大型医院联盟统一医疗数据交换平台数据脱敏解决方案

一、概述

1、建设背景

近年来，数据安全已经成为一个热点话题，各类数据泄露的安全事件频繁发生。美国电信巨头 Verizon 综合多个合作伙伴的数据分析结果并采用严格的数据驱动方法来分析安全漏洞和事件后得出了《2018 年的数据泄露调查报告》（DBIR 报告），从该报告中可得出如下结论：

1）2018 年已经发生了 5.3 万多起安全事件，其中 2216 起被确认为数据泄漏事件，数据安全形势不容乐观；

2）对企业信息安全来讲，外部威胁和内部威胁所占的比重分别为 70%和 30%。其中，在外部人员导致的泄漏事件中，62%都来自有组织的犯罪团伙；

3）在公司资产因素中，19.6%的数据泄漏事件都与数据库受攻击有关；

4）从总体上来看，医疗、住宿行业、公共事务管理、零售和金融，是如今信息泄露事件最多的 5 个行业。

随着信息化的不断发展，信息系统越来越多地使用于日常工作，成为不可或缺的工具和手段。与此同时随着医疗信息化系统的进一步发展，信息化大大提高了医院的诊疗效率并促进了科研进步，因此围绕医疗行业数据安全问题提升信息安全防护能力已经刻不容缓。

2、系统现状

**大学创建于1958年,是我国创办较早的高等中医药院校之一，是省重点建设高校。学校现有教职医护员工（含四所直属附属医院）3000多人，其中具有高级职称的专业技术人员700多人；拥有1名国医大师、3名全国名中医、2名国家中医传承与创新“百千万”人才工程（岐黄工程）岐黄学者，5名教育部教学指导委员会委员（其中中医学类专业教学指导委员会副主任委员1名、中西医结合类专业教学指导委员会副主任委员1名）；拥有一批对国家和卫生部有突出贡献的中青年专家、国务院特殊津贴专家、国家级名老中医学术继承人指导老师、全国百名杰出青年中医、全国优秀教师等。

大学拥有四所直属附属医院，分别为大学附属人民医院、**大学附属第二人民医院、**大学附属第三人民医院和**大学附属康复医院。随着医疗卫生事业的发展，**大学各个附属医院的医疗信息化建设已经取得显著成果。已经上线的主要的医疗业务信息化系统包括HIS(Hospital information system，医院信息系统）、EMR(Electronic medical records，电子病历系统)、PACS(Picture archiving and communication system，医学影像存档与通信系统)、LIS(Laboratory information system，检验信息系统）、UIS(Ultrasound information system，超声信息系统)、ECGIS(ECG network information system，心电网络信息系统)、PEIS(Physical examination information system，体检管理信息系统)等。

以上信息化系统的建设，完成了**大学各附属医院医疗信息化过程的第一个步骤，逐步实现了医疗业务数据的信息化采集与存储。随着医疗信息系统的不断深入应用，使得医院对医疗信息化的需求已经从简单的医疗业务数据采集与存储发展到了对医疗业务数据的共享与交换，并逐步向医疗业务数据的分析与挖掘方向延伸。

**大学结合医疗行业信息化的特点，提出了“医疗行业数据交换与共享”解决方案，针对直属的 4 所附属医院，建设医疗数据交换与共享平台，打破存在于医院中的各种“信息孤岛”，使得各附属医院的信息化发展迈入新阶段。

二、医疗数据交换平台脱敏安全需求

1、医疗数据交换平台现状

统一医疗交换平台建立之后，各附属医院已经对院内的各个信息系统包括 HIS(医院信息系统)、EMR(电子病历系统)、PACS(医学影像存档与通信系统)、LIS(检验信息系统)、UIS(超声信息系统)、ECGIS(心电网络信息系统)和 PEIS(体检管理信息系统)等数据进行数据汇总，每周定期将数据通过前置机发送到统一医疗数据交换平台进行汇集汇总。

2、医疗系统数据脱敏现状

目前**大学的统一医疗数据交换平台中各个附属医院，在数据外发存储到平台内数据中心内的数据均为包含个人真实信息的数据。

在数据提交到统一医疗数据共享平台进行数据分析时，现阶段做法如下：

1）数据不经过任何脱敏处理，直接提供真实数据到平台进行分析；

2）内部人员手工或者编写简单的函数进行脱敏；

3）交由第三方开发商处理敏感数据等手段。

3、技术方案

针对复杂的 IT 环境，通过部署数据库脱敏系统，将医院生产系统内涉及到 4.1 章节内的脱敏对象（主要包含医患个人用户信息和财务等敏感信息）提前进行脱敏处理，将脱敏后的数据通过前置机装载到数据交换平台的目标库，让非授权人员获得敏感数据后，也无法看懂数据信息，保证核心数据的保密性，防止第三方人员利用个人用户信息进行医疗诈骗等恶意行为。

各附属医院内数据交换脱敏流程如下图所示：

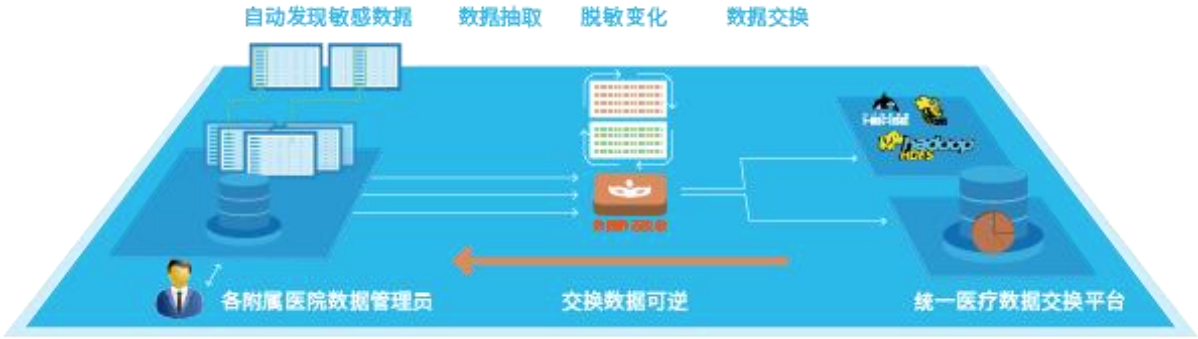

图 4 1 医疗数据脱敏系统工作流程

1）脱敏系统根据脱敏对象设定的敏感数据发现规则对原始数据库进行数据扫描，自动发现敏感数据类型和所在位置；

2）从原始数据库上抽取数据，在脱敏平台上进行脱敏处理，对用户敏感数据进行遮蔽或者仿真等操作，在此过程中各家医院保持脱敏规则和算法一致；

3）经过脱敏后的数据，写入到指定的数据外发或者医疗大数据信息共享交换平台环境中。

4）各医院通过统一医疗数据交换平台取得数据，然后将从交换平台取得的脱敏数据通过脱敏系统进行可逆计算，恢复成原始真实数据。

三、方案优势与客户收益

1、客户收益

通过上述的解决方案能够有效解决**大学统一医疗数据交换平台中所面临的数据安全问题，提高数据的安全性、机密性。最大程度地保证不会产生因外部与内部数据窃取、敏感数据被直接拷贝等原因，带来的个人用户信息泄露等后果。满足网络安全法、信息安全等级保护及各行业相关政策要求。

具体给客户带来的价值如下：

1）部署实施过程简便快捷

中安威士数据库静态脱敏系统内置了丰富的敏感数据发现规则，通过简单而灵活的配置即可对敏感数据进行扫描、脱敏，而且能够提

供通用、定制要求的脱敏算法，在不需要投入更多的人力物力的基础上快速部署实施。

2）保护隐私数据，满足法规要求

通过使用中安威士数据库静态脱敏系统，可以有效防止各附属医院信息系统内敏感数据随意导出，防止敏感数据和个人用户信息在未经处理的情况下从开放的环境中被复制、流出、泄露等。提高统一医疗数据平台的敏感数据和个人用户数据的防护能力，提升统一医疗信息共享交换平台整体的安全等级，满足合规性要求。

3）多方位保证业务的正常运行

中安威士数据库静态脱敏系统针对每种敏感数据类型均提供了高度仿真的脱敏算法，保证脱敏后保持原有特征、语义，保证不同表之间相同字段的数据关联性，保证数据的长度不超过表结构，能够顺利入库，满足大数据分析对医疗数据真实性的需求。通过可逆算法，还原个人用户信息等原始数据，满足各个医院之间互相共享数据需要。在避免敏感数据外泄的前提下，保证了各类业务的正常推进。