就医者信息泄露与信息系统故障

个人信息、病历、照片泄露或丢失，以及诊疗和收费系统无法使用时

版本 V202611，法规核对日期 2026 年 11 月 11 日。复核状态　文中法定要求已核对原文。向哪个部门报告及具体时限按当地规定，启用前填入属地联系表。

适用情形

就医者的个人信息、病历或照片被泄露、篡改、丢失，包括员工外传、工作手机丢失、账号被盗、设备中病毒或被勒索。诊疗、预约、收费系统无法使用。

第一动作

1 发现人立即报告负责人和信息管理人员，不自行处理。

2 止损。断开受影响设备的网络，停用相关账号，修改密码，收回权限。设备不关机、不重装系统，保留现场。

3 保全。截存泄露的内容和传播位置，导出系统日志、登录记录和访问记录。

4 判断范围。涉及哪些就医者、哪些信息、多少人，信息流向了哪里。

处置步骤

步骤	做什么	要点	责任人
1	补救	要求持有信息的人删除并书面确认，向平台申请删除已发布的内容，更换被盗用的账号和密钥。	信息管理人员、法务
2	报告	按规定向履行个人信息保护职责的部门和有关主管部门报告。涉嫌违法犯罪的向公安机关报案。	负责人
3	通知就医者	逐一通知受影响的就医者，可以用电话、短信、即时通信工具、电子邮件或公告。	投诉岗
4	接待与答复	就医者由此提出投诉或索赔的，按规程建立事件编号处理。	投诉岗
5	恢复	用备份恢复系统和数据，恢复后核对数据是否完整，再重新启用。	信息管理人员
6	追责与整改	查明原因。员工外传的按制度处理，权限过宽的收紧权限。	负责人

通知就医者的内容

《个人信息保护法》规定，发生或者可能发生个人信息泄露、篡改、丢失的，应当立即采取补救措施，并通知履行个人信息保护职责的部门和个人。通知包括以下内容。

1 泄露、篡改、丢失的信息种类、原因和可能造成的危害。

2　机构已经采取的补救措施，以及就医者可以采取的减轻危害的措施。

3　机构的联系方式。

采取措施能够有效避免信息泄露、篡改、丢失造成危害的，可以不通知个人。主管部门认为可能造成危害的，有权要求通知。是否通知个人由负责人和法务判断并记录理由。

系统无法使用时

1　启用纸质流程。使用纸质病历和治疗记录单，手工开具收款凭证，预约用纸质登记本。

2　无法查到既往病历和过敏史的，由医生重新问诊，判断是否暂缓治疗。

3　系统恢复后 3 个工作日内把纸质记录补录进系统，纸质原件留存，补录时注明补录日期。

4　系统故障期间的收款与财务对账。

平时准备

1　就医者信息按岗位设权限，照片和病历不存放在个人手机和个人网盘。

2　数据定期备份，备份与主系统分开存放，每季度做一次恢复测试。

3　员工离职当日收回账号、工作手机和权限。

4　前台备有纸质病历、治疗记录单、收款凭证和预约登记本。

常见错误

为了掩盖删除日志。重装系统后无法查明原因。只处理技术问题，没有通知就医者。员工把就医者照片发到聊天群，被当作小事处理。

事件记录

栏目	填写
发现时间与发现人	
事件类型（泄露、篡改、丢失、系统故障）	
涉及的信息种类与就医者人数	
原因与信息流向	
已采取的止损和补救措施	
报告的部门与时间	
通知就医者的方式、时间与人数	
不通知个人的，理由与决定人	
恢复时间与数据核对结果	

栏目	填写
整改措施	

记录人 _____　　负责人 _____　　日期 ____ 年 __ 月 __ 日