定功能。报警内容包括异常调阅用户的IP、时间、账号、访问内容，并能够进行自动阻断。同时制定应急预案等。重点关注处理结果和处理率。调阅日志保存时间宜不少于6个月，定期审核调阅日志，并对敏感数据及特殊身份患者的调阅记录进行审计。

11.2 患者查询数据安全

11.2.1 概述

适用于患者通过在线方式查询其本人健康医疗数据的场景。患者承担主体角色。

11.2.2 重点安全措施

11.2.2.1 身份识别

患者通过在线系统查询其健康医疗数据，首次注册需关联实名制手机，后通过实名制手机登录，发送手机号验证码。考虑子女代替年老父母等查询信息需要，帐号可绑定子女手机（上传身份证或户口本扫描件即可或由系统后台认证），监护人代替未成年人查询信息等情况，仿照处理。

完成注册后，个人需设置帐号与密码，系统宜对密码复杂度有一定要求，包括定期更改密码等。

11.2.2.2 信息查询

为防止账户落入他人之手，造成个人信息大量泄漏，系统宜对可查询信息进行适当限制。例如HIV、肝炎等敏感检查结果不予显示。默认仅可查询三个月内相关检查检验报告、用药情况等信息。

11.2.2.3 操作权限

系统宜对个人的操作权限有所考量，权限包括另存、复制、打印、下载等。个人进行相应操作时，页面宜显示用户需知，例如告知患者下载后数据的信息安全义务在于其本人等，提示个人注重信息保护，同时重点语句突出显示（例如标红）。

11.2.2.4 传输安全

宜采用校验技术或密码技术保证个人健康医疗数据在传输过程中的保密性、完整性，加密方法的选择宜考虑应用场景、传输方式、数据规模、效率要求等。设备宜默认开启数据加密功能。

11.3 临床研究数据安全

11.3.1 概述

本标准涉及的临床研究指以患者或健康人为研究对象，由医疗机构、学术研究机构和/或医疗健康相关企业发起的，以探索疾病原因、预防、诊断、治疗和预后为目的的科学研究活动。临床研究可以是医疗机构临床医生发起的科研项目，政府资助的科研项目，科研机构发起的以社会公共利益为目的的医学科学研究，或者涉及公共卫生安全的临床科学研究，也可以是医疗健康相关企业发起的以科学或商业为目的的临床研究。临床研究一般是在学术性的医学中心、研究机构或者医疗科研机构进行，其过程主要包括临床试验的方案设计、组织实施、监查、核查、检查，以及数据的采集、记录、统计、分析总结和报告等。

临床研究主要包括以下类型：

a) 按临床数据获取方法区分：回顾性临床研究和前瞻性临床研究；

b) 按研究目的区分：临床基础研究、临床应用研究和临床路径研究；

c) 按产品获准上市与否区分：产品上市前研究和产品上市后研究。

以产品上市获批为目的的临床试验的数据安全，请参照相关主管部门规定，不属于本标准范畴。