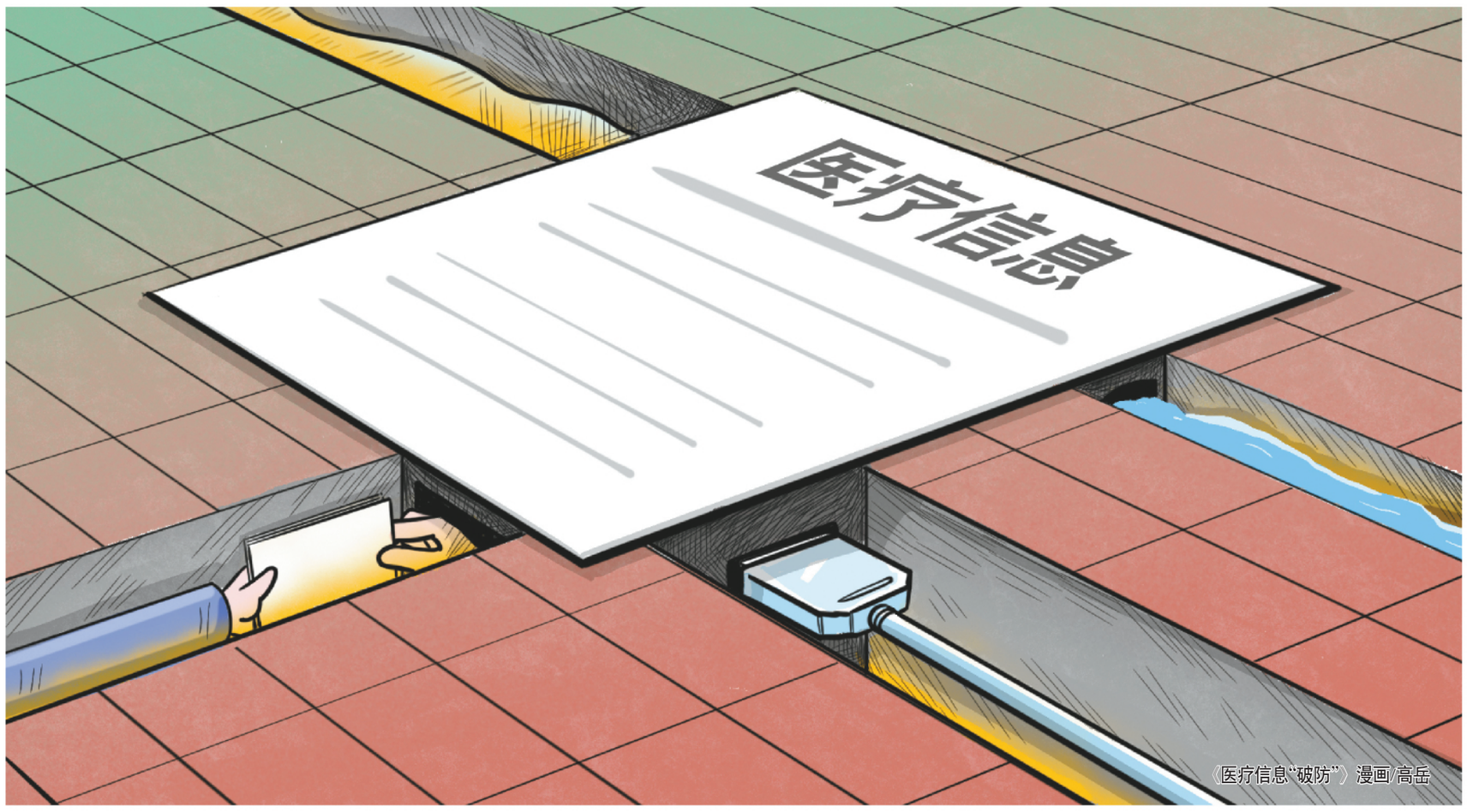
一条产妇信息售价50元

记者调查医疗信息泄露问题



《医疗信息“破防”》漫画/高岳

□ 本报记者 文丽娟

近日，山东孕妇刘丽(化名)突然收到一条加“好友”申请：“××月子中心，为您提供专业产后服务。”她心头一紧——几天前，她刚在当地一家医院和妇幼保健院做完产检，并且此前从未在任何机构留下孕产信息。

“电话、住址、怀孕周数，各种隐私信息对方了如指掌。”刘丽立即拨打12345投诉。次日，医院客服联系她：“可能是××月子中心冒用医院名义进行推销。”工作人员坦言，这类事件“并非第一次发生”，医院承诺彻查此事，并希望刘丽配合取证追责。

刘丽的遭遇并非个例。近年来，从明星病历外泄到普通患者就诊记录被贩卖，医疗信息泄露俨然形成一条成熟的黑色产业链。

患者隐私如何被窃取？违法交易如何运作？又该怎样斩断这只“黑手”？《法治日报》记者对此展开调查。

花钱能查医疗记录

记者近日在社交平台以“就诊信息”“病历”等关键词进行搜索，发现不少包含隐晦话术的帖子，比如可cx(即查询)“地址出行”“定位追踪轨迹”“开房”“流水”“档案”“记录(社保记录、医保记录、医疗记录等)”等。

其中一个帖子的信息，指向一个IP归属地为境外的社交账号。记者私信该账号咨询“如何查询某人医疗记录”，对方发来一张“业务单”，上面写着能够查询他人手机定位、身份证正反面信息、婚姻记录、社保记录、医保记录、医疗记录、学籍学历、全部资产等信息。其中，查询医疗记录需提供手机号、身份证号码、城市，查询结果包含所有医疗记录、医保记录、住院记录，出单时间为1至2天，售价为1200元。

“只有对方手机号，没有身份证号码，也不知道他在哪座城市，能查询医疗记录吗？”面对记者的提问，对方很快回复道：“再加100元就可以”。

该账号曾于今年4月中旬发布一条名称为“历史医疗记录，医保记录，精准出；婚前健康检查、堕胎记录等个人隐私随便查”的帖子，正文内容包含两张图片，附有某人的就医记录、消费记录、社保缴费三个选项。在就医记录一栏，可以看到定点医疗机构名称、经办时间、开始时间、结束时间、就诊凭证类型、医疗类别、病种名称、住院诊断名称、手术操作名称等信息。其中，在“病种名称”一栏，有月经不规则、病毒性皮疹、流行性感冒、月经紊乱、人流术后、抑郁状态、难免性流产等信息。

该类账号大量存在于互联网上。据“网信上海”公众号消息，近期，上海市网信办在专项执法行动中发现，一批医疗服务类互联网企业(主要从事医疗软件开发与维护、医疗服务培训、数字健康服务等)未依法履行网络安全、数据安全保护义务，所属系统存在网络安全漏洞，被境外IP访问并窃取。发生个人信息泄露情况，反映出部分医疗服务类互联网企业存在个人信息制度不规范不健全、安全防护不严密、存储不合规等问题。上海市网信办根据相关法律法规对一批医疗服务类互联网企业予以行政处罚。

一位在“开盒群”卧底过的业内人士直言，有“开盒者”会将大量医疗信息非法曝光，并进行恶意揣测。一些人的体检报告、内脏、骨科的彩超图片被非法公开，成为他人窥伺、意淫的对象；还有人的妇科、精神科医疗报告被非法公开，被他人肆意点评、嘲讽。

多种途径泄露信息

这些医疗信息是如何被泄露的？

中国政法大学证据科学研究院教授、中国政法大学医药法律与伦理研究中心主任刘鑫告诉记者，可能的泄露途径主要有以下几种：外包服务漏洞，第三方检验机构、医疗设备维保商等合作方接触患者数据；患者自身疏忽，随意丢弃带有个人信息的检查单据、处方笺；公共场景泄露，医院Wi-Fi被植入窃取程序、自助终端遭遇窃密。此外，一些患者的用药记录在医保结算环节流转时，也可能产生数据泄露风险。

“产科、新生儿科是重灾区。”刘鑫指出，少数医务人员将患者信息视作“资源”，当成“商品”出售。

最高人民检察院《关于印发检察机关依法惩治侵犯公民个人信息犯罪典型案例的通知》曾通报这样一起典型案例：吴某甲、吴某乙系一家保健按摩中心的经营者，为扩大客源，吴某甲向某医院产科主管护师韦某提出，由韦某提供产妇信息，并承诺每发展一名客户就给韦某50元或60元报酬，若客户后续办卡消费则另外向韦某支付10%的提成。截至案发，韦某向吴某甲、吴某乙出售包括产妇姓名、家庭住址、电话号码、分娩日期、分娩方式等在内的产妇健康生理信息500多条。

记者梳理公开资料发现，类似案件时有发生：北京某医院员工符某某将明星病历发至微信群炫耀，导致隐私扩散；上海某医院主任私下传播患者裸照，被暂停执业。

还有系统漏洞，让第三方平台成为“后门”。

在浙江某妇产医院32名产妇信息泄露事件中，罪魁祸首是一款第三方签到软件。该软件违规上传孕周、预产期等数据，最终流入黑产市场。四川省某精神卫生中心2.7万份患者档案被盗，则是因省级医疗信息共享平台接口未做好加密工作，遭黑客轻易攻破。

重拳之下屡禁不止

记者梳理发现，目前我国已有多款守护患者隐私权的法律条文。

比如个人信息保护法第28条将医疗健康信息列入敏感个人信息范畴，第55条要求个人信息处理者应当事前进行个人信息保护影响评估，并对处理情况进行记录。民法典第1226条明确规定，医疗机构及其医务人员应当对患者的隐私和个人信息保密。泄露患者的隐私和个人信息，或者未经患者同意公开其病历资料的，应当承担侵权责任。《医疗机构病历管理规定》规定，除为患者提供诊疗服务的医务人员，以及经卫生计生行政部门、中医药管理部门或者医疗机构授权的负责病案管理、医疗管理的部门或者人员外，其他任何机构和个人不得擅自查阅患者病历。

受访专家指出，尽管相关法律法规明确保护医疗隐私，但现实中维权难、执法软、违法成本低等问题突出。

在刘鑫看来，虽然我国现有“三合一”法律保护，如民法典明确医疗机构泄露隐私需承担侵权责任；医师法、护士条例规定泄露者可被警告、停业甚至吊销执照；刑法修正案规定，公职人员泄露信息需从重处罚，但实践中多处罚直接责任人，很少追究管理者连带责任，违法成本低导致威慑不足。

“医疗记录被泄露屡禁不止，深层原因有很多。一是管理失职，职能部门对隐私界定模糊(如‘就医痕迹是否属于隐私’)，未细化员工行为规范；二是利益驱动，医务人员贩卖信息获利空间大(如每条产妇信息售价50元)，且查处困难，查处概率低；三是相关社会顽疾，比如公民个人信息买卖猖獗，骚扰电话精准投放等暴露治理手段失效。”刘鑫说。

他指出，破局之道应该从“追责个人”到“系统治理”，比如强化警示教育，借鉴反腐模式，制作泄露隐私典型案例的警示片，强制相关岗位人员学习；完善连带问责机制，不仅处罚泄露者，还需追责机构管理者，倒逼医院加强内部管控；严打黑产链条，加大对数据交易平台、非法买家的打击力度，提高违法综合成本；借鉴国际经验，规定只有在必要时才能调阅病历，降低数据泄露风险。

“医务人员需树立‘隐私即红线’的职业伦理，将保密意识融入日常操作；患者也要培养‘隐私洁癖’，妥善处理废弃医疗单据，对可疑营销电话主动取证维权。”刘鑫说。

受访的业内人士和专家指出，守护医疗隐私不只是法律命题，更是文明社会的底线。从加密技术到严厉刑罚、从医院自查到公众警惕，唯有织密这张防护网，才能让每个人安心走进诊室，不必担心隐私成为他人手中的“商品”。

经纬观

保护患者隐私需构建医患协同“防护网”

□ 刘鑫

在医疗系统内部，个人信息与隐私的泄露风险广泛存在，且涉及线上、线下两大途径。

线上环节涵盖了App挂号、互联网诊疗、医疗平台的注册咨询及网站留言等场景，每一次指尖的操作都可能留下信息安全隐患。

线下部分，门急诊流程中的挂号、台账记录、叫号系统声音及显示、门急诊病历资料，乃至留观患者的各种标签，都可能成为信息泄露的源头；住院环节中，护士站的各类文件、留言板信息，病历在流转过程中的各个节点，均存在信息暴露风险。此外，行政后勤部门在收费、财物管理以及医疗废物处理等工作中，也可能接触并意外泄露患者信息。值得注意的是，病历查阅、复制以及行政单位出于管理目的调用病历等操作，同样可能成为患者个人信息与隐私泄露环节之一。

这些潜在的风险点，如同“暗箭”一般，时刻威胁着患者信息安全，亟待引起高度关注。

《医疗卫生机构网络安全管理办法》第二十二条规定，采取数据脱敏、数据加密、链路加密等防控措施，防止数据收集过程中数据被泄露。医疗机构可通过数据脱敏、数据库防火墙拦截、生物识别替代等方式提高数据安全性。例如，对批量导出、异常时段访问等行为实时拦截，在门诊叫号屏、检验报告打印机等公共终端显示信息时，自动隐去患者全名等身份信息，如使用“张×华”代替全名，隐去部分身份证号(如110××××××××××××5678)等，防止患者信息在挂号、取药等多个环节被频繁暴露。什么时候可以使用“去标识化”处理技术、什么时候应当使用“匿名化”技术，需要医疗机构管理者在医疗机构的内部管理规定中予以明确和细化。

医疗机构可以遵从“数据最小化”原则，建立岗位权限清单，不同岗位的医务人员权限相互独立，例如，医院实施电子病历分段加密后，药剂师只能查看用药记录，无法查看影像资料，检验科仅可查看检测数据。医务部门或病案管理部门要加大病历查阅、复制及调取的管理力度，谨慎甄别调阅目的及权责，避免因管理不善导致数据泄露而引发纠纷。同时，加强年度隐私核查，聘请第三方机构模拟“数据黑客”攻击路径，通过全方位模拟测试发现潜在的数据泄露风险。此外，应对离职人员进行数据追踪，医护人员调岗或退休后，医疗相关账户应立即予以注销或权限变更，及时防范泄密风险。

医疗机构在与第三方合作时，应注重防范数据泄露风险。建立合作服务商“安全保障”制度，在合同中约定数据泄露的细则及赔偿条款，例如，要求HIS、LIS、PACS系统(医院主要业务系统)运维商缴纳年度服务费的一定比例作为安全押金。第三方App接入医院数据前，须在封闭环境完成相关压力测试，及时发现管理漏洞。

应构建快速响应机制，制定应急预案，加强应急演练。同时，提醒就诊患者进行隐私自检，在挂号单背面或相应位置印制自查清单，提醒患者及时销毁带个人信息的废弃单据，检查候诊区是否有人偷拍电子屏等。医疗机构应对患者进行反骚扰话术宣教，告知患者接到疑似数据泄露的推销电话时，应要求对方提供个人信息来源合法性证明并录音取证。患者则应养成“隐私洁癖”，当接到可疑营销电话时，可依据个人信息保护法要求对方立即说明信息来源；不要随便放置、丢弃包含个人信息和隐私的文件、纸张，如挂号条、处方、发票等。

医疗机构需以“零信任”原则重构数据安全防线。在管理层面，要构建完善的数据分级分类制度，对患者病历、检查报告等敏感信息进行细致分级，不同等级匹配相应的加密、访问权限。同时，强化数据安全培训，定期开展信息安全教育，提升全员对数据保护的认知，让每一位医护及行政后勤人员都成为信息安全的捍卫者。建立严密的内部监督机制，设立信息安全监督岗位，对病历查阅、数据调用等操作进行全程监控，发现异常及时预警、处置。

患者也应注意，在AI时代，隐私保护从来不是单方面的责任。唯有医患携手筑牢安全防线，将技术硬核防御、完备的管理流程与人文软性关怀相结合，方能真正保护医疗数据安全，让AI技术回归治病救人的正道，而非变成探秘隐私的黑手。

(作者系中国政法大学证据科学研究院教授、中国政法大学医药法律与伦理研究中心主任)

信团伙把猪肉『浸泡』牛肉粉后当牛肉卖

贵阳检察治罪+治理筑牢食品安全防线

□ 本报记者 王家梁
□ 本报见习记者 胡特旗
□ 本报通讯员 丁艳红

“我买的牛肉不容易煮熟、没有牛肉味、吃起来也不香，您看看这肉是不是有问题？”

2023年以来，贵州省贵阳市观山湖区市场监督管理局陆续接到市民反映相关问题，市场监管部门立即联合有关部门开展集市假冒伪劣牛肉专项治理行动。

根据有关线索，公安机关启动立案调查程序。经查，贵阳市销售假牛肉的违法犯罪团伙有3个，其作案方式为低价购买猪肉，用浸泡“牛肉粉”、胶水粘牛角等方式处理后，利用乡镇赶集天设立临时摊点，假冒牛肉提高价格销售。

近日，由观山湖区人民检察院提起公诉的白某峰等人涉嫌销售伪劣产品案，经法院审理后作出有罪判决。该团伙是3个销售假牛肉犯罪团伙中人数最多的，也是案情最复杂，最后一个作出判决的案件。

售假团伙互相勾连

2023年4月，观山湖区市场监管局陆续接到市民反映，称其在辖区多个集市上购买的牛肉存在质量问题。同年7月10日，该局联合街道办、派出所等进行突击检查。经检测，白某峰、丁某亮、王某兰等多人售卖的牛肉均未检出牛源性成分。白某峰等人辩称，其销售的牛肉是从别处购买，自己并不知情。市场监管局随后将案件线索移交公安机关。

公安机关高度重视，经研判后组织侦查，逐步锁定3个贩卖假牛肉的犯罪团伙。一个是以白某锋为主犯，丁某焰、杨某勇、李某定等为从犯的犯罪团伙；一个是丁某高、丁某亮、胡某涛3人组成的犯罪团伙；还有一个是以石某、王某兰夫妇为主犯，黄某庚、王某付、王某贵等为从犯的犯罪团伙。

经侦查发现，3个犯罪团伙都以贩卖假牛肉为主，各做各的生意，但又相互联系。3个犯罪团伙的成员大多来自同一个地方，相互之间都是亲戚朋友关系，比如丁某高是白某峰的三叔，石某、王某兰夫妇与丁某高、白某峰系同乡，并且犯罪手段基本一致，都是购买猪肉后，先剔除猪骨头、猪肉筋膜和肥肉，再通过浸泡“牛肉粉”增香增色等手法，将猪肉充当牛肉销售。为了让售假行为看起来更逼真，3个犯罪团伙还购买少量牛头、牛肉、牛油、牛脚等，把伪造后的猪肉用胶水粘在牛脚上，有时候还会把猪肉和少量牛肉混在一起充当牛肉售卖。

公安机关在掌握大量犯罪证据后，集中收网，一举抓获3个犯罪团伙的主要成员，并当场查获鲜肉若干，后经对查获的鲜肉进行检测，检测出猪源性成分，未检测出牛源性成分。

提前介入引导侦查

3个犯罪团伙主要成员到案后，丁某高犯罪团伙和王某兰犯罪团伙成员很快交代了自己的犯罪事实。据供述，2022年8月左右，丁某高、丁某亮父子用猪肉充当牛肉对外进行销售。2023年7月，胡某涛在明知被告人丁某高、丁某亮实施销售假牛肉的情形下，参与其中，又自行或与他人合作销售假牛肉。石某、王某兰夫妇也早在2022年3月就开始对外销售假牛肉。2022年10月至2023年10月，王某贵、黄某庚、王某付、罗某富先后加入石某、王某兰团伙一起销售假牛肉。

白某峰团伙中，丁某焰等人供述了参与销售假牛肉的违法犯罪事实，但白某峰却拒不承认，称自己销售的牛肉系从他人处购买，自己并不知道是假牛肉。

因犯罪嫌疑人人数较多、案情重大复杂，2023年12月，公安机关邀请检察机关提前介入。“除白某峰外，其他几个犯罪团伙成员都承认了犯罪事实，该系列案看似简单，但仔细审阅卷宗后发现，不同人参与销售假牛肉的时间不一样，在销售方式上既存在以猪肉充当牛肉，也存在牛肉猪肉混合销售的情况，在收款方式上既有微信收款也有现金收款，因此在查清犯罪金额上存在困难，而销售金额是认定是否构成销售伪劣产品罪的关键。”承办检察官王卫国说。

“进一步调取犯罪嫌疑人转账记录，核实销售金额；对白某峰供述的上家进行调查，查清是否确实存在向上家购买假牛肉的情况；加大追捕力度，使在逃犯罪嫌疑人尽快到案……”观山湖区检察院就3起关联案件共发出32条引导侦查意见。

经公安机关进一步侦查，未发现白某峰向周边大型屠宰场进购牛肉的记录，但发现其进购大量猪肉的记录，确定白某峰供述的上家是其编造的，白某峰才是制作假牛肉的元凶。2024年7月至9月，石某、王某贵、罗某富陆续被追捕归案，几人到案后也如实交代了犯罪事实。

守护舌尖上的安全

2024年3月5日，公安机关就白某峰犯罪团伙、丁某亮犯罪团伙全部成员和王某兰犯罪团伙中到案成员涉嫌销售伪劣产品罪，移送检察机关审查起诉。同年10月15日，公安机关将石某、王某贵、罗某富3人移送检察机关审查起诉。

检察官审查后认为，2023年8月至11月，白某锋、丁某焰、杨某勇等通过以猪肉充当牛肉，猪肉与牛肉掺杂等方式，按照每斤25元至35元不等的单价以售卖牛肉为名对外销售，销售假牛肉共计85万余元，丁某焰、杨某勇、李某定、唐某春4人参与销售的金额为12万元至36万余元不等，均达到构罪标准。该团伙成员中兰某、胡某、陈某龙等人因参与时间短、次数少、金额小、仅从事驾驶工作而不知情等原因，不构成犯罪。丁某高犯罪团伙3人、石某和王某兰犯罪团伙6人均构成犯罪。

2024年4月至11月，观山湖区检察院就3起团伙案分别向观山湖区人民法院提起公诉。2024年7月至2025年2月，法院经审理后作出判决：对白某峰以销售伪劣产品罪判处有期徒刑九年，并处罚金五十万元，对丁某焰等4人分别判处有期徒刑一年八个月至八个月不等，并处十九万元至九万元不等的罚金；对丁某高等3人以销售伪劣产品罪判处有期徒刑二年六个月至六个月不等，并处十三万元至四万五千元不等的罚金；对石某、王某兰以销售伪劣产品罪，分别判处七年二个月、七年有期徒刑，分别并处三十万元、二十八万元罚金，对黄某庚等4人分别判处有期徒刑一年三个月至八个月不等，并处十四万元至四万五千元不等的罚金。

针对假牛肉在市场中流通的问题，观山湖区检察院会同公安机关、市场监管局等部门到集贸市场、乡镇赶场点等进行现场宣传，广泛公开不法分子常用欺骗手段，引导消费者到有销售牛肉相关资质和检验资质的正规商超、农贸市场固定摊位等购买牛肉，不购买流动商贩销售的来源不明的低价牛肉。

今年年初，观山湖区检察院向相关街道办事处发出检察建议，建议对销售生鲜肉的流动摊贩加强管理，保障流动摊贩生鲜肉类等食用农产品安全。该院与区市场监管局、综合行政执法局就相关问题进行磋商，就加强食品安全监管达成一致意见，观山湖区某街道办事处、区市场监督管理局等行政机关根据各自职责对辖区流动摊贩进行了全面检查，要求流动摊贩在摊位明显位置公示营业执照、向消费者主动出示“溯源码”，对发现的问题及时整改等。

前不久，观山湖区检察院对整改情况跟踪回访，未发现市场中生鲜肉类农产品食品安全问题。