Open Journal of Legal Science 法学, 2023, 11(6), 5884-5890
Published Online November 2023 in Hans. https://www.hanspub.org/journal/ojls
https://doi.org/10.12677/ojls.2023.116843

Hans汉斯

电子病历引发的个人信息保护研究

向　阳

武汉工程大学法商学院，湖北　武汉

收稿日期：2023年7月31日；录用日期：2023年8月15日；发布日期：2023年11月22日

摘　要

数字技术已经彻底改变了我们的世界，智能手机、平板电脑和支持网络的设备已经改变了我们的日常生活和沟通方式。由电子健康记录(EHR)创建的数字医疗基础架构中的信息流更大，更无缝，涵盖并利用了数字技术进步，可以改变医疗提供和补偿的方式。但同时，病历电子化也给患者医疗信息的保护带来了全新的法律挑战。加之我国存在患者医疗信息保护意识较为薄弱，立法体系不完善等问题，患者医疗信息随时面临大量的威胁。在这样的背景下，对于患者医疗信息的保护刻不容缓。

关键词

电子病历，个人信息，法律保护

Study on the Protection of Personal Information Arising from Electronic Medical Records

Yang Xiang

School of Law and Economics, Wuhan Institute of Technology, Wuhan Hubei

Received: Jul. 31st, 2023; accepted: Aug. 15th, 2023; published: Nov. 22nd, 2023

Abstract

Digital technology has revolutionized our world. Smart phones, tablets and web-enabled devices have changed our daily lives and the way we communicate. Medicine is an information-rich enterprise. The flow of information in the digital healthcare infrastructure created by electronic health records (EHRs) is larger and more seamless, encompassing and leveraging digital advances that can transform the way healthcare is delivered and reimbursed. But at the same time, the electronicization of medical records also presents a whole new legal challenge to the protection of patient

文章引用: 向阳. 电子病历引发的个人信息保护研究[J]. 法学, 2023, 11(6): 5884-5890.
DOI: 10.12677/ojls.2023.116843

medical information. Coupled with the relatively weak awareness of patient medical information protection and an imperfect legislative system in China, patient medical information faces a large number of threats at any time. In this context, the protection of patients' medical information can not be delayed.

Keywords

Electronic Medical Records, Personal Information, Legal Protection

1. 电子病历的界定

1.1. 电子病历的含义

电子病历是随着医院计算机管理网络化、信息存储介质——光盘和 IC 卡等的应用及 Internet 的全球化而产生的。电子病历是信息技术和网络技术在医疗领域的必然产物，是医院病历现代化管理的必然趋势，其在临床的初步应用，极大地提高了医院的工作效率和医疗质量。电子病历也叫计算机化的病案系统或称基于计算机的病人记录，它是用电子设备(计算机、健康卡等)保存、管理、传输和重现的数字化的病人的医疗记录，取代手写纸张病历。它的内容包括纸张病历的所有信息。电子病历是医疗机构对门诊、住院患者(或保健对象)临床诊疗和指导干预的、数字化的医疗服务工作记录，是用电子设备(计算机、健康卡等)保存、管理、传输和重现的数字化的病人医疗记录，取代手写纸张病历，具有主动性、完整和正确、知识关联、及时获取等特征。

1.2. 电子医疗的法律属性

电子医疗信息兼具人格属性和财产属性。一方面来说，法律保护电子医疗信息的目的，主要因为这些信息中包含了病人的人格利益，法律主要是对人格利益的保护。电子医疗信息中蕴含着广泛的人格利益，所侵犯的人格利益也有多种表现形式。另一方面，人身权是人格权中至关重要的一部分，在高速发展的时代，似乎所有的东西都被明码标价，当然人格权也不例外。由于个人信息有潜在的巨大经济价值，并且呈现不断增长的趋势。个人将自己的电子医疗信息提供给某些信息需求者，以期得到信息需求者的服务，例如，百度浏览器中的线上问诊，要想使用该功能，就必须同意该软件收集自己的电子医疗信息，百度浏览器通过向使用者提供具有价值的问诊服务，从而获得患者的电子医疗信息。另外，个人还可以决定将自己的电子医疗信息授权给医疗机构以收集、教学、科研之用，或者将个人的电子医疗信息作为可交换的商品转让给个人医疗信息需求者使用。当然，不少法学家已经意识到该过程中可能带有风险和隐患。但无可否认的是，在当今社会，个人电子医疗信息有潜在的巨大经济价值[1]。

电子病历是具有法律证明力的医疗文书。包括两个涵义：其一，电子病历是一种医疗文书。医疗文书，是指取得执业资格的医务人员在诊疗、护理、预防等工作中，依照有关的法律法规和行业技术规范，记载并制作反映人体生理病历状况与各类形式证明文件的总称。它不仅指纸质记录，而是包括了文字、符号、图形、视听资料等在内的全方位的医疗材料和健康信息。根据前面概念分析，电子病历是一种更高级的医疗记录形式，包括了常规病历所有的功能，当然属于医疗文书。其二，电子病历具有证明力，

可以作为证据使用。卫生部《全国医院工作条例》第 23 条规定：“病历是医疗、教学和科研的重要资料，也是法律的依据。”所以病历不仅是医疗文书，还是法律上的证据。电子病历作为医疗文书的另一种表现形式，当然能够成为法定的证据种类。

2. 电子医疗信息保护面临的问题

2.1. 缺少专门的立法

我国医疗领域患者信息保护法律法规的立法滞后性较为严重，现有的法律法规也存在效力不足的问题。尽管我国已经颁布了一些法律法规来规范电子医疗记录的个人信息，例如《电子病历应用管理规范(试行)》第 13 条强调要对患者进行唯一身份标识，保护患者的各项权益。《医疗机构、医师、护士电子化注册管理规范(试行)》第 21 条指出要加强对电子化注册过程中，采集、利用和存储敏感数据各环节的安全管理，第 22 条指出根据“谁提供、谁负责”的原则，应由数据提供者确保信息的真实、准确和安全。其中不乏明确要求，在实施诊疗的过程中，医务人员需要保护患者的隐私，但这些规定都缺少明确的指引，可操作性不强。从目前的情况来看，急需制作一个专门的电子医疗记录的法律体系，否则，将不能应对患者电子医疗信息保护中存在的问题，难以平衡患者、医疗机构、互联网医疗平台和政府等的利益，不利于电子医疗产业的发展。

2.2. 缺少健全的司法保护

在实践中，患者隐私权遭受侵犯的情况具有复杂性，我国对于患者电子医疗信息的保护目前还不够完善和全面。当前法律已经明确的规定了要保护患者的个人信息，但是很多类似的受害人往往由于无法提供证据证明被告方具有泄露信息的行为而败诉，原告方的举证责任过重。《民法典》规定，我国的医疗损害责任采取过错责任原则，但是也有例外，如果情况符合第 1222 条规定，举证责任可采取过错推定原则。而在司法实践中，大多数时候的举证是需要原告完成的，而原告作为医患关系中的患者一方，本就处于比较弱势的地位，承担了过重的举证责任，往往因为无法取得有利于自己的证据而败诉，显然，这不合理[2]。

此外，判决思维的僵化，造成知情同意原则成为被告的避风港。知情同意延伸到患者个人信息领域，表现为患者对其本人信息的控制和知情的权利，要求在对个人信息进行收集、处理前告知信息主体所收集信息的种类、目的以及处理方式，核心就是在于充分的尊重信息主体的意愿。基于告知同意最大的挑战就是其实施可能流于形式，导致“无限授权”，但这一规则对于个人信息的保护又是如此重要，以致不能轻言放弃，只能缓解。电子病历在共享过程中，授权是前提条件，而知情同意又是患者做出是否授权的关键环节。知情同意权是患者最基本的一项权利，贯穿于诊疗活动的始终，包含两个方面“知悉”和“同意”。知情同意首要意义在于“知”，医疗机构只有明确具体的告知收集的信息以何种方式用于何种目的，患者才会同意，才能放心的将自己的信息尤其是敏感信息告知给医疗机构。“知”除了被动地知晓之外，也包含积极主动的行使权利，《民法典》第 1037 条和 1225 条规定了患者作为信息主体所享受的权利，即患者可以复制查阅病历资料，当发现医疗机构收集的个人信息出现错误时，有权申请更正。然而在具体实践中由于没有专门的知情同意书，通常是作为某一项条款置于医疗合同中，医患双方大多不会签订正式的知情同意书，而是采取推定同意，至于同意的范围多是模糊处理，一笔带过。这将成为被告在庭审中抗辩的有利证据，极大打击了原告维权的信心[3]。

2.3. 缺少完整的监管程序

当患者医疗信息受到侵害时，除去诉讼程序外，可以对非法泄露、利用医疗信息的医疗机构进行投

诉。但《医疗机构管理条例实施细则》第 68 条中只规定了医疗机构监督管理办公室可以受理患者的投诉，但涉及对侵害医疗信息行为进行投诉的具体流程及细则不明。病历电子化环境下对侵害患者医疗信息的行为进行救济的渠道狭窄。尽管《电子病历应用管理规范(试行)》第 5 条对电子病历应用监督管理工作的行政主体作出了规定。但一方面，该规定法律效力层级较低，应提升对于患者医疗信息监管制度设计的相关规定的法律位阶。另一方面，该规定并不专门针对对于患者医疗信息的保护。可以说，我国依然没有设置专门对医疗信息流通、利用行为进行监管的机构，在监管机构设置及相应权限设置上依然不明确。行政执法部门的定位及权限的不明确为病历电子化环境下患者医疗信息的保护增加了难度。并且从机关内部的监管来说，卫生行政部门对自身信息利用行为的内部监管不足，缺乏相应的法律规定对其行为进行约束及制约，极易导致权力寻租等现象的发生[4]。

3. 域外立法

3.1. 欧盟

欧盟的个人信息保护的理论基础是从人的基本权利保护延伸出的数据控制理论，秉持“人权保护”的理念和宗旨，奉行“保障个人人权”的价值取向，通过立法加强对个人信息的保护。欧盟对个人信息的保护非常严格，采用了统一立法的模式，如 1981 年的《第 108 号公约》、1995 年的《个人数据保护指令》。同时，欧盟还顺应时代的发展要求，出台了新的法律法规——《通用数据保护条例》，进一步完善了个人信息保护的机制。为了更好实现保障人权，立法机关根据个人信息的敏感度高低进行分类，并在法律条文中明确列举[5]。

3.2. 美国

美国的个人信息保护理论是基于个人自由保护的隐私自治理论，其对个人信息保护的立法较宽松，倡导各行业自律，保障公民的民主自由，注重对个人信息的利用，重视商业利益和价值。自由的价值观导致美国并没有采取统一立法的模式，而是将权力下放到地方各州、各个行业，由其自主制定个人信息保护政策。美国采用“场景衡量”的方式，综合判断个人信息的具体类型。

为加强对个人医疗和个人健康信息的保护，1996 年美国国会颁布了《健康保险责任法案》。该法案确立了美国保护个人健康信息的法律框架。该法案涉及多个方面，如有关于卫生信息化过程中的交换规则，数据交换的标准规格，医疗机构、从业人员的识别规则，医疗数据安全、医疗隐私、患者识别规则等，其中医疗数据的机密性和安全性对于患者权益的保护具有重要意义。

3.3. 评价与选择

我国可借鉴欧洲对患者电子医疗信息的保护模式，其优点在于：一是当某一行为还没有达到影响个人独处和生活安宁的程度时，患者可以通过信息权对他们的个人电子医疗信息进行保护。二是“个人的电子医疗信息同时具有人格属性和财产属性”，其保护范围更为宽泛。

4. 病历电子化环境下患者医疗信息法律保护的完善

4.1. 立法路径——确立原则和建立制度

法律原则是指法律的基础性真理、原理或为其他法的要素提供基础或本源的综合性原理或出发点。其基本原则具有基础性、统率性和概括性的特点，根据电子病历中信息处理的实践经验，本人主张，电子病历中信息处理原则应当有目的限定原则、知情同意原则、区分对待原则。

目的限定原则要求医疗机构在收集患者信息时，应该首先明确其目的，不能用在最初收集的目的之

外的地方，旨在限制信息管理者和处理者的行为。并且医疗机构在收集、查看患者的个人信息时，要依据之前的目的限定原则，遵循适当必要性，不能为达到目的而扩大收集的信息范围。然而，个人信息利用的目的往往难以在收集之初就被完全估计，传统目的限定原则已经不适用现今大数据时代。以场景为导向的理论被广泛推崇，“场景”一词源于尼森鲍姆的“情景脉络完整性”理论，指个人信息原始收集时的具体语境应得到尊重，其后续传播及利用不得超出原初的情景脉络。欧盟的《通用数据保护条例》在传统的目的限制原则上增加了场景理论，要求在判断是否符合原始数据收集目的时应该考虑一些因素，如：二次利用的目的与原始目的的关系，数据主体和数据控制者的合理期待，数据处理的安全保障等。其突出特点就是将利益衡量细化到具体场景中，它从用户的接受度出发，而并非僵化审视与原始目的的“符合性”，脱离场景的抽象式预判往往导致过度保护，总的来说，场景理念是对目的限定原则的超越与升华。对于个人医疗信息的利用和患者的生命健康相关联，因此，在利用时有突破传统目的限定原则的客观需要，要为发生危及患者生命健康的紧急情况设定例外条款，还要关注到患者信息对于科学研究以及公共安全的意义，对于科学研究来说，医院不可能在每项研究之前都一一通知患者这个信息主体，操作困难，所以要坚持匿名化的原则。当然，绝对的匿名化是做不到的，经过深层次挖掘都是可复原的，可以结合法律规制来拒绝个人信息被匿名化后再次识别出来[6]。

制定严格的分类制度。电子医疗信息包括了病人的一般信息、诊断信息、生理信息、经济信息等，这些信息并非全部属于个人信息或敏感信息，如果不加以区别保护，在实际操作中就很难使用，病人信息也无法充分利用。《人口健康信息管理办法(试行)》提出要实行分类管理和分级存储，因此，要按照电子医疗信息的不同类别，采取相应的防护措施。一般信息、经济信息、某些生理信息和诊疗信息可以在去识别化后在一定范围内使用；当涉及一些遗传信息或者传染病史等，未经授权披露会对患者造成较高的损害，就仅限于参与诊疗活动的人员访问；尤其是涉及基因信息时，需要受到严格的限制，参与诊疗的医务人员也要严加管控。

从个人信息立法模式上可将各国和地区分为两种：以美国为代表的分散式行业自律立法和以德国、英国及多数欧洲国家采用的统一交叉立法。美国的保护模式较为复杂，可以称之为分散立法和行业自律相结合的保护模式。而德国、英国等国家规定了统一的个人信息保护法，适应于各自领域的不同种类的资料保护，并设有专门的个人信息保护机关，负责个人信息保护事宜。显然我国借鉴了德国的立法模式，制定并颁布统一的个人信息保护法。在欧盟《个人数据保护指令》中，允许各成员国就特殊领域的个人信息保护制定专门的法律规范，这些领域包括新闻媒体领域、文学艺术领域、医疗卫生领域、科学研究领域等。这一点也是值得我国借鉴的，总的来说，由于以信息处理为核心的行业本身的情况千差万别，指望以一部法律解决所有行业和领域的个人信息保护问题是不现实的，因此针对各种行业的不同情况制定特别规范是必要的。医疗行业领域有其自身鲜明的特点，应当由国务院专项立法《电子病历管理条例》，该条例不仅仅涉及对个人医疗信息的保护，更重要的是全面构建电子病历的相关制度，包括电子病历的制作、签名、保管、流通、使用等等。

4.2. 司法路径——强调个人权利本位

医疗机构及其工作人员侵犯了患者的隐私权，应当追究患者的法律责任，并且按照过错归责原则，只有在特定的情况下，才会采取过错推定原则，具体内容包括违反法律法规、隐瞒或者不提供病历及相关资料、伪造或者篡改病历资料。尽管在法律上，这三种情形都是通过过错推定来确定的，但是在实际生活中，这三个严重情形经常会出现，也就是说，对于除了这三种情形以外的所有情形，都可以适用过错归责原则，这是不合适的。第一，法律要求医院承担的职责就是认真的保管好电子病历信息，医院方需主动履行义务，在发生法律纠纷时，医院方需提供证据证明自己已经履行应尽义务。第二，如果医方无法证明自己尽到应

尽义务，那么根据过错推定原则，可以推定医方存在过错。第三，随着互联网社会的快速发展，医学信息学科的地位仍然处于一个被动的状态。因此，规定医院侵害个人电子医疗信息的侵权责任时采用过错责任推定原则，这样才更加科学合理。患者只要能证明医院方没有尽到自身义务即可，医院方则需要举证证明己方已尽到了安全保存患者电子医疗信息的义务，这样对于侵权认定会更加合理和公平，也会在无形中监督医院方合理保存患者的个人医疗信息，减少医疗信息泄露事件的发生[7]。

建立最低限度的利用原则。在利用和披露病人电子病历信息时，我们可以参考美国在对病人电子病历信息进行保护方面所制定的最低限度利用原则。考虑使用的必要性，披露和最低侵犯的可能性。在医患关系中，对医患关系的维护与公共知情权和第三人知情权之间的利益冲突，应建立最低使用原则，以达到调和这一冲突的目的。根据这一原则，公众知情权的满足，应该通过细化的、有针对性的发表来实现。比如，在卫生部门收集公共卫生健康数据的时候，应该明确指出所收集的信息的目的，并考虑要不要对患者信息进行去识别化。另外，卫生部门还保证加密保存患者医疗信息，以求满足最低限度的利用原则，将对患者医疗信息的侵害控制在最低限度[8]。

4.3. 构建患者医疗信息保护渠道机制

要使法律发挥效力，就必须有健全的监管机制来配合。一方面，在信息化建设中，医疗机构的档案部门应该与电子病历的发展同步，重视对医疗机构内部病人的医疗信息的保护，并对其进行安全保护方面的专门培训，通过对医护人员账户的使用情况、电子病历的保存情况、信息的内部流动情况以及建立安全保护的自我评价机制等方式，来实现内部保护。另一方面，既然卫生部门也参与了病人医疗信息的数据平台的构建，那么就应该制定相应的行政法规来规范和限制各级卫生部门收集、曝光和处理病人医疗信息的行为。

病历电子化对病人健康信息的侵犯具有大规模、广泛性和低成本等特点，对病人健康信息的保护具有重大的意义。笔者认为，通过对病人的健康状况进行评估，可以对病人的健康状况进行评估，并对病人的健康状况进行评估。这既是对风险经济理论的应然，又是对“健康中国”战略实施的实际要求。在损失分散理念的指导下，可以对病人的医疗信息损失保险进行进一步的完善。在损害分散思维下，对侵权损害的社会化分散通常是通过损害行为企业或机构的内部消化，再表现在服务价格函数上，或是借助责任保险制度，将其分散出去，以求在侵害人不至因为赔偿损失而导致破产的情况下，让被侵害人得到救济。具体而言，可以在医疗责任强制保险中增加关于侵害患者医疗信息的相关条文，亦可以设立网络信息隐私保护责任险，在该险种中草拟侵害患者医疗信息的规定，以保护患者医疗信息[9]。

我国 2012 年修改后的《民事诉讼法》对此作出了明确的规定，对维护消费者权益和保护环境起到了积极的促进作用。但是，该制度仅局限于对这两种侵权行为的救济，很明显，在很多涉及公众利益的情况下，该制度无法适用。笔者以为，在保障病人健康权益方面，可以引进公益诉讼来保障病人健康权益，从而建立病人健康权益保障的通道机制。在电子病历中，因其对病人健康信息的价值挖掘特性，使病人个人难以得到有效的保障。首先面临的就是信息价值的确定问题。虽然个人信息具有财产性，但单条的个人信息的价值往往十分有限。侵害人往往是通过大规模地利用、分析患者隐私数据才能挖掘出数据背后隐藏的价值。在这样的情况下，分散的个体需要一个公益的组织代为寻求法律帮助与救济。这些特点与环境保护、消费者权益保护实施公益诉讼制度的原因有一定相似性。所以，在患者医疗信息保护的问题上引入公益诉讼制度，利于患者医疗信息的保护。

5. 结论

我国电子病历共享工程处于起步阶段，电子病历中的个人信息面临的安全问题比较多，在处理电子

病历中的个人信息时，要遵循以下基本原则：目的限定原则要求运用以场景为导向的理论，将利益衡量细化到具体场景中；知情同意原则要求在对患者信息进行收集、处理前，告知信息主体所收集信息的种类、目的以及处理方式，充分尊重患者的意愿；区分对待原则要求对电子病历中患者的一般信息、诊疗信息、经济信息等，分类管理分级存储，采取不同的保护方式，把基本原则贯穿于处理电子病历信息的始终。还要明确患者、医疗机构和政府间的义务关系，患者有如实告知的义务，医疗机构有为患者保密、明确告知患者共享个人信息的目的、方式、风险以及安全管理电子病历的义务，政府也有相应的监管责任。

参考文献

[1] 彭诚信, 史晓宇. 论个人信息财产价值外化路径的重构[J]. 当代法学, 2023, 37(2): 62-74.

[2] 彭飞荣. 《个人信息保护法》第 13 条第 1 款第 2 项(合同中个人信息处理)评注[J]. 法治研究, 2023(3): 132-147.

[3] 龙卫球. 论个人信息主体基础法益的设定与实现——基于“个人信息处理规则”反射利益的视角[J]. 比较法研究, 2023(2): 152-171.

[4] 姬雨童, 李筱永. 电子病历共享中个人信息安全的法律保护研究[J]. 中国卫生法制, 2023, 31(2): 1-5.

[5] 邓灵斌. 欧盟、美国敏感个人信息保护法律规制比较研究及我国立法特色分析[J]. 图书馆, 2023(3): 67-73.

[6] 吴国喆, 王文文. 数据共享视域下个人信息“合理使用”的场景化判定[J]. 西安交通大学学报(社会科学版), 2023, 43(3): 142-156.

[7] 钱继磊. 何以个人信息权为新兴(型)人权——人工智能与大数据新时代背景下的思考[J]. 北方法学, 2023, 17(2): 5-14.

[8] 王鹏鹏. 论敏感个人信息的侵权保护[J]. 华中科技大学学报(社会科学版), 2023, 37(2): 41-51.

[9] 彭诚信, 史晓宇. 论个人信息财产价值外化路径的重构[J]. 当代法学, 2023, 37(2): 62-74.