GXLH
Inspection Certification
国信联合检验认证

# 医疗健康信息安全管理体系认证规则

文件编号：GXLH-R-HIS-01

文件版本：A/2

文件编制：技术发展部

文件审核：安晔

文件审批：同永刚

**国信联合检验认证有限公司**

发布日期：2024 年 08 月 01 日　修订日期：2025 年 06 月 08 日　实施日期：2024 年 08 月 01 日

# 目录

| 修订次数 | 修订日期 | 修改内容/原因 | 更改人 | 审核人 | 批准人 |
|---|---|---|---|---|---|
| 1 | 2025 年 6 月 8 日 | 根据《国家认监委关于加强认证规则管理的公告》的要求修订 | 技术发展部 | 安晔 | 同永刚 |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |

## 1 适用范围

1.1 为规范医疗健康信息安全（以下简称 HIS）认证工作，根据《中华人民共和国认证认可条例》和《认证机构管理办法》等法律法规，结合相关技术标准制定本规则。

1.2 本规则规定了认证机构实施 HIS 认证的程序与管理的基本要求，是认证机构从事 HIS 认证活动的基本依据。

1.3 在中华人民共和国境内从事 HIS 认证活动应遵守本规则。

## 2 认证依据

ISO/IEC 27799:2016 健康信息学-基于 ISO/IEC27002 的健康领域信息安全管理实践规范

## 3 对认证机构的基本要求

3.1 本机构获得国家认监委批准、具备从事 ISMS 认证的资质。

3.2 开展 HIS 认证活动，应当围绕国家经济和社会发展目标，重点服务于经济社会高质量发展，不得影响国家安全和社会公共利益，不得违背社会公序良俗。

3.3 内部管理和认证活动符合 GB/T 27021.1/ISO/IEC 17021-1《合格评定管理体系审核认证机构要求 第 1 部分：要求》，以确保机构持续满足开展 HIS 认证的基本要求。

3.4 建立风险防范机制，对从事 HIS 认证活动可能引发的风险和责任采取合理有效措施。认证机构应能证明已对其开展的 HIS 认证活动可能引发的风险进行了评估，对可能引发的责任做出了充分安排（如保险或储备金）。

## 4 对认证人员的基本要求

4.1 遵守认证认可相关法律法规及规范性文件的要求，具有从事认证工作的基本职业操守，对认证活动及其结果的真实性承担相应责任。

4.2 认证审核员应取得国家认监委确定的认证人员注册机构批准的 ISMS 审核员注册资格，并经评价具备医疗健康信息安全管理体系审核能力，取得本机构的资格确认。

4.3 不得发生影响认证公正性的行为，应主动告知本机构他们所了解的任何可能使其或认证机构陷入利益冲突的情况。因认证人员未履行告知义务而导致非公正性认证结果的，认证人员应当负有连带责任（如承担因此造成的经济损失）。

4.4 按要求接受人员注册/保持注册所要求的继续教育培训，以及机构要求的能力（包括知识和技能）提升活动，以持续具备从事 HIS 认证工作相适宜的能力。

## 5 初次认证程序

### 5.1 认证申请

5.1.1 本机构应向认证委托人至少公开以下信息：

（1）可开展认证业务的范围，获得认可的情况，以及分包境外认证机构业务的情况；

（2）开展 HIS 认证活动所依据的认证标准或其他规范性要求以及相关的认证方案、认证流程；

（3）授予、拒绝、保持、更新、暂停（恢复）或撤销认证以及扩大或缩小认证范围的程序规定；

（4）拟向组织获取的信息以及保密规定；

（5）认证收费标准；

（6）认证证书、认证标志及相关的使用规定；

（7）认证证书有效、暂停、注销或者撤销的状态

（8）对认证过程和结果的申诉、投诉规定；

（9）认证标准换版的规定（必要时）；

（10）本认证实施规则；

（11）其他需要公开的信息。

5.1.2 提出认证申请时，认证委托人应具备以下条件：

（1）取得法人资格（或其组成部分）；

（2）取得相关法规规定的行政许可（适用时）；

（3）已按认证标准建立 ISMS 和 HIS 体系，且运行满三个月；

（4）因获证组织自身原因被原发证机构暂停、撤销认证证书已满一年（适用时）；

（5）原 HIS 证书发证机构被国家认监委撤销 HIS 认证资质已满三个月（适用时）；

（6）未被行政监管部门责令停业整顿；

（7）未被列入国家企业信用信息公示系统和“信用中国”发布的严重违法失信名单；

（8）一年内未发生行政监管部门责令停产整顿的重大信息安全事件；

（9）一年内未发生信息安全事件国家监督抽查（以下简称“国抽”）不合格，或发生国抽不合格但已按相关规定整改合格；

（10）其他应具备的条件。

5.1.3 本机构应要求认证委托人提供以下信息和文件资料：

（1）认证申请，包括认证委托人的名称、地址、认证标准、申请的认证范围、认证范围内组织人员数量及影响体系有效性的外包过程；

（2）法律地位的证明性文件，当 HIS 覆盖多个法律实体时，应提供每个法律实体的法律地位证明性文件；

（3）申请认证范围所涉及医疗健康信息安全相关法律法规要求的行政许可文件、资质证书、强制性产品认证证书等；

（4）组织机构及职责；

（5）工艺流程/服务流程及生产和（或）服务的班次及轮班情况；

（6）ISMS 和 HIS 体系运行满足三个月的证据；

（7）三年内所发生的信息安全事件与信息安全相关的行政处罚、国抽不合格，一年内所发生的其他信息安全信息事件抽查不合格的情况以及整改情况；

（8）信息安全管理体系和医疗健康信息安全成文信息(适用时)；

（9）其他需要提供的文件。

**5.2 申请评审**

5.2.1 按照本机构申请评审程序，对认证委托人提交的申请文件和资料实施申请评审，根据申请认证的活动范围及场所、员工人数、完成审核所需时间和其他影响认证活动的因素，综合确定是否有能力受理认证申请，依据医疗健康信息安全认证业务范围分类（附录 A）评价相应专业，并保存相应评审记录。

5.2.2 对被执法监管部门责令停业整顿或在全国企业信用信息公示系统中被列入“严重违法企业名单”的申请组织，本机构不应受理其认证申请。

5.2.3 满足以下条件的，本机构可以受理认证申请：

（1）认证委托人已具备受理条件（见 5.1.2）；

（2）本机构具备实施认证的能力；

（3）双方就认证事宜达成一致。

5.2.4 对于新的认证委托人，本机构按照初次认证开展认证活动，无论其是否持有其他本机构颁发的 HIS 有效证书。

5.2.5 本机构应将申请评审的结果告知认证委托人补充和完善，或者不受理认证申请。

**5.3 认证合同**

5.3.1 通过申请评审的，在实施认证审核前，本机构应与认证委托人签订具有法律效力的认证合同，以明确认证委托人和本机构的责任。

5.3.2 本机构的责任至少包括：

（1）及时向符合认证要求并已缴纳认证费用的组织颁发认证证书，通过其网站或者其他形式向社会公布获证信息；

（2）对获证组织 HIS 体系运行情况进行有效监督，发现获证组织的 HIS 不能持续符合认证要求的，应及时暂停或者撤销其认证证书；

（3）因本机构原因（如机构或其 HIS 认证资质被注销或撤销）导致获证组织 HIS 证书无法有效保持的，需及时告知获证组织并做出妥善处理，并承担由此导致的获证组织的经济损失。

5.3.3 获证组织的责任至少包括：

（1）遵守认证程序要求，认证过程如实提供相关材料和信息，通过 HIS 认证后持续有效运行 HIS；

（2）申请组织对遵守认证认可相关法律法规，配合认证监管部门的监督检查，对有关事项的询问和调查如实提供相关材料和信息的承诺。配合本机构对投诉的调查；

（3）在广告、宣传等活动中正确使用认证证书、认证标志和有关信息，认证证书注销或被暂停、撤销的，不得继续使用该证书和相关认证标志、信息，不利用医疗健康信息安全认证证书和相关文字、符号误导公众认为其产品或服务通过认证；

（4）发生如下情况，应及时向本机构通报：发生重大信息安全事件、受到市场监管部门行政处罚、被市场监管部门公布存在不符合、被媒体曝光存在信息安全问题、HIS 不能正常运行或发生重大变更，以及其他应通报的情况等；

（5）承担选择本机构的风险，如：因本机构资质被撤销而带来的认证证书无法使用的风险；

（6）按合同约定及时向本机构缴纳认证费用。

**5.4 认证策划**

5.4.1 审核方案

5.4.1.1 本机构应针对每一认证委托人建立认证周期内的审核方案，以清晰地识别所需的审核活动。

5.4.1.2 初次认证的审核方案应包括两阶段初次审核、获证后的监督审核和认证到期前进行的再认证审核。

注：一个认证周期通常为 3 年，从初次认证（或再认证）决定算起，至认证的有效期截止。

5.4.1.3 初次认证审核和再认证审核是对认证委托人完整体系的审核，应覆盖 ISO/IEC27799 所有要求，以及认证范围内的典型产品和服务。认证证书有效期内的监督审核应覆盖 ISO/IEC27799 所有要求。

5.4.1.4 初次认证及再认证后的第一次监督审核应在认证决定日期起 12 个月内进行。此后，监督审核应至少每个日历年（应进行再认证的年份除外）进行一次，且两次监督审核的时间间隔不得超过 15 个月。

5.4.1.5 本机构应考虑认证委托人不同班次完成的过程，以及其所证实的对每个班次的 HIS 控制水平来策划对不同班次实施的审核程度，以确保审核的有效性：

（1）每次审核应至少对其中的一个班次的生产或服务的活动现场进行审核；

（2）对于未审核的班次，应记录不对其审核的理由。

若需获取完整文本资料，请与国信联合检验认证有限公司市场拓展部联系。

联系电话：029-87873805