能力，模型迭代后预测性能应持续提升或保持稳定。

11.2 AI 辅助程度量化要求

系统AI辅助程度应通过以下量化指标进行确认：

- (1) 任务自动化率：AI 自动完成的安全性评价任务（包括数据录入、初步分析、报告草稿生成等）占总任务的比例应不低于 60%；
- (2) 评价效率提升率：AI 辅助模式下单次安全性评价的平均耗时与传统纯人工模式平均耗时相比，效率提升应不低于 70%；
- (3) 人工干预率：需人工复核和修正的评价结论占总结论的比例应不高于 40%，其中涉及关键安全性判定的环节人工干预率应不高于 20%；
- (4) 预测覆盖率：AI 模型应能覆盖不少于 90%的常规毒理学评价终点，包括急性毒性、遗传毒性、亚慢性毒性、慢性毒性及生殖发育毒性等主要评价类型；
- (5) 假阴性/假阳性控制率：AI 辅助评价中漏判安全风险的假阴性率应不高于 5%，假阳性率应不高于 5%；

(6) 数据处理规模：系统应能在单次评价中处理不少于 1000 条实验数据，并自动完成统计分析与结果判定。

11.3 记录要求

应完整记录验证与确认过程，形成下列文档：

- (1) 验证计划与方案；
- (2) 验证记录与结果；
- (3) 问题跟踪与整改记录；
- (4) 确认报告。

12 运维与持续改进

12.1 变更管理

变更管理包括：

- (1) 应建立系统变更管理流程；
- (2) 重大变更应经过评审与测试；
- (3) 应记录所有变更历史。

12.2 持续优化

持续优化包括：

- (1) 应建立用户反馈收集机制；
- (2) 应定期评估 AI 模型性能；
- (3) 应及时更新知识库与规则库。

12.3 版本管理

版本管理应包括：

- (1) 应建立规范的版本编号体系；
- (2) 每次版本更新应形成变更说明；
- (3) 应保留历史版本可供追溯。

参 考 文 献

- [1] 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
- [2] GB 16740 食品安全国家标准 保健食品
- [3] GB/T 22239—2019 信息安全技术 网络安全等级保护基本要求
- [4] GB/T 35273—2020 信息安全技术 个人信息安全规范
- [5] 国家市场监督管理总局. 保健食品及其原料安全性毒理学检验与评价技术指导原则（2020 年版）
- [6] 保健食品注册与备案管理办法