# 角色与权力限制Matrix

# 角色说明：

1. 系统提供者：专指医院信息系统的提供方，例如：医院HIS厂商、电子病历厂商、系统研发人员等；
2. 采集设备：专指可产生医院信息系统所需数据的医疗设备，例如：麻醉机、超声机、检验设备、CR、CT、心电监测、血糖仪、床旁监护等医疗设备；
3. 患者：专指系统所在医院就诊并发生数据存储的人员；
4. 业务工作人员：专指在医院与数据发生关系的一般工作人员，是数据的主要采集者，包括：临床医生、检查技师、临床药师、窗口工作人员等；
5. 业务管理人员：专指医院的各类业务管理人员，是医院中运营数据的主要使用者，包括：医务处、财务处、病案室等；
6. 临床研究：专指医院内外进行临床科学研究的人员，是医院中临床数据的主要使用者，包括：课题负责人，临床试验指控人员等；
7. 系统接口：专指医院内部各个系统的对应接口；
8. 公共卫生：专指使用卫生专网的公共卫生部门，是医院数据向院外转移的主要对象，包括：各级卫生管理机构；
9. 公共安全：专指公共安全部门，在特殊条件下需要医院提供数据，包括：公安局等部门；
10. 系统运维人员：专指医院信息系统的运行维护人员，包括：医院信息中心工作人员、厂商派驻人员；
11. 数据管理人员：专指医院服务器、数据库管理人员，主要负责数据库维护、调优、备份、恢复等，包括：医院专职维护人员、服务器/数据库厂商维护人员；
12. 数据审计人员：专指数据库审计人员，负责审计数据流、审计异常数据操作行为的审计，包括：医院专指审计人员；
13. 机房管理人员：专指负责机房、服务器、磁盘阵列的维护人员，包括：医院专指机房管理人员、厂商技术支持人员等；
14. 医院： 专指数据产生的医院；
15. 公共卫生部门：专指社区医院、下级医院、协作医院、卫计委等公共卫生部门；
16. 医保机构：专指医保、新农合、保险公司等机构；
17. 云平台（集中）：专指提供主机托管、主机租用、云平台租用的IPS企业。

# 数据安全功能

1. 写入：专指对医院信息系统的采集操作，包括采集过程中一般的“增、删、改、查”操作，数据来源可能为人工输入、设备采集、系统接口等；
2. 获取：专指在医院数据产生后的数据浏览操作，包括完整或部分数据的浏览；
3. 修改：专指数据产生后，改变存储数据内容或状态的操作，包括对数据库、文件等内容的修改；
4. 删除：专指数据产生后，对存储数据的删除操作，包括对数据库、文件等内容的修改；
5. 备份：专指数据备份，包括系统配置备份、文件备份、数据库备份等；
6. 统计：专指数据产生后的检索、统计等操作，包括数据查询、分类报表、数据分析等
7. 身份认证：
8. 全文档加密
9. 文档个体化信息清除
10. 临床数据所有者
11. 赋予对数据操作的不同权限
12. 审计（对数据的操作记录，统计，异常操作记录，审计）
13. 病人隐私保护
14. 敏感数据保护
15. 数据持续可用性保证
16. 数据的灾难备份
17. 数据的恢复
18. 防病毒
19. 防黑客

# 权限划分：

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 角色/权限 |  | 写入 | 获取 | 修改 | 删除 | 备份 | 统计 |
| 采集者 | 系统提供者 | **×** | **×** | **×** | **×** | **×** | **×** |
| 采集设备 | **√** | **×** | **×** | **×** | **×** | **×** |
| 使用者 | 患者 | **×** | **√** | **×** | **×** | **×** | **×** |
| 业务工作人员 | **√** | **√** | **×** | **×** | **×** | **×** |
| 业务管理人员 | **×** | **√** | **×** | **×** | **×** | **√** |
| 临床研究 | **×** | **√** | **×** | **×** | **×** | **√** |
| 系统接口 | **√** | **√** | **×** | **×** | **×** | **×** |
| 公共卫生 | **×** | **√** | **×** | **×** | **×** | **√** |
| 公共安全 | **×** | **√** | **×** | **×** | **×** | **×** |
| 管理者 | 系统运维人员 | **×** | **√** | **×** | **×** | **×** | **×** |
| 数据管理人员 | **×** | **×** | **×** | **×** | **√** | **×** |
| 数据审计人员 | **×** | **×** | **×** | **×** | **×** | **×** |
| 机房管理人员 | **×** | **×** | **×** | **×** | **×** | **×** |
| 存储者 | 医院 | **×** | **×** | **×** | **×** | **√** | **√** |
| 公共卫生部门 | **×** | **√** | **×** | **×** | **×** | **√** |
| 医保机构 | **×** | **√** | **×** | **×** | **×** | **×** |
| 云平台（集中） | **×** | **×** | **×** | **×** | **√** | **×** |

1. 系统提供者：作为系统的设计者、开发者属于第三方，仅有程序框架的知识产权，系统里运行的数据与其无关，因此不应具备对医院数据的“任何”操作权限。
2. 采集设备：可自动将医疗仪器等设备的数据上传至信息系统，仅具备“写入”权限，其他所有权限均不具备。
3. 患者作为医疗对象，有 “获取”本人的部分医疗数据的权限，如检查结果、检查报告、用药情况、费用明细以及部分医疗文书信息（例如：诊断证明书、入院记录、出院记录等），其他所有权限均不具备，可“获取”的权限也局限在本人部分数据。
4. 业务工作人员：作为医院业务活动的主体是数据主要的写入者，同时也应具备一定的数据“获取”权限，但其写入与获取的数据范围应根据其职务特点、职务权限范围进行有效控制，而其他权限均不具备。
5. 业务管理人员：是医院运营数据的主要使用者，其应不具备数据“写入”权限，但必须具备“获取”与“统计”权限，数据使用的范围应根据其业务范围进行有效控制。
6. 临床研究人员：应具备进行临床研究所需数据的“获取”与“统计”权限，其数据权限范围应不得超过研究范围，且应具备严格的审批流程。
7. 系统接口：是各个医院信息系统间数据交换的主要方式，包括“写入”与“获取”，这两方面的权限应根据业务活动的要求控制数据的范围。
8. 公共卫生机构：是数据主要的转移对象，应根据严格的控制流程“获取”、“统计”要求范围内的数据。
9. 公共安全：在进行特殊社会活动（例如侦查）时，需具备“获取”的医疗数据的权限，应有严格的审批流程。
10. 系统运维人员：原则上应不能对数据进行任何操作，必要的情况下只可在在监管下进行数据“获取”操作，以便解决系统问题，排查系统BUG等。
11. 数据管理人员：主要业务是维护数据的可用性、可靠性、完整性，仅具备数据的“备份”权限，其他所有权限应均不具备。
12. 数据审计人员：主要是审计数据在各环节的使用情况，是数据使用安全的监督者，对于数据本身应不具备任何权限。
13. 机房管理人员：主要是对数据的物理存放环境进行维护，业务活动应不涉及具体的数据内容，对于数据本身应不具备任何权限。
14. 医院：作为数据存放的主体，应仅具备“备份”与“统计”权限，对于数据内容的操作只能由具体业务人员进行，医院不具备这类权限。
15. 公共卫生部门：作为医院数据的接受者，在权限范围内具备“获取”、“统计”的权限，同时应保证医院、患者数据的隐私保护。
16. 医保机构：与医院间的费用明细数据的接受者，在权限范围内具备“获取”、“统计”的权限，同时应保证医院、患者数据的隐私保护。
17. 云平台：作为医院数据的第三方存储机构出现，应对数据存储的物理环境负责，仅具备数据的“备份”权限，应不具备其他数据数据操作权限。