ICS 11.120.99
CCS C 07

T/ACCEM

团　　体　　标　　准

T/ACCEM XXXX—XXXX

制药企业文档管理系统

Document management system for pharmaceutical enterprises

（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

中国商业企业管理协会　　发 布

目　　次

前言 II
1 范围 1
2 规范性引用文件 1
3 术语和定义 1
4 缩略语 1
5 一般要求 2
6 系统架构 3
7 系统功能 3
8 数据管理 8
9 安全管理 9
10 运行与维护 9

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。

本文件由珠海亿胜生物制药有限公司提出。

本文件由中国商业企业管理协会归口。

本文件起草单位：珠海亿胜生物制药有限公司、XXX、XXX。

本文件主要起草人：XXX、XXX、XXX。

制药企业文档管理系统

1 范围

本文件规定了制药企业文档管理系统的一般要求、系统架构、系统功能、数据管理、安全管理、运行与维护。

本文件适用于制药企业文档管理系统的设计与应用。

注：在不引起混淆的情况下，“制药企业文档管理系统”以下简称“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 20271 信息安全技术 信息系统通用安全技术要求

GB/T 28827.1 信息技术服务 运行维护 第1部分：通用要求

3 术语和定义

下列术语和定义适用于本文件。

3.1

制药企业文档 pharmaceutical enterprises documentation

在制药企业业务活动过程中形成的文件，包括但不限于管理标准文件、技术标准文件、工作标准文件。

3.2

制药企业文档管理系统 document management system for pharmaceutical enterprises

用于协助制药企业进行文档管理的系统。

3.3

元数据 metadata

用来定义和描述数据的数据。

3.4

电子签名 electronic signature

电子记录中以电子形式所含、所附用于识别签名人身份并表明签名人认可其中内容的数据。

4 缩略语

下列缩略语适用于本文件。

ERP：企业资源计划 （Enterprise Resource Planning）

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

MES：制造执行系统（Manufacturing Execution System）

QMS：质量管理系统（Quality Management System）

SSL：安全套接层（Secure Socket Layer）

TLS：传输层安全协议（Transport Layer Security）

TMS：培训管理系统（Training Management System）

WMS:仓库管理系统（Warehouse Management System）

5 一般要求

5.1 系统应符合国家相关法律法规、药品监管要求以及行业标准规范，确保制药企业在文档管理方面合法合规。

5.2 系统应具备安全防护机制，保障文档数据的保密性、完整性与可用性。采用加密技术对敏感文档进行存储与传输加密，防止数据泄露与非法篡改。

5.3 系统应建立严格的用户身份认证与授权体系，基于角色的权限管理应精细到文档类型、文档目录及具体操作功能，确保只有授权用户才能访问与操作相应文档。

5.4 系统应具备数据备份与恢复功能，定期对文档数据进行全量与增量备份，并存储在安全的异地位置，以应对数据丢失、损坏或灾难事件，确保数据能够及时恢复且完整无误。

5.5 系统应具备高稳定性与可靠性，能够承受制药企业日常大量文档处理的负载压力，保证 7×24 h 不间断运行。

5.6 采用冗余技术与容错设计，如服务器集群、存储冗余等，确保在硬件故障或软件异常情况下，系统能够自动切换或快速恢复，不影响文档管理的正常开展。

5.7 系统界面设计应简洁直观、操作方便，符合人体工程学与用户操作习惯，降低用户学习成本与操作失误率。应提供清晰的菜单导航、操作提示与帮助文档，方便用户快速上手与熟练使用系统各项功能。

5.8 系统应支持多种文档格式的上传、下载与在线预览。

5.9 系统架构应具有良好的可扩展性，能够随着制药企业业务的发展与变化，方便地进行功能模块扩展、用户数量增加、存储容量扩充等，以适应企业不同阶段的文档管理需求。

5.10 系统应具备必要的用于描述原始数据所需的元数据，包括时间戳、唯一识别号/码等描述。

5.11 系统中人员操作行为应使用电子签名来进行确认。包括但不限于文档的修订、撤销、审批、分发、定期复审等关键操作行为。

5.12 应结合系统的生命周期阶段，基于风险评估结果制定策略，开展必要的确认或验证工作,以证明有关操作的关键要素能够得到有效控制。确认和验证工作应包括但不限于：

a) 验证计划制定；
b) 用户需求收集；
c) 供应商审计；
d) 系统风险与功能风险评估；
e) 设计确认；
f) 安装确认；
g) 运行确认；
h) 性能确认；
i) 验证总结。

6 系统架构

6.1 总体架构

制药企业文档管理系统应采用分层架构设计，包括硬件层、网络层、数据层、应用层和用户层。

6.2 硬件层

6.2.1 硬件层包括服务器、存储设备、网络设备等硬件设施，应根据企业的规模和业务需求进行合理配置。

6.2.2 服务器应具备高性能、高可靠性，能够满足用户并发访问和数据处理的需求。

6.2.3 存储设备应具备足够的存储容量和数据冗余能力，确保文档数据的安全存储。

6.3 网络层

6.3.1 建立安全可靠的内部网络环境，采用防火墙、入侵检测系统等网络安全设备，防止外部网络攻击。

6.3.2 根据企业的组织架构和业务需求，划分不同的网络区域，实现网络隔离和访问控制。

6.4 数据层

6.4.1 构建统一的数据存储平台，对文档的元数据进行集中管理。

6.4.2 采用关系型数据库或非关系型数据库存储文档数据，确保数据的高效存储和查询。

6.4.3 建立数据索引和搜索引擎，方便用户快速查找和定位文档。

6.5 应用层

6.5.1 提供文档生命周期管理，如文档起草、修订、撤销、审批、生效、分发、打印、借阅、回收、定期复审、归档、补发、增发、建议、检索、销毁等。

6.5.2 集成工作流引擎，实现文档审批流程的自动化和规范化。

6.5.3 提供与 LIMS、WES、QMS、TMS、WMS 等其他业务系统的接口，实现数据的共享和交互。

6.5.4 集成合规性控制模块。

6.6 用户层

6.6.1 为用户提供统一的登录入口，根据用户的角色和权限分配相应的功能模块和操作权限。

6.6.2 支持多种终端设备的访问，如电脑、平板电脑、手机等，方便用户随时随地使用文档管理系统。

7 系统功能

7.1 基础功能

7.1.1 用户及权限管理

7.1.1.1 应支持对用户信息及权限进行管理，系统管理员可维护人员信息，包括添加、修改、失效等。人员管理中还包含账号密码的重置、修改。

7.1.1.2 应支持多角色用户注册、登录与注销功能，提供基于组织架构的用户分组管理。

7.1.1.3 应实现细粒度权限分配机制，支持基于角色、任务和属性的权限模型，确保不同岗位人员仅能访问其职责范围内的文档和操作。

7.1.1.4　应支持强密码策略、账号锁定机制、密码过期提醒、双因素认证等功能，保障系统账户安全。
7.1.1.5　应记录用户登录、登出、权限变更等关键操作日志，便于追踪与审计。
7.1.1.6　应提供灵活的访问控制策略，并按 GB/T 20271 的规定执行。

7.1.2　审计跟踪

7.1.2.1　应支持查看可审计跟踪的功能清单。
7.1.2.2　应支持开启审计跟踪,并控制开启后不可关闭。
7.1.2.3　审计跟踪数据不应被人为删除。
7.1.2.4　应支持按时间轴、业务对象或事件来查看审计跟踪信息。
7.1.2.5　应支持导出或打印审计跟踪信息。

7.1.3　电子签名

7.1.3.1　应支持设定签名要求,如签名确认、双人确认等。
7.1.3.2　电子签名信息至少包含：签名含义、签名人姓名、签名时间戳。
7.1.3.3　应支持查看可添加电子签名的功能清单。
7.1.3.4　应能验证电子签名是否有效。
7.1.3.5　电子签名应与对应的电子记录紧密关联。
7.1.3.6　应保证电子签名无法修改及转移。
7.1.3.7　每份电子签名应唯一绑定至特定操作，并记录签名时间、互联网协议地址、设备信息等上下文信息。
7.1.3.8　电子签名应与文档审批、生效等流程无缝集成，支持多级签名、会签、否决等复杂场景。

7.1.4　日志管理

7.1.4.1　应记录系统运行状态、错误信息、性能指标等，用于故障排查与系统优化。
7.1.4.2　应记录用户登录失败、权限异常、非法访问尝试等安全相关事件
7.1.4.3　系统管理员应可查看系统操作日志记录。
7.1.4.4　操作日志信息应不可被删除。
7.1.4.5　日志应定期归档并异地备份，防止数据丢失。
7.1.4.6　应支持日志自动分析与异常检测，触发告警机制，提升系统安全防护能力。

7.1.5　时钟管理

7.1.5.1　系统内置的时钟应以中国国家标准时间为统一标准
7.1.5.2　联网设备通过网络或卫星实时获取标准时间作为系统的时钟。
7.1.5.3　本地设备通过定期校准或与联网设备实时互联等方式获取标准时间作为设备的时钟。

7.2　配置管理

7.2.1　表单配置

7.2.1.1　应支持可视化表单设计器，允许用户自定义文档元数据字段、布局样式、校验规则等。
7.2.1.2　应提供文本框、下拉框、日期选择器、附件上传等控件库，满足不同业务场景需求。
7.2.1.3　应支持表单模板版本管理，确保历史文档结构一致性。

7.2.2　流程配置

7.2.2.1 应提供图形化流程建模工具，支持自由设定审批路径、节点顺序、条件分支、并行任务等。
7.2.2.2 应支持流程版本管理、启用/停用、回滚等功能，确保流程变更可控。
7.2.2.3 应支持流程监控与统计分析，提供流程执行效率、瓶颈分析等报表。

7.2.3 数据源配置

7.2.3.1 应支持对接多种数据库（如 Oracle、MySQL、SQL Server）及外部系统（如 ERP、LIMS）。
7.2.3.2 应提供数据映射、同步、清洗、转换等功能，确保数据一致性与准确性。
7.2.3.3 应支持接口协议的配置与管理。

7.2.4 清单配置

7.2.4.1 应配置文档清单模板，包括字段定义、显示格式、默认值等。
7.2.4.2 应支持清单数据导入导出、批量编辑、权限控制等操作。
7.2.4.3 应支持清单与文档生命周期关联，实现动态更新与联动管理。

7.2.5 通知配置

7.2.5.1 应支持多种通知方式（邮件、短信、站内信、微信等）的灵活配置。
7.2.5.2 应设置通知触发条件（如流程节点到达、文档到期、任务超时等）。
7.2.5.3 应支持通知模板管理、消息队列、发送失败重试机制等功能。

7.2.6 主数据配置

7.2.6.1 应提供主数据管理模块，支持组织机构、岗位、角色、部门、人员等核心数据的统一维护。
7.2.6.2 应支持主数据的同步、校验、版本控制及权限隔离。

7.2.7 报表配置

7.2.7.1 应支持自定义报表设计，提供拖拽式报表生成工具。
7.2.7.2 应支持多种数据源接入，可生成文档数量、流程效率、培训完成率等统计报表。
7.2.7.3 应支持报表定时自动生成、订阅推送、导出为 PDF 文档、Word 文档、Excel 文档等功能。

7.3 系统应用

7.3.1 文档起草

7.3.1.1 应支持在线文档创建与编辑，提供文本编辑器、模板库、版本对比等功能。
7.3.1.2 应支持文档属性填写、关联清单、附加说明材料等操作。
7.3.1.3 应支持多人协作起草，具备冲突检测与合并建议功能。

7.3.2 文档修订

7.3.2.1 应支持文档版本管理，记录每次修改内容、修改人、修改时间等信息。
7.3.2.2 应支持新旧版本对比、差异高亮、恢复历史版本等功能。
7.3.2.3 修订应经过审批流程后方可生效。

7.3.3 文档撤销

7.3.3.1 应支持在文档生效前或在特定条件下撤销文档。
7.3.3.2 撤销操作需记录原因、审批人、时间等信息，并触发通知机制。

7.3.3.3　已分发文档应支持回收处理。

7.3.4　文档审批

7.3.4.1　应能根据文档信息，确定对应的审批流程、关键审批节点。
7.3.4.2　应能根据审批流程和文档信息，确定文档中需要特别关注和审批的部分，如涉及特定的章节、条款或内容要点等。
7.3.4.3　应能通过文档的审批部分提取出每个分析单元的内容信息。
7.3.4.4　应能利用文本分析技术，如自然语言处理（NLP）,自动识别和提取每个分析单元内容信息对应的关键词。
7.3.4.5　应集成合规性控制模块，建立法规数据库。
7.3.4.6　应能通过法规数据查询关键词，找到对应的法规条款，进行合规性检查，判断每个分析单元的内容信息是否符合法规条款的要求。
7.3.4.7　应集成工作流引擎，实现文档审批流程的自动化和规范化。
7.3.4.8　应提供与其他业务系统的接口，实现数据的共享和交互。
7.3.4.9　应可根据合规性检查结果自动生成提示信息，并展示给审批人。
7.3.4.10　应在审批过程中，采用加密解密、防偷窥测量等安全技术，防止信息泄露。
7.3.4.11　应支持多级审批流程，可配置审批节点、审批人、审批方式（如会签、一人通过即可等）。
7.3.4.12　审批意见应可记录并作为文档历史的一部分保存。
7.3.4.13　应支持电子签名审批，确保审批过程合规、可追溯。

7.3.5　文档培训

7.3.5.1　应能根据审批通过的文档信息，确认培训流程和培训单位。
7.3.5.2　支持将文档与相关人员培训计划关联，生成培训任务。
7.3.5.3　提供培训资料下载、在线学习、测试评估、成绩记录等功能。

7.3.6　文档生效

7.3.6.1　应能根据培训结果信息，将文档草案转化为正式文档。
7.3.6.2　应支持设定文档生效时间，系统在指定时间自动激活文档。
7.3.6.3　生效文档应可设置阅读确认机制，确保相关人员已知悉内容变更。
7.3.6.4　生效文档进入正式使用阶段，后续变更应重新走修订流程。

7.3.7　文档分发

7.3.7.1　应支持文档分发至指定部门、人员或系统，分发记录可追踪。
7.3.7.2　分发方式宜包括内部通知、邮件、移动端推送等。
7.3.7.3　应支持文档查阅权限控制，确保分发对象只能查看授权内容。

7.3.8　文档打印

7.3.8.1　应支持文档打印输出为 PDF、Word、Excel 等标准格式，并保留原始文档的元数据（如版本号、生效时间、审批状态等）。
7.3.8.2　打印权限应与用户角色绑定，仅授权用户可发起打印操作。敏感文档（如质量协议、验证报告）需通过审批后方可打印。
7.3.8.3　打印输出应自动添加动态水印（如用户名、打印时间、设备编号），防止非法复制或篡改。

7.3.8.4　应记录每次打印操作的详细信息，包括打印人、打印时间、打印内容、互联网协议地址、设备信息及打印份数。
7.3.8.5　打印日志应与系统审计追踪功能集成，支持按用户、文档名称、时间范围等条件查询和导出。

7.3.9　文档借阅

7.3.9.1　用户应通过系统提交借阅申请，说明借阅目的、预计归还时间及使用范围。申请需经相关责任人审批后方可生效。
7.3.9.2　借阅期间，系统应为借阅人分配临时访问权限，仅允许查看或下载指定文档（禁止修改、复制或转发）。
7.3.9.3　应支持设置借阅有效期，到期后自动收回权限并通知借阅人。支持续借功能，需经审批后延长有效期。
7.3.9.4　阅人归还文档时，系统应记录归还时间、归还状态（如是否完整归还）及归还人信息。归还后，权限自动解除。
7.3.9.5　对于超期未归还的文档，系统应触发预警通知（如邮件、短信）并记录逾期日志，严重逾期可触发强制归还或权限终止。

7.3.10　文档回收

7.3.10.1　对于失效或需要撤回的文档，系统应支持回收操作。
7.3.10.2　回收文档可标记为“已回收”状态，禁止进一步访问或使用。
7.3.10.3　回收记录应包含回收人、回收时间、回收原因等信息。

7.3.11　定期复审

7.3.11.1　应支持设定文档复审周期，系统自动触发复审任务。
7.3.11.2　复审流程应包括责任人确认、是否继续有效、是否需要修订等内容。
7.3.11.3　复审结果应记录并影响文档生命周期状态。

7.3.12　文档归档

7.3.12.1　文档在生命周期结束后可进入归档状态，归档文档不可再被修改。
7.3.12.2　应支持归档文档的分类管理、快速检索、权限控制。
7.3.12.3　归档数据应长期保存，并符合法规要求的数据保留期限。

7.3.13　文档补发

对于已打印的纸质文件，由于文件丢失、破损、缺页等情况，应可进行补发申请，经批准后，可获得完全一样的文件进行替换。

7.3.14　文档增发

应给未分发到的部门发放文档或者已分发的部门增加文档的分发份数。

7.3.15　文档建议

应可对归档的任意文档提出自己的建议。

7.3.16　文档检索

7.3.16.1　系统所有列表应含有检索功能，可通过文件类型、名称、编号、时间段、部门、角色、状态等关键字进行搜索查看。
7.3.16.2　应可对账号权限内的所有文件进行检索并在线查看。

7.3.17　文档销毁

7.3.17.1　对于达到保存期限或无保留价值的文档，系统应支持销毁流程。
7.3.17.2　销毁操作应经过审批，并记录销毁人、销毁时间、销毁方式等信息。
7.3.17.3　销毁记录应永久保存，确保审计可追溯。

8　数据管理

8.1　数据结构设计

8.1.1　应设计合理的文档数据结构，包括文档基本信息（如标题、类型、创建时间、创建者等）、元数据信息（如关键词、摘要、所属项目或部门等）、内容数据（文档正文或文件内容）以及版本信息（版本号、修改时间、修改者等）等字段。各字段应具备明确的数据类型与长度限制，以确保数据的准确性与完整性。
8.1.2　应采用关系型数据库表结构存储结构化数据（如用户信息表、权限配置表、文档元数据表等），实现数据的规范化存储与高效查询。
8.1.3　对于非结构化的文档内容数据，可存储在文件系统中，并在数据库中建立相应的文件路径索引字段，以便通过数据库查询快速定位与访问文档文件。

8.2　数据采集与录入

8.2.1　在文档创建或导入过程中，系统应自动采集与记录文档的相关信息，如创建时间、创建者等元数据信息，并根据用户输入或选择自动填充文档基本信息字段。
8.2.2　对于从外部系统导入的文档数据，系统应进行数据清洗与转换，确保数据格式符合系统要求，并准确提取关键信息存入数据库。
8.2.3　应提供数据验证机制，在用户输入或上传文档数据时，对必填字段进行校验，确保数据的完整性，对于一些特定格式的数据字段（如日期格式、数字格式等），应进行格式校验，防止错误数据录入。

8.3　数据存储、备份与恢复

8.3.1　文档数据应存储在安全可靠的存储设备中，采用冗余存储技术提高数据存储的可靠性，防止因硬盘故障导致数据丢失。
8.3.2　对于文档数据，应进行异地备份或云备份，备份数据应定期进行完整性检查与恢复测试，确保在主存储设备发生故障或灾难事件时能够及时恢复数据。
8.3.3　应根据文档的重要性与敏感性，对存储数据进行分类分级管理。
8.3.4　应定期清理过期或无用的文档数据，以节省存储空间，但在清理前应按照相关规定进行审批与备案。
8.3.5　应支持数据恢复功能，确保在数据丢失或损坏时能够迅速恢复数据，数据恢复应定期进行测试，以确保数据恢复的完整性和可靠性。

8.4　数据安全与隐私保护

8.4.1　应采用加密技术对文档数据进行存储与传输加密：

a) 在存储方面，对敏感文档内容宜采用对称加密算法进行加密存储，对数据库中的用户密码等敏感信息宜采用哈希算法进行加密处理；
b) 在传输方面，宜使用 SSL/TLS 协议对网络传输数据进行加密，防止数据在传输过程中被窃取或篡改。

8.4.2 应建立数据访问控制机制，控制用户对数据的访问权限。根据用户角色与权限设置，只允许授权用户访问其有权访问的数据范围。对于涉及个人隐私或商业机密的数据，应进行特殊的隐私保护处理，如数据脱敏（将敏感信息进行模糊化或替换处理），在保证数据可用性的前提下，最大限度地保护数据隐私。

8.4.3 定期开展数据安全审计与风险评估，检查系统是否存在数据安全漏洞与隐私泄露风险。及时发现并整改安全问题，加强数据安全管理措施，确保文档数据始终处于安全可控状态。

9 安全管理

9.1 系统安全

系统安全应符合GB/T 20271的规定。

9.2 防火墙与网络安全

9.2.1 系统应部署防火墙设备，作为内外网之间的安全屏障。防火墙可以过滤潜在危险的服务，降低网络内部环境的风险。同时，防火墙还能防止内部信息的外，保护企业数据安全。

9.2.2 系统应采用网络安全防护措施，如安装网络防火墙、禁止不必要的网络连接、严格限制网络访问权限等，以确保网络的安全性。此外，系统还应定期进行安全洞扫描和修复，防止黑客利用漏洞进行攻击。

9.3 安全审计与监测

系统应记录用户操作和安全事件，以便后续的审计和监测。安全审计和监测应包括访问日志、操作日志、安全事件日志等内容，并应定期进行审计和监测。通过安全审计和监测，企业可以及时发现和处理安全问题，确保系统的安全稳定运行。

9.4 应急响应

企业应建立应急响应计划，以应对安全事件的发生。应急响应计划应包括安全事件的分类、应急响应流程、联系方式等内容，确保在发生安全事件时能够迅速响应和处理。

10 运行与维护

系统运行与维护应符合GB/T 28827.1的规定，并符合下列要求：

a) 制定系统运行管理制度，建立系统运行监控机制，安排专人负责系统的日常运行维护工作；
b) 定期对信息系统进行维护，包括硬件设备的维护、软件系统的等；
c) 系统出现异常情况时，及时发出报警信息，并采取相应的处理措施；
d) 建立故障处理机制，对故障进行分类和分级管理，对故障处理过程进行记录和总结。