医生收回扣多地屡禁不绝，新型高端药品是高发区

新华视点

新华社记者马晓媛、赵阳、刘翔霄、宋育泽

近日，山西大同一家三甲医院医生自曝当医生十几年间，共收受回扣超过50万元，且医院领导也参与其中，引发舆论热议。目前，大同市卫健委已牵头组成调查组对相关问题进行调查。

事实上，医疗行业收受回扣问题早已不是新鲜事。根据公开可查的法院判决文书统计，2016年至2019年间全国百强制药企业中，有超过半数被查实存在直接或间接给予回扣的行为，其中频率最高的企业三年涉案20多起。

“新华视点”记者调查发现，近一两年来，随着药品集采等改革措施的实施和医疗领域反腐的深入推进，医疗行业收受回扣现象已明显减少。但在一些高值药品、耗材领域依然大量存在，同时回扣的隐蔽性增强。

医生曝医院“塌方式”收回扣，当地称已成立调查组

在网上热传的视频中，一位穿着白大褂的中年人自称是“某西省某同市最大的那家三甲医院的执业医师”，表示“做医生十几年，在此期间参与收受医疗回扣，保守估计在50万以上”，还称“这事情不是我一个人做的，我和我的同事、主任、副院、正院，基本上都在参与这个事情，还包括药师，可谓是塌方式的、全员参与的。”

记者联系了这名举报者。对方表示与医院“有点过节”，但“爆料的目的不重要，重要的是我说的都是实话。”他说，医疗回扣会导致该用的药用，不该用的药也用，医生滥用药物加重患者负担。“说白了就是经济利益驱动，小病大治，欺骗患者。这不光在我们医院普遍，在全国都很普遍，是公开的秘密。”

记者从大同市卫健委了解到，此次自曝收受回扣的医生丰某是国药同煤总医院呼吸与危重症医学科的一名主治医师。国药同煤总医院前身是大同煤矿集团有限责任公司总医院，现隶属于国药同煤（大同）医疗健康产业有限公司，国药集团占股51%，晋能集团占股49%，是大同市三家三级甲等综合医院之一。

山西省大同市卫健委负责人王继武表示，4月10日在网上关注到涉事医生反映情况后，已第一时间派出一名副主任带队进入医院进行调查了解。根据医院的隶属关系，目前已由国药集团、晋能集团和大同市共同组建事件调查组；对违反管理规定的行为，一经查实，将依法依规严肃处理。

国药同煤总医院党委书记王全印说，丰某在2016年与同科室一女护士发生口角并与其丈夫发生肢体冲突，经派出所调解后女护士道歉并赔偿3000元，次日丰某追索赔偿1000元未果，后以各种理由反映医院存在包庇和袒护行为，一直对医院存在不满情绪。2018年开始，丰某多次向医院纪委、省委巡视组反映医疗回扣等问题，被相关部门认定“证据无法落实”“与事实不符”。

“丰某说收受药品回扣，他提供的证据是一些写在纸条上的与药品有关的数据，但证据不充分、不能形成链条；丰某本人也无法说清哪个药商给过他现金，或者哪个人给他转过账，没有查实过。”王全印说。

大同市卫健委及国药同煤总医院方面均表示，相关调查结果出来后，将及时向社会公布。

新华社发 徐骏 作

新型和高端药品回扣高发，利益输送更加隐蔽

事实上，医疗行业收受回扣问题屡被曝光。2019年，海南万宁市和乐中心卫生院一名医生通过网络举报自己和同事收受回扣，称医药代表按药品价格10%至15%的比例给回扣。同年，有网民举报苏州大学附一院医生杨某乱装支架，装一个给一万元回扣。

“前些年拿回扣现象严重，腰上打个钉子4000元，就要给医生1500元回扣，所以耗材大户骨科、心血管科不少医生都发财了。”一位医疗行业人士说，“但是近年来实行两票制、集采、医疗反腐，拿回扣的空间大大缩小了。”

山西省一位从业十多年的医药代表告诉记者，国家推行药品集中采购后，有降压药从30元降到2元，心脏支架从2万元降到3000元，基本没有赚头，更没有回扣。“原来一个药企在一个省有几百个药代，现在几个人就够了，很多药代都失业了。”

记者调查了解到，虽然近年医疗行业收受回扣现象明显减少，但仍然大量存在。

一位医卫专家表示：“推行集采后，一些医生不愿意开集采药品，一些医院手术中的非集采耗材的费用明显增长。”一位业内人士告诉记者，一些刚研发出来的新型药品、器械、材料往往都很贵，又没有纳入集采，是医疗回扣的高发区。

某肿瘤医院一位医生说，肿瘤治疗领域拿回扣现象相对严重，治疗肿瘤周期长，所用的药物都比较昂贵，药企多是“带金销售”；此外做肿瘤基因检测的患者也多是由医生介绍检测企业，医生会从中收取回扣。

重拳打击之下，医疗回扣还出现了新形式。中国社科院当代中国研究所科研办副主任陈秋霖说，互联网医疗的合规化为药企打通了线上市场，以药养医问题从线下转移到线上，通过“带金销售”导致过度开药。

有医疗行业人士告诉记者，现在医药代表与医生之间的利益输送更加隐蔽。“过去是直接送钱，现在是送服务——大专家出门时车接车送，请客吃饭时帮着结账，大专家的亲友有了困难帮助解决。”

医疗行业回扣缘何“禁而不绝”？

医疗回扣现象由来已久，从中央到地方也一直不乏治理之策，但为何这一乱象始终难以禁绝？

一位业内人士告诉记者，当前国内药企间存在激烈的同质化竞争，拼不了技术就只能拼市场，推动了营销费用走高。特别是一些辅助用药和检验项目，属于可开可不开，为了增加销量，就只能通过给医生回扣的模式销售。“一个企业送了，别的企业也要立刻跟进，都争着给医生送钱，慢慢地大家都这么干。”

同时，医疗系统关键岗位权力集中且缺乏有效监管也导致回扣难以禁绝。多位受访者表示，在集采实施之前，医院各科室是药品从生产到进入药房的必经之路，科室负责人通常拥有主导甚至是绝对话语权，因此是医药代表猛攻的对象。

“对重点岗位和关键环节的廉政风险防控重视程度不够、监管流于形式，是医疗系统的通病。”一位业内人士说。

此外，不少业内人士认为，医生往往工作量大，还面临高风险，相比之下收入却并不高。“医生的收入与付出不相符，导致部分医生会通过一些‘非正常途径’获取收入。”某三甲医院的医生表示。

整治药企违规营销，保持医疗领域反腐高压态势

近年来，从国家到地方，持续对各种医疗腐败进行整治。

2020年7月，国家卫健委宣布，新一轮药企违规营销专项整治开始，重点整治医务人员收取回扣、药企违规营销等行为。

去年，国家医保局推动建立医药价格和招采信用评价制度，涉及医药商业贿赂等7种失信行为的医药企业将被纳入失信“黑名单”。国家医保局价格招采司有关负责人说：“医药企业对于回扣个案的罚款往往不敏感，但给予回扣会导致其丧失进入集采市场的机会，就会产生强大的震慑效应。”

业内人士普遍认为，药品、耗材集中带量采购，在遏制医疗回扣中发挥了有效作用。随着越来越多的药品、耗材被纳入集采范围，医疗回扣的生存空间将大大缩小。

采访中，不少医疗从业人士表示，治理医疗回扣现象，还需统筹考虑、多管齐下。“要提高医生的薪酬待遇，让他们的正常收入能够体现自己劳动的价值。”山西白求恩医院院长吴华说。

此外，陈秋霖等专家建议，紧盯关键环节廉洁风险，运用信息化手段加强筛查、防控，对顶风违纪违法的，发现一起、查处一起，持续保持医疗领域反腐高压态势。

新华社太原4月14日电

二手手机交易存个人信息安全隐患

我们的旧手机该如何处理

新华社记者高亢

近日，网络上传出二手手机交易可能存在个人信息泄露风险，引发社会广泛关注。

二手手机交易存在哪些风险？旧手机中删除的个人信息能否恢复？我们的老旧手机究竟应该如何正确处理？

二手手机个人信息泄露引发担忧

经过简单操作，即可将一台已删除数据，并且已使用了手机自带的“恢复出厂设置”功能的手机，恢复出它原有的数据。而且还有商家在专门从事这种“生意”。

近日，网上流传二手手机经技术手段可恢复出原有数据的新闻，引发公众对于二手手机回收导致信息泄露的新焦虑。

那么，将手机恢复出厂设置，删除相关内容和软件后，出售自己的旧手机到底靠谱吗？

“传统的电脑和如今的智能手机，信息存储的原理和规则基本一致，简单的恢复出厂设置和删除文件，并不代表彻底删除了信息。”网络安全专家、奇安信行业安全研究中心主任裴智勇表示，手机上“删除”文件，其实系统只是将该文件的指示路径删除，等于一般人找不到该文件了，然而实质的内容信息依然存储于手机内部。

“所以，想恢复手机之前的存储内容信息，是可以做到的，而且技术门槛不高。”裴智勇坦言，目前在一些不正规的二手手机回收店，有人会通过这种方式，来恢复手机里的储存信息，比如手机通讯录、短信等涉及个人信息的内容，再将其进行二次售卖，赚取暴利。

业内专家认为，当前，二手手机已成为个人信息泄露的源头之一，形成了一条成熟的灰色产业链条，从中获取的个人信息，可能会被用于垃圾电话、短信乃至电信诈骗。

旧手机如何处理成为“手机族”新困扰

“手机更换越来越频繁，我家里已有7、8台旧手机，几年了不知道该怎么处理，只能放着。”北京市民小王说，除了手机她还有几台旧笔记本电脑和台式电脑放在家里，很占地方。

工业和信息化部公布数据显示，2021年1至2月，我国手机产量达2.1亿台，同比增长49.2%，其中智能手机产量达1.4亿台，同比增长48.8%。

“我国是智能手机使用大国，每年生产和淘汰的手机数量庞大。”电信专家付亮预测，二手手机规模将有望持续提升。

随着智能手机和网络的快速发展，与小王类似的情况将越发普遍，有的消费者家里甚至已有几十台旧手机，大部分人不太知道应该如何回收和妥善处理，只能把旧手机、旧智能产品放在家里“吃灰”。

“不卖觉得可惜，卖了又会担心。”“放在家里不但占地方，也发挥不了手机残值。”“半旧手机也能卖个好价钱，但又担心个人信息被泄露。”网友在网络里的留言代表了不少消费者的心声。

伴随旧手机数量的持续增长，街上、商场里消费者不时能看到“高价回收手机”等标语和回收店铺。但大部分消费者对于手机回收、二手手机售卖行业并不熟悉，对于曾经贴身使用过的旧手机进行回收，公众普遍会有担忧是否会导致自己重要的个人信息、隐私泄露等潜在风险。

处理旧手机的正确打开方式来了

“一般，临近更换手机时，人们普遍会注意在旧手机上减少关键信息的使用和存储，旧手机上信息的价值随着时间开始衰减。”付亮表示，部分APP应用、与支付相关的身份等信息，即使被别人恢复，直接造成移动支付危害的几率也比较低。

据付亮介绍，金融机构的APP、移动支付等智能应用软件，版本升级迭代速度相对较快，二手手机中恢复的用户相关信息，很难再应用到新版本的支付功能中去。但比如隐私照片，尤其是身份证等重要证件照片数据如果被恢复出来，隐患就比较大了。

过时电子产品回收再利用是大势所趋。那么问题来了，我们如何才能在保障信息安全的前提下出售、回收自己的旧手机？

裴智勇建议，首先旧手机出售尽量到大平台、大型店里进行，尽量避免通过个人渠道或小店。其次，旧手机换下来后，不要着急出售，出售前除了恢复出厂设置、删除老旧文件外，可以选择下载“文件粉碎”类软件，对淘汰手机、电脑进行重复覆盖、复写处理。

“用户可将手机连接至电脑，先将手机内容全部删除，再向手机内写入新的大型文件，反复进行几遍，尽量将其空间占满。”裴智勇说，这样基本就可以保证旧手机内的个人信息和痕迹被彻底清除。

专家建议，手机上尽量不保存敏感、秘密信息，重要信息保存使用后应尽快删除掉，其后经过多次数据覆盖，数据被恢复的几率也将大大降低。

付亮认为，当前从世界环保和资源再利用等角度出发，以智能手机、电脑等为代表的二手电子产品回收行业发展势在必行。相关部门应提早研究举措和法规，为相关的回收产业提供助力，让回收渠道更透明，回收方式更科学、精准，以推动行业健康有序发展。

“明确回收者专业资质认定标准，出台更加详细的法规和举措，我们消费者才能对不明身份的回收者说‘不’。”裴智勇表示，在立法和制定规范时，应将二手手机个人信息泄露列入信息保护的整体范畴中，统一规划部署举措为提高个人信息安全保护力度添砖加瓦。

新华社北京4月14日电

一个App控制全球18万个网络摄像头

会员付费可偷窥隐私“直播”

新华社记者鲁畅、吴文诩

不法分子利用黑客技术轻易破解并控制家用及公共场所摄像头，搭建App或利用其他视频管理平台向客户收取“会员费”“套餐费”牟利，无数隐私画面通过“第三只眼”被窥探无余…… 4·15全民国家安全教育日前夕，记者调查发现，在相关部门加大对网络摄像头隐私泄露黑灰产打击力度的同时，仍有不法分子采用隐蔽的方法出售破解摄像头ID及破解软件，且价格“水涨船高”，对公民隐私安全带来巨大的威胁和隐患。

还在卖——隐私监控黑灰产仍存“隐秘角落”

记者日前调查发现，在部分社交软件中，不法分子通过较为隐蔽的方式出售已经被破解的摄像头ID和破解软件。例如，在QQ上，他们以“摄像头”为用户名吸引客户，在客户添加好友时，会收到提醒，需添加另一个名为“客服”的QQ号才能通过。

简单咨询后，这名客服人员列出“价目表”。其中，包括168元、238元的“家庭套餐”以及收费更高的“酒店套餐”和大学附近酒店，破解摄像头ID数量在12个至15个之间。当记者询问是否用某App（可公开下载的网络监控系统）进行绑定观看时，对方表示，现在不能用了，需换成另一款远程监控系统。此外，该客服列出的价目表中还包括摄像头破解软件，可扫描破解附近摄像头，价格为520元。记者注意到，随着相关部门和网络平台加强该黑灰产业的防范打击，这些违法资源价格也有所上涨。去年同期，存在大量以“摄像头”为关键词的QQ群组，目前已无法检索到。此外，破解软件的价格上涨了200元，破解ID的单价也上涨了近一倍。

这些破解ID是否真能对公民隐私实时监控？在客服人员展示的某App中，包括大量未解锁的隐私摄像头监控截图，他表示，通过付费绑定后，客户就可以在手机端观看。这些摄像头大部分对准的是卧室或客厅，部分清晰度较高。记者注意到，该App上还有大量通过其他渠道充值注册的人员。

记者采访发现，在执法部门查处的案件中，犯罪分子正是利用了客户偷窥心理非法牟利。在北京市第三中级人民法院日前审结的一起案件中，被告人巫某某控制了全球18万个摄像头。“我收藏或录制的都是一些私人住宅里人体裸露的视频。”一名巫某某的“客户”李某证言称，他注册这个App的会员后，分两次支付668元成为终身会员。“观看不限时间，随机出现6个镜头内容，可以收藏、录制，内容有私人住宅、公共场所、培训机构等。”

门槛低——为违法犯罪大开“方便之门”

记者调查发现，目前，摄像头隐私泄露黑灰产的门槛非常低，一些不法分子甚至不需要拥有较高的计算机水平，只需要买到“傻瓜操作”的黑客软件或付费寻找技术人员帮助，就可获取大量破解的摄像头ID。

上述案件的承办法官告诉记者，巫某某就是从网上购买了一款“反编译软件”，并非法获取了某品牌网络摄像头的用户数据库，在这个数据库的基础上搭建了名为“上帝之眼”的App，后又重新经营名为“蓝眼睛”的App，数据从“上帝之眼”导入，服务器挂在境外。再通过吸引用户有偿登录应用程序，观看网络摄像头实时监控内容。

记者了解到，巫某某搭建App是通过社交软件花钱寻求技术人员帮助实现，而该人员明知巫某某的非法用途，仍然为其搭建。巫某某说：“我把建网站的要求告诉他，对方负责做好，当时收了我1000元钱。这个人是知道我的网站内容是做什么的，而且网站上面的内容很明显就是推广摄像头。”

就这样，从2018年至2019年3月5日案发被抓获，巫某某通过在网络推广上述摄像头实时监控画面非法获利人民币70余万元。即使在被抓获后的2019年3月5日至3月26日期间，其专门用于收取贩卖监控实时画面钱款的第三方支付平台仍收款人民币17万余元。最终，巫某某犯非法控制计算机信息系统罪，被判处有期徒刑5年，罚金人民币10万元，并追缴违法所得。

据了解，目前，类似隐私摄像头破解等以黑客类犯罪为前端的涉网犯罪，产业化特征明显。该案一审法官、朝阳法院法官王杨说，当前网络犯罪已成产业化，如果某些不法分子想从事网络黑灰产，他所做的只是在一些网站上发布需求信息，就会有散落在各地的人提供包括黑客破解、“黑网站”架设、推广引流乃至客服人员等，每一个步骤都有人去实施。

齐动手——重拳打击，构建立体防御体系

根据百度去年发布的《2020网络黑灰产犯罪研究报告》，网络犯罪将会是未来十年全球显著的风险之一，同时黑灰产犯罪即将进入AI时代，AI安全也将成为各行各业不容忽视的关键问题。

报告建议，通过司法与行政部门联动、政府与企业共治共享、强化黑灰产宣传教育的方式，积极灵活地发挥社会各主体的优势力量，群策群力，共同重拳打击网络犯罪黑灰产生态，真正做到源头治理，维护网络社会秩序。

北京师范大学刑法所副所长彭新林认为，各部门应联合行动，加大对利用物联网设备犯罪行为的打击力度，在鼓励创新发展的同时加强行业监督和指导。网民也要增强安全意识，强化安全防护措施，发现黑客违法犯罪线索后要及时举报。

受访人士同时指出，企业要重视办公环境网络安全，定期检查摄像头等设备，建立网络安全防护体系，同时要重视对员工的网络安全培训，并在设备生命周期内做好软件、系统的漏洞修复、安全更新等运维工作。此外，网民对网络社交平台的账号、密码尽量采取分类管理，针对各个平台使用不同的密码，且尽量使用高强度的密码，还要经常性地更新重要网络平台的密码。

新华社北京4月13日电