医院患者信息保护实践

沈剑欢,瞿怀荣

(连云港市第一人民医院信息部,江苏 连云港 222000)

摘要:在临床医疗中,无论有意或无意泄露患者隐私都会对患者造成伤害,而患者隐私保护有利于切实保障患者合法权益,利于减少医疗纠纷,建立和谐医患关系。本文从底层数据库处理患者个人信息,到医院的数据平台建设,患者就诊过程中的公共场所信息展示、线上身份核验等环节,建立严格的患者隐私保护管理。通过数据保护,从医院内部至外部网络环境,从底层架构至顶层应用,对患者就诊时提交的个人敏感信息实现全方位保护,保障患者的合法权益。

关键词:信息保护;数据脱敏;隐私

中图分类号:R197 **文献标识码**:B **DOI**:10.3969/j.issn.1006-1959.2023.19.002

文章编号:1006-1959(2023)19-0005-05

Practice of Patient Information Protection in Hospital

SHEN Jian-huan,QU Huai-rong

(Department of Information,the First People's Hospital of Lianyungang,Lianyungang 222000,Jiangsu,China)

Abstract:In clinical medicine, whether intentionally or unintentionally divulging patient privacy will cause harm to patients. While, patient privacy protection is conducive to effectively protect the legitimate rights and interests of patients, reduce medical disputes, and establish a harmonious doctor-patient relationship. In this paper, from the bottom database processing of patient personal information to the construction of hospital data platform, public place information display, online identity verification and other links in the process of patient treatment, establish strict patient privacy protection compliance management. Through data protection, from the hospital internal to the external network environment, from the underlying architecture to the top-level application, the personal sensitive information submitted by patients at the time of treatment is fully protected to protect the legitimate rights and interests of patients.

Key words:Information protection;Data desensitization;Patient privacy

目前,医院虽然在竭尽所能的确保患者的个人信息不被泄露,但医疗信息泄露事件一再发生。包括患者在医院就诊时的信息,如姓名、手机号、身份证号等常见隐私数据,以及就诊科室、就诊时间和次数等特殊敏感的医疗信息泄露事件。究其原因主要是医院信息系统保护能力不强,漏洞防护不够全面,患者隐私被轻而易举地窃取[1]。为遵循患者信息保护的义务,切实筑牢个人信息安全防线,有效保护患者个人隐私[2],某医院从核心业务数据库患者数据脱敏、数据平台患者健康档案数据脱敏、智慧服务就诊过程中患者隐私保护等维度,形成一整套个人信息保护方案。传统的数据脱敏通过识别 SQL 语句中的敏感字段内容并改写 SQL, 在数据库实现脱敏处理,并返回结果[3]。本文从患者隐私保护的角度重点介绍了新型数据库动态脱敏技术和患者智慧就诊的功能及应用效果。

1 核心数据库数据脱敏和数据平台患者健康档案脱敏系统

数据库脱敏和健康档案脱敏系统充分考虑用户数据库安全管理需求,采用全新的技术架构及理念,从数据库虚拟化、安全准入、访问控制、数据脱敏、全面审计多维度全方位保护数据安全, 有效抵御口令入侵、特权提升、漏洞入侵、SQL 注入、窃取备份、勒索病毒、脱库等数据库攻击手段,满足数据库安全管理,符合运维安全内部控制和法规法令的要求,有效保障患者重要敏感信息的安全[4]。

1.1 设计理念 数据脱敏系统支持多个平台数据库,医院核心数据库采用 Oracle 12C, 数据平台数据库采用 SQL Server 2012,系统可以直接对原数据库脱敏,通过数据库虚拟化技术和数据库引擎管理,采用数据水印、敏感信息替换和访问控制的手段,加上访问日志审计、SQL 语句审计、终端身份识别等功能,达到了数据脱敏、防脱库和防统方的目的。安全性方面,系统设计有防火墙、数据传输加密和 SQL 注入防护,通过建立黑白名单来限制访问用户,数据传输的加密方式防止数据窃取,根据 SQL 注入的特征智

作者简介:沈剑欢(1986.10-),男,江苏苏州人,硕士,工程师,主要从事网络安全、数据库、服务器管理研究

通讯作者:瞿怀荣(1982.7-),男,江苏扬中人,硕士,高级工程师,主要从事网络安全、信息管理研究

能检测、识别及阻断，防止通过应用系统的 SQL 注入入侵数据库[5]。针对高危操作的管理，系统建立审批流程，通过系统自动生成或者手动提交申请单方式，管理者对定义的高危操作进行审批，审批通过后才能执行，真正做到管理者和使用者的职权分离，防止敏感信息的泄露（图 1）。

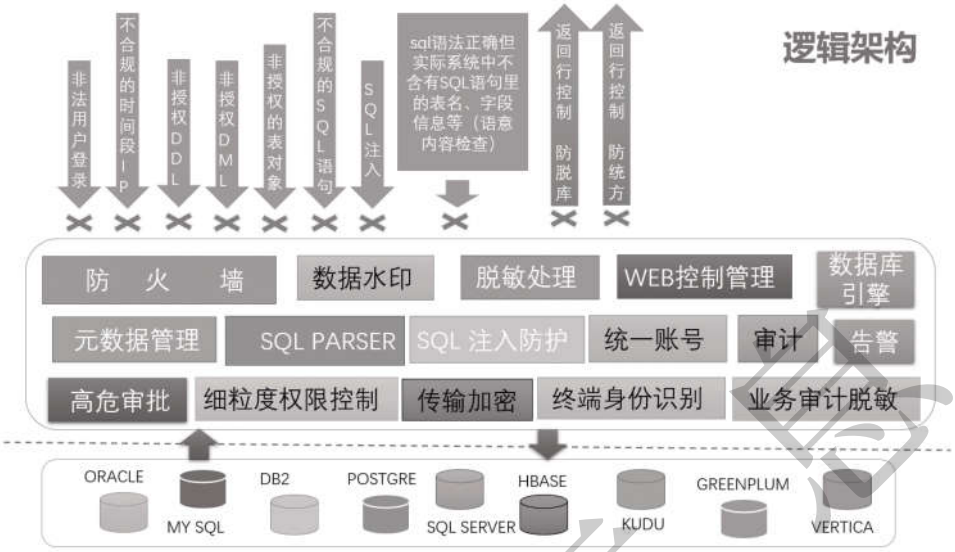

图 1 数据库和数据平台患者健康档案脱敏系统逻辑架构

1.2 实现数据库安全管理 针对开发、运维、系统管理过程中账号管理混乱、操作不透明等一系列不合规现象造成的数据泄漏事件，系统通过多因素认证、细粒度的权限控制和细粒度的数据对象授权管理，实现操作管理定位到人、责任到人的目的，实现开发、运维人员的身份统一管理、操作合规，全面保障数据库的安全管理需求，最大程度保障用户敏感信息的安全，防止数据泄漏事件的发生[6]。

1.3 实现动态脱敏 实现运维人员、外包开发人员根据其工作所需和安全等级访问敏感数据，并对核心生产库的重要敏感数据进行动态脱敏，如患者的身份证号、手机号码、账户信息等，减少患者敏感数据泄漏的风险，保证患者隐私安全。无论多复杂的 SQL，都需实现 100%的动态脱敏[7]。

2 线上线下就诊信息泄露风险及应对

从 2007 年开始，国家要求患者实名制就诊，在医疗机构线下诊疗工作中取得了显著效果，全国范围内开展互联网医院就诊以来，也采用患者实名制就诊的方式。实名制就诊便于医生掌握患者的既往史、过敏史等重要信息，避免就医过程中“张冠李戴”，确保诊断准确；实名制有利于维护互联网诊疗环境的公平性与有序性，可以从源头上堵住号贩子抢号的漏洞[8]。但其也存在一定不足，一是线下就医存在患者姓名在公共场所暴露的问题；二是由于互联网诊疗要求患者实名制就诊，线上就医需建立患者电子档案，如何保证患者电子档案的安全，如何证明就诊人是真实的本人也是一个问题[9]。

医院需提升互联网线上诊疗管理，必须保证患者信息的安全性和保密性。系统通过手机端人脸识别进行身份核验，患者数据的存储和传输加密，重要数据放置医院内部网络等手段，有效保护患者就医数据[10]。线下诊疗过程中对患者隐私进行保护，防止患者个人信息泄露。

3 系统功能

3.1 数据库和健康档案脱敏系统 以往一个数据库一套权限管理，账号创建管理复杂，权限管理维护复杂，重复劳动多。通过多因素准入控制和多维身份认证的功能，规范数据准入控制。要素包括：应用工具名称、主机名、IP 地址、登陆时间等。系统具有账号锁定策略，对于密码猜测等试图恶意登陆数据库的行为，可通过设置账号锁定策略进行防护，达到阻止暴力破解的目的。敏感数据自动发现、管理功能，系统具有内置敏感数据特征库，可对姓名、地址、电话、身份证、就诊日期等敏感信息自动识别；通过快速的敏感发现功能，一键式对数据库内的敏感信息进行扫描，对发现的敏感信息进行快速的分级分类，达到

敏感数据的快速梳理，减少人为配置工作[11]。

敏感数据分类分级是数据安全管理的基础工作，是数据共享、开放、利用的基础，系统将敏感数据从普通业务数据中脱离出来进行独立管理能更有效、更有针对性地做好安全管控。根据敏感表格、敏感列为单元组成敏感数据集合，并根据数据的敏感程度自定义敏感等级，便于更有针对性地进行分类分级管控，自动管理敏感数据表格的生成、变更和消亡，简化敏感数据管理[12]。细粒度的权限控制，权限控制是数据库安全管理体系的重要一环，系统具有 130 多种 DDL、DML 权限。同时，有角色脱敏、角色控制、角色准入等角色授权功能，使用户权限配置管理简单化。支持灵活可视化设置及控制表级别的访问权限（insert、update、delete、select）。细粒度的数据对象授权，系统可以灵活设置访问的数据库对象范围，包括表对象及 schema 对象。

为避免相关人员利用合法的语句导出大量用户敏感信息，最大限度控制敏感信息的安全性，系统具有基于敏感表格访问的返回行控制技术，表级别修改和删除行数控制。一方面，可以设置表级别的删改影响行数控制，一旦操作语句中的行数高于阈值，则语句无法正常执行，防止大批量的误删误改的发生；另一方面，支持删改操作审批执行。针对一定时间内频繁访问数据的行为进行访问频次控制，对规定时间内访问次数超过限制后对访问操作进行拦截，有效保证数据安全。数据库危险性操作如 Create User、Drop Table、Truncate Table 等是数据库面临的巨大安全风险，系统拥有高危审批功能，可以阻止危险操作的执行，避免误删误改数据库的数据，做到危险操作需高权限的审核通过处理，可依据实际使用场景选择是否需要进行高危操作管理。

系统支持敏感数据的动态脱敏管理，对未授权的账户访问敏感数据实现动态脱敏功能，确保业务人员、运维人员以及外包开发人员严格根据其工作所需和安全等级访问敏感数据。提供随机映射、固定映射、遮盖填充、范围内随机、浮动、截取、截除、时间偏移、散列等脱敏算法。可自定义脱敏算法，做到真正的 100%脱敏，无遗漏，无泄漏。系统的数据水印功能可通过向数据中添加不易识别的水印，来实现对泄露数据来源的追溯。一旦出现数据泄露，可通过水印功能实现追责。通过对结构化数据或文件数据的头部、中间和尾部自动增加数据水印的方法实现数据的权属证明和泄漏者的溯源[13]。

全面审计功能可记录单个用户对数据库的操作行为，包括用户名、IP 地址、MAC 地址、客户端程序名、执行语句的时间、执行的 SQL 语句、操作的对象等，对其行为进行全程细粒度的审计分析。登录审计功能主要记录登录通过、拒绝、锁定等响应行为；访问审计主要记录通过、拒绝、模拟拒绝、执行异常等响应行为；能记录 SQL 执行时长、标记语句里的敏感信息及脱敏处理规则、该语句的抽取行数等信息；带参数和影响行数的 SQL 注入审计功能[14]。系统具备风险态势感知监控功能，数据库的全方位风险监控，分别从数据库用户访问、访问终端、SQL 语句、风险策略、敏感资产等多角度进行监控。

3.2 线上线下就诊服务

3.2.1 智慧身份核验 系统通过手机端人脸识别进行身份核验，将姓名、身份证号、人脸图片与权威数据源进行核验，得出比对分数，并基于此进行业务判断是否为同一人。活体检测能力方面，提供了实时炫瞳、实时动作、拍照、录制动作视频、语音读数字（含唇语）等 10 种活体检测能力，按照实际业务需求进行了灵活选择。专项活体模型，针对互联网业务场景进行专项活体模型优化，适配不同业务需求的同时，提供高效的防御拦截能力，可抵挡屏幕、照片、视频、换脸、面具、3D 模型等非活体攻击，并保证高通过率和识别率。

互联网医院小程序具有大数据风险控制功能，在接收 SDK 端传入的设备指纹信息后，基于海量大数据设备因子，对 SDK 端进行设备风险识别，辨别是否为高险设备，返回识别结果，可有效防御黑产批量虚拟机、病毒侵入等攻击手段。系统具有云端安全加密功能，SDK 端对人脸图片信息进行加密，在云端接口进行图片信息的解密，利用这种端云结合的加解密方案，可有效避免第三方非法黑产绕过 APP 模拟请求攻击云端接口的行为，如脚本攻击、ROM 注入、视频劫持等，增加了对黑产常用 APP 攻击的防御能力，保障终端、云端双重验证的数据一致性[15]。数据加密防篡改功能可以防止数据被恶意修改，摒弃了传统人脸 SDK 直接采集摄像头数据的方式，升级为安全数据通道采集方式，从代码逻辑、采集方式、传输层多维度确保人脸数据采集真实有效。

为提高防作弊能力，系统提供多达 10 种离线检测方案，支持图片质量校验、多帧图片识别，有效抵

御照片、合成图、视频翻拍、3D 模型等作弊行为；通过应用合成图校验技术，可有效应对 PS、人脸融合后的图片/视频等多种防作弊手段[16]。医院内实际应用场景多，各种软件交互需求广，因此本系统提供的交互形式多样，支持在 APP、通用/微信 H5、API 等接入方式，形态全面丰富，灵活组合使用。

3.2.2 线下就医隐私保护 在门诊急诊就诊、检查检验过程中的分诊、报到和叫号环节，对各种显示屏上所显示的患者姓名均进行掩饰符号替换，保护患者隐私。患者的各种检查检验报告单要求专人管理或自助打印，严禁随意摆放暴露患者信息，线下就诊过程中通过数据隐私保护，更好的保护了患者在公共场所的身份信息，防止重要信息和隐私暴露[17]。

4 应用效果

4.1 数据脱敏和健康档案脱敏系统 脱敏系统采用内部运维管控模式，该系统具有独立于源数据库的使用者账号管理体系，使用一套账号就可以管理所有数据库的账号权限控制，用户、角色、权限可视化授权管理，以减轻管理压力。同时，使用者无需知道真实数据库的账号、密码、源 IP 和端口等信息，有效保障数据库的安全。系统对患者敏感信息通过设定的规则进行数据的变形，实现了敏感隐私数据的可靠保护，这样就可以在外包用户、开发、测试和其它非生产环境中安全地使用脱敏后的真实数据集(图 2)。

医院各管理部门用户、运维人员、外部用户等通过脱敏系统访问数据库中患者相关信息以及数据平台患者健康档案信息，在满足临床诊疗、科研、教学工作的同时，实现了患者数据的底层保护。通过数据脱敏，可以有效防止医院内部对患者隐私数据的滥用，防止患者信息在未经脱敏的情况下从医院流出，满足医院保护患者隐私数据的同时合理使用数据开展医、教、研等工作[18]。

4.2 智慧就诊服务实名认证 人脸识别实名认证功能通过一系列的数据核验、风险检测、智能认证、信息录入、活体检测和人脸信息比对等步骤，解决了身份快速辨别、信息采集录入以及安全认证等问题[19]，并可快速在线完成认证流程；身份证信息输入支持 OCR 识别(电子扫描)、手动输入和后台传入(后台已有建档信息)三种方式，方便患者自行选择，见图 3。

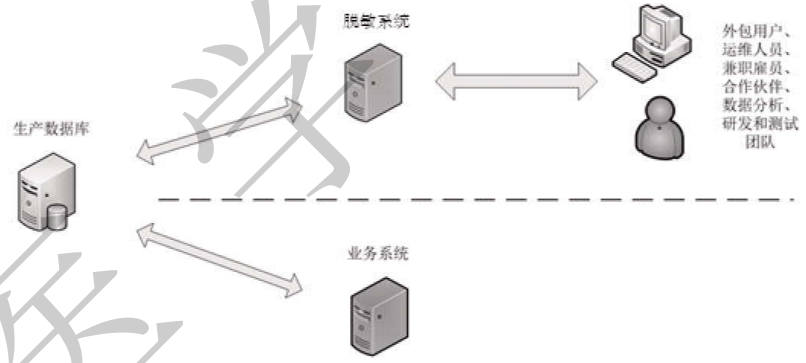

图 2 内部运维管控模式

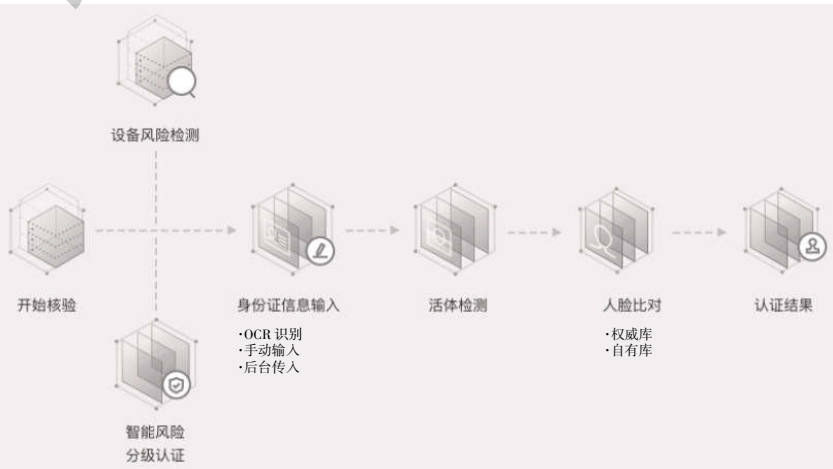

图 3 在线认证流程

实名认证系统可以确保通过认证目标为真人，通过端云配合活体检测，确定操作者是否为真人，可有效抵御彩打照片、视频、3D 建模等攻击。系统为确保所认证的人为本人，基于“真人”的基础，将现场采集的人脸图片、姓名、身份证号码与权威数据源身份信息库对比，确保操作者身份的真实性，避免身份证或人脸图像伪造等欺诈风险，权威可靠，同时也确保了数据安全。患者在互联网医院就诊过程中，通过人脸识别进行身份核验，确认为本人操作方可挂号、就医和修改个人信息，实现患者非见面式信息服务，为患者提供便捷的就医服务体验，有效拦截了非正常人脸录入。

5 总结

本系统基于结果集流式处理的精准敏感识别和动态脱敏处理，通过对 SQL 的精准解析，并对返回结果集做精准识别和标记，从而实现快速的脱敏处理，是动态脱敏领域的开拓创新。核心数据库和健康档案数据脱敏系统均通过数据处理技术对敏感字段替换或者隐藏，从而实现保护患者隐私的目的。智慧就诊服务实名认证具有很强的安全性和优秀的交互体验，互联网医院患者身份核验通过人脸识别的方式，对比权威信息库以及预留手机号码进行双重校验，确认为本人操作。通过核心业务数据库脱敏，实现了信息运维人员因工作所需访问的数据进行隐私信息的动态脱敏；患者健康档案数据脱敏实现了院内各业务系统访问患者历次就诊信息时，可根据业务场景进行隐私数据保护；通过患者线上建档信息录入和修改时的人脸识别进行身份校验，确保就诊人为患者本人，线下就诊过程中在院内公共场所叫号系统中进行姓名关键词隐藏，实现了患者线上就诊和线下就诊全流程的隐私保护。

参考文献：

[1]刘海一.智慧医院建设中个人信息保护方式的探讨[J].中国数字医学,2022,17(3):20-25.

[2]郝晓霞.论电子医疗的患者信息保护[D].济南:山东大学,2018.

[3]陈天莹,陈剑锋.大数据环境下的智能数据脱敏系统[J].通信技术,2016,49(7):915-922.

[4]杨红玉,王少伟.重大心脏疾病专病数据库脱敏系统的设计[J].中国数字医学,2018,13(7):46-48.

[5]裴成飞,杨高明,方贤进,等.数据库脱敏技术研究与应用[J].牡丹江师范学院学报(自然科学版),2020(1):16-21.

[6]徐进宇.“互联网+医疗”背景下的医院信息安全防护建设与实践[J].无线互联科技,2019,16(20):22-24.

[7]郑瑶.面向关系型数据库的数据脱敏系统的设计与实现[D].福州:福州大学,2018.

[8]刘芸,梁玉敏.浅谈医院病案管理中患者隐私的保护[J].右江医学,2014,42(6):745-746.

[9]古伟峰.医疗档案信息化与隐私保护共同发展的探讨[J].管理观察,2017(10):191-192.

[10]左晖.谈病案管理与患者的隐私保护[J].中国病案,2015(10):20-37.

[11]杨建民,苏秀兰.大数据背景下医疗档案信息化管理工作及患者隐私权保护[J].中国医药导报,2019,16(29):175-178.

[12]王海燕.Oracle 数据库后台操作的脱敏处理[J].电信技术,2015(7):91-92.

[13]张宁池,朱小娟,张宇,等.互联网商业模式下大数据脱敏方法的探讨与研究[J].自动化技术与应用,2021,40(1):150-154.

[14]王闻星,蒋协远.互联网中大型医院患者隐私信息保护仿真研究[J].计算机仿真,2018,35(4):270-273.

[15]董静.论患者隐私权的保护[D].上海:复旦大学,2011.

[16]李莉.大数据背景下医疗档案信息化管理及患者隐私权保护[J].办公室业务,2020(22):90-91.

[17]邓勇,生杰元.医院泄露患者信息侵权行为之规避对策[J].中国医院院长,2019(10):84,86,88.

[18]戴赢.电子病历中患者信息保护的探讨[J].电子技术与软件工程,2015(8):221.

[19]姬雨童,李筱永.北京电子病历互联互通中的患者信息保护研究[J].卫生软科学,2020,34(9):44-48.

收稿日期：2022-11-16；修回日期：2022-12-09

编辑/成森