**技术参数**

**（“★”条款应针对陪护系统终端，需提供国家认证的第三方机构出具的投标产品的检测报告证明；“▲”条款需提供相关证书证明）**

**一、需求概述**

系统应由身份信息识别设备（人脸自助录入）、人脸门禁设备（校验用途）、陪护管理基础包、陪护管理主模块、陪护管理门禁模块、陪护管理人脸算法及H5移动端陪护录入组成。身份信息识别设备（人脸自助录入）设备部署位置：1号楼住院服务中心（3台）、急诊科室（1台）、三号楼住院区（1台）、心血管科室（1台）、15号楼结核病科室（2台）、机动备用（1台）；人脸门禁设备（校验用途）部署位置：1号楼住院服务中心（1台）。

**二、基本功能概述**

**（一）陪护管理门禁版块**

基础门禁管理通过接入多种门禁设备，利用卡片、人脸、指纹介质，实现人员身份识别、出入管控等智能应用，主要提供门禁权限管理、事件管理、门禁状态查看、门禁远程控制、人员出入记录实时展示、远程呼叫对讲等应用。默认包含50路门禁点授权。

1、提供门禁权限管理应用

1）、支持按组织、人员、人员分组、门禁点维度配置权限；

2）、支持设置权限有效期、计划模板、假日计划；

3）、支持按人员特征属性生成人员分组，如证件类型、岗位等级、职称等；

4）、支持权限增量下发、初始化下发；

5）、支持按时段配置门的常开常闭状态；

6）、支持认证方式设置，可按不同时段设置不同的认证方式，如刷卡+人脸、刷卡+指纹；

7）、支持首卡常开，刷首卡可使门保持常开至常开时间段结束，若此期间再次刷首卡，门恢复正常状态；

8）、支持特殊卡设置，包括残疾人卡（可延长开门时间）、黑名单卡（无法开门）、胁迫卡（正常开门并上报胁迫报警）、超级卡（不受限于门常闭、刷卡+密码认证需要密码确认的规则，刷卡直接开门）；

9）、针对刷卡开门方式，即使卡片权限未同步到设备，也可通过中心平台完成权限认证开门。

10）、支持调整已超出或即将超出设备容量的人员生物特征；

11）、支持按门禁点、人员、组织、区域等多维度，综合查询权限配置、下发状态等信息；

2、提供门禁事件管理应用

1）、支持配置平台接收到事件类型；

2）、支持配置事件保存时长；

3）、支持查询人员出入事件和设备事件；

3、提供门禁状态查看及远程控制应用

1）、支持查看门禁状态，包括开关状态、在离线状态；

2）、支持对门禁点反控，包括对门进行开、关、常开、常闭的反控操作；

3）、支持远程呼叫应用，门禁一体机呼叫中心发起开门请求，cs客户端弹窗显示一体机视频，中心可选择接听、拒绝、开门；

3、提供人员出入记录实时展示应用

1）、支持人员进出事件实时展示，包括人员基础信息、抓拍图片、进出时间、设备名称等，可全屏展示

**（二）陪护管理主模块**

支持住院区人员严格管理，避免未经允许的陪护，同时支持人脸、二维码、IC卡、手环等多种身份认证方式。

**（三）移动终端应用**

1、住院人员/陪护人员人脸录入；

2、人脸数据下发；

3、流调表格填写及收集；

4、出院自动删除人脸；

5、执行一患一陪规则；

**三、设备参数**

# 身份信息识别产品（人脸自助录入）

1. 设备需采用Android系统，配备不小于10英寸LCD触摸显示屏，分辨率不小于1280\*800；
2. ★设备需内置身份证阅读器，支持通过身份证内照片与现场抓拍人员照片比对，进行身份核验；（提供公安部检测报告复印件证明，并加盖厂商公章或投标专用章）
3. 设备需配置高清双目相机，分辨率不小于1920\*1080，上下调节角度可调节，适应强光、逆光、暗光等条件的人脸识别，支持在0.001lux低照度无补光环境下实现人脸识别；
4. 设备需支持存储不少于100000名黑名单人员，抓拍照片容量不少于10000张，本地记录（刷脸刷卡）存储容量不少于10000条；
5. 设备需支持本地黑名单信息比对，并可将本地黑名单事件，黑名单事件信息可上传平台。
6. **▲提供公安部检测报告复印件证明，并加盖厂商公章或投标专用章。**

# 人脸门禁设备

1. 设备应采用嵌入式linux系统，需支持壁挂安装；
2. 设备应采用不小于7英寸触摸显示屏，屏幕比例9:16，屏幕分辨率≥600\*1024；
3. 采用不低于200万像素宽动态双目摄像头，需支持人脸、刷卡、密码认证方式；
4. ★人脸比对平均时间应＜120ms（1:1对比方式）；最大人脸识别距离：＞4m；最小人脸识别距离：＜0.2m；认假率（FAR）＜0.0002%；拒真率（FRR）＜1%；准确率＞99.95%；（提供公安部检测报告复印件证明，并加盖厂商公章或投标专用章）
5. 本地支持≥10000人脸库、≥50000张卡、≥15万条事件记录；
6. 支持口罩检测模式，可配置提醒戴口罩模式、强制戴口罩模式，关联门禁控制；
7. 支持认证成功界面的“照片”、“姓名”、“工号”信息可配置是否显示；
8. ★应能在0.001lux低照度无补光环境下正常实现人脸识别，可在强光、逆光、暗光环境条件的人脸识别；在无可见光补光及低照度环境下实现全彩图输出预览图像；（提供公安部检测报告复印件证明，并加盖厂商公章或投标专用章）
9. 应支持防假体攻击功能，对视频、电子照片、打印照片等攻击应能防伪；
10. 10.支持通过RS485或韦根接口外接1个读卡器，同时可实现单门反潜回功能；
11. ★应支持 IC 卡（mifare卡）识读；支持识读模块的扩展功能，模块支持热插拔连接，形成一体化识别终端；应支持人脸、刷卡、指纹、二维码、蓝牙和密码认证；蓝牙识读区域直径范围应≥3 米，基于蓝牙识读的开门时间应≤1 秒；二维码模块应支持静态及动态二维码识读，应能对由 512 字符生成的二维码进行识读，支持格式应包括：QR Code、Micro QR、Code128、Code39、Codabar；应支持配置防卡片复制安全机制，功能开启后第三方卡片或复制卡片可屏蔽识读；应支持刷卡+密码、指纹+密码、指纹+刷卡、人脸+指纹、人脸+密码、人脸+刷卡、指纹+刷卡+密码、人脸+二维码+蓝牙、人脸+指纹+刷卡、人脸+密码+指纹的复合认证。（提供公安部检测报告复印件证明，并加盖厂商公章或投标专用章）
12. 设备接入系统平台后应能支持视频联动报警功能；未授权人员刷人脸时，设备应能支持抓拍图片并实时上报平台预警；系统应具有应急开启的方法，如设备支持接入消防应急信号联动开门；根据设定事件的联动关系，当检测到该事件发生时，应能触发对应的动作。
13. **▲提供公安部检测报告复印件证明，并加盖厂商公章或投标专用章。**