依法治国研究

HIPAA 法案健康信息隐私保护借鉴研究*

蔡宏伟 龚赛红

【提 要】我国现有立法对于患者隐私权法律保护的规定还需要进一步完善。美国 HIPAA 法案隐私规则对于患者健康信息隐私保护的规定具体、具有可操作性、立法体系性强，值得我国患者隐私权保护立法借鉴。在立法中应明确立法法理基础；明确健康信息隐私侵权主体；明确细化规定，增强可执行性；应注意平衡个人健康信息保护和社会利益；赋予个人更多有关个人健康信息相关的自主权利。

【关键词】患者隐私权 HIPAA 社会利益 自主权利
〔中图分类号〕D913〔文献标识码〕A〔文章编号〕1000－2952（2017）05－0114－08

引 言

健康信息隐私是患者隐私的重要组成部分，我国已有关于患者隐私权法律保护的相关规定，但还需进一步完善。虽然中美两国处于不同法系，立法传统和立法技术不尽相同，但保护健康信息隐私的出发点和目的都是相同的。《健康保险携带和责任法案》（Health Insurance Portability and Accountability Act，简称 HIPAA 法案）[①]的隐私规则作为美国健康信息隐私保护的基本法律，对于健康信息隐私的保护规定具体、详细、具有可操作性、立法体系性强，值得我国患者隐私权保护立法借鉴。

一、美国健康信息隐私保护的立法基础

美国对于隐私权的承认和保护较早，始于 1898 年沃伦和布兰蒂斯的论文《论隐私权》，只不过当时的隐私权指的是“独处的权利”，后来经过普洛瑟教授和其他大法官的解释，隐私权成了一项保护范围很广的权利。美国法并无人格权的概念和体系，但隐私权却具有大致相同的功用。[②]在美国模式下，个人信息被置于隐私的范畴而加以保护。[③]美国法是在普通法及宪法上以个案发展出对隐私保护的标准，对隐私采广义的解释，包括个人自主决定和信息隐私二个类型，其范围扩张并及于堕胎、死亡权利

* 基金项目：2016 年国家社科基金项目《患者隐私权法律保护研究》（16BFX121）的阶段性研究成果。

① http://www.legalarchiver.org/hipaa.htm，2016 年 11 月 1 日。下引该法案条文不再一一标出出处。

② 参见高圣平：《比较法视野下人格权的发展——以美国隐私权为例》，《法商研究》2012 年第 1 期。

③ 参见王利明：《论个人信息权的法律保护—以个人信息权与隐私权的界分为中心》，《现代法学》2013 年第 4 期。

等。[①] 因此，在美国立法中，健康信息作为隐私进行保护没有法理障碍。实践中，健康信息隐私被泄露的情况也要求对于健康信息隐私进行保护、合理使用和公开。2009 年以来，美国共有 489 家 HIPAA 管辖机构报告了大规模信息泄漏事件。2011 年 9 月 14 日，TRICARE 管理集团健康信息泄露案中，受影响人数多达 4，901，432 人，集体诉讼要求赔款 49 亿美元。[②]

二、美国健康信息隐私保护立法现状

在国际上，隐私法律保护模式主要有两种：一是以欧盟为代表的统一保护模式，不区分行业，对个人隐秘信息予以统一的保护；二是以美国为代表的分类保护模式，基于各行业的特点、保护目的、保护手段等，分别给予不同的保护。[③]

美国的医疗保障主要包括两大类：第一类是国家健康保险，主要由政府承办，主要包括医疗照顾（Medicare，也称为老年医疗保险）、医疗救助制度（Medicaid）和儿童健康保险计划（State children' s Health Insurance Program）；第二类是私人医疗保险，主要由私人或社会组织承办，可分为非营利性和营利性两种。私人医疗保险是自愿的，主要是由雇主提供的商业保险，也有一部分人群从社会组织或保险供应商直接购买医疗保险。[④] 美国雇主型医疗保险处于主体地位，大部分的美国民众通过雇主型医疗保险给付昂贵的医疗费用。[⑤] 可见，美国个人健康信息隐私被保险机构、雇主所掌握，健康信息直接影响健康保险的承保、连续性和转移，保险机构和雇主很可能对个人健康信息隐私造成威胁。

1996 年 8 月，为了提高团体和个人保险中健康保险的可携带性和连续性，打击健康保险和卫生保健服务中的浪费、欺诈、滥用行为，促进医疗储蓄账户的使用，提高长期保健服务及保险的使用，简化健康保险管理，[⑥] 以及建立保护个人健康信息国家标准，[⑦] 克林顿政府制定和颁布了《健康保险携带和责任法案》。与此同时，国会也认识到卫生保健产业日益增长的复杂性，以及健康信息系统技术和通讯的进步对健康信息保密带来的诸多挑战。因此，HIPAA 法案管理简化条款（Administration Simplification）规定：如国会不能在 1999 年 8 月 21 日前颁布卫生保健隐私立法，则由美国卫生和公共服务部（Department of Health and Human Services，简称卫生部）颁布个人可识别性健康信息隐私标准。HIPAA 法案也要求卫生部向国会提供卫生保健信息秘密保护的立法建议。卫生部于 1997 年 9 月 11 日向国会提交了立法建议，但是国会未能在自己设定的最后期限通过该法案。经过多次修改，最终的隐私规则于 2002 年 10 月 15 日生效，完善了 1996 年 HIPAA 法案中对隐私保护的规定。隐私规则修改的目的是：澄清隐私规则条款的实质，解决隐私规则在卫生保健质量或卫生保健适用中无意的负面影响，减轻隐私规则产生的无意的管理负担，进而为个人可识别性健康信息隐私提供强有力的保护。作为美国最彻底的医疗保健立法，HIPAA 法案中的管理简化部分条款的修改和内容的增加最为频繁，其中的修改和增删包括了隐私规则。为了和科技进步同步，尤其是随着电子邮件和其他形式的电子交流方式的使用，以及电子健康记录的广泛采用，HIPAA 法案在 1996 年通过后进行了多次修改。[⑧] 2009

---

① 参见王泽鉴：《人格权的具体化及其保护范围·隐私权篇（上）》，《比较法研究》2008 年第 6 期。

② 参见 Erin McCann："美国 HIPAA 信息泄漏十大事件"，王连美译，http：//news. hc3i. cn/art/201210/21482. htm，2016 年 11 月 1 日。

③ 参见党玺：《欧洲与美国隐私保护法律冲突的解决路径》，《中国社会科学院研究生院学报》2015 年第 1 期。

④ 参见陈蒙蒙：《美国社会保障制度研究》，江苏人民出版社 2008 年版，第 161 页。

⑤ 参见李国炜、丁春艳：《信息科技语境下的个人健康信息立法保护——以 Iv. Finland 案和 HIPAA 为切入点》，《中国卫生法制》2012 年第 5 期。

⑥ 参见 Health Insurance Portability and Accountability Act of 1996，http：//www. legalarchiver. org/hipaa. htm，2016 年 11 月 1 日。

⑦ 参见 http：//what－when－how. com/privacy/health－insurance－portability－and－accountability－act－of－1996－hipaa，2016 年 11 月 1 日。

⑧ 参见 Bendix J，Editor S：HIPAA compliance requires informing patients of privacy rights，Medical Economics，No. 3，2014.

年《经济和临床健康信息科技法案》（Health Information Technology for Economic and Clinical Health Act，简称HITECH）指引中对HIPAA法案所管辖组织的商业伙伴（Business associates）责任作出了规定。为了能与该指引的规定相一致，美国卫生部于2013年将Omnibus规则增加到HIPAA法案中，对患者健康信息保护隐私规则、安全规则和违约通知规则进行了修改。①

三、HIPAA法案对健康信息隐私的保护

《美国行政法典》第45篇为公共福利（Public Welfare）的规定，HIPAA法案隐私规则规定在标题为“美国卫生和公共服务部”（Subtitle A-Department of Health and Human Services）一章中。HIPAA法案隐私规则由该章的第160部分和第164部分的子部分A部分和E部分构成。② 第160部分为管理要求的一般规定；第164部分的规定为安全和隐私，其子部分E部分规定的是个人可识别性健康信息，其中包括了诸多受保护的健康信息使用和公开的标准（Standards）和实施规范（Implementation specifications），还包括了受保护健康信息隐私实践通知、健康信息隐私保护请求权、受保护健康信息修改权、受保护健康信息获取权的标准和相关实施规范。HIPAA法案隐私规则对于患者健康信息隐私的保护规定特色明显、适用性强，试析如下：

（一）受管辖机构涵盖范围广

HIPAA法案隐私规则对患者健康信息隐私的保护非常全面，其突出表现就是适用范围很广，尽可能涵盖能够接触患者隐私的机构和个人。HIPAA法案隐私规则第160部分第102节规定：除非另有规定，以下规定的标准、要求和实施规范适用范围包括以下机构：健康计划（Health plans）、卫生保健信息处理机构（Health care clearinghouses），以及在业务中传输电子健康信息的卫生保健服务提供者（Health care providers）。2013年，HIPAA法案管理简化部分修改实施的Omnibus规则，将以上机构的商业合作者也加入到了适用主体范围，使得HIPAA法案适用主体涵盖范围进一步扩大。

HIPAA法案隐私规则给健康计划、卫生保健信息处理机构、卫生保健服务提供者、受管辖机构商业伙伴作出了如下定义：

健康计划，是指为医疗保健提供费用或付费的个人或团体计划，包括单个计划或计划的组合，具体涵盖团体健康计划、健康保险、健康维护组织、医疗保险计划A部分和B部分、医疗救助计划、自愿处方药福利计划、医疗救助补充政策保险、长期护理政策保险、员工福利计划、军人卫生保健计划、退伍军人健康护理卫生保健计划、印第安人健康服务计划、联邦雇员健康福利计划、各州儿童健康计划、医疗特惠计划、各州法律规定的适格个人高风险健康保险或高风险比较保险和其他计划。

卫生保健信息处理机构，是指公共的或私人组织，包括账单服务机构、重新定价公司、社区卫生管理信息系统或社区卫生信息系统、增值性网络和交换机构。其从事以下业务：将从另一实体接收到的非标准格式健康信息数据或含有非标准数据内容的信息处理为标准数据，或进行标准数据传送；为信息接收实体接收另一实体传送的标准数据，或为其将健康信息处理为非标准格式数据或含有非标准内容的数据。

卫生保健服务提供者，是指本法案以及美国法典等法案规定的医疗和健康服务提供者；或者提供任何卫生保健服务、账单服务或为卫生保健付费等正常业务的个人或组织。由于卫生保健服务提供者已经在本法其他部分和美国法典中做了规定，所以在HIPAA隐私规则中的规定相对简略。

受管辖机构商业伙伴，是指与受管辖机构相关的组织或个人，代表受管辖机构或有组织的卫生保健计划，进行创造、接收、保存、传

① http://searchdatamanagement.techtarget.com/definition/HIPAA，2016年12月5日。

② The HIPAA Privacy Rule，http://www.hhs.gov/hipaa/for-professionals/privacy/，2016年8月1日。

输受保护健康信息或进行其他活动；为机构或有机构参与的有组织卫生保健计划提供法律、保险精算、记账、咨询、数据收集、管理、制证或金融服务。一个组织可能成为另一个组织的商业伙伴。受管辖机构商业伙伴包括健康信息组织、电子处方通道或给受管辖机构提供受保护健康信息数据传输服务的个人、或因常规需要获取受保护健康信息的其他个人、代表受管辖机构向一个以上个人提供个人健康记录的个人、代表商业伙伴创造、接收、保存或传输受保护的健康信息的分包商。

另外，HIPAA 法案也给人（Person）作出了定义，是指自然人、财产信托机构、合伙、公司、专业协会或其他公共的或私人组织。

（二）隐私规则的规定内容丰富，体系性强

1. HIPAA 法案隐私规则具有一般性规定和总则性规定，简化了条文

HIPAA 法案第 160 部分为管理要求一般规定，在其总则部分规定了立法基础、立法目的、定义、修改和实施日期等内容，适用于隐私规则和安全规则；第 164 部分为安全和隐私相关规定，其总则部分规定了立法基础、定义、适用性、组织要求以及与其他部分的关系等内容，第 164 部分的 E 部分是受保护个人健康信息隐私规定，其 502 节为受保护个人健康信息隐私使用和公开的一般规则。一般性规定和总则性规定简化了法律条文，使得法律文本更加简洁，增强了体系性。

2. 定义部分的规定丰富、具体

HIPAA 法案隐私规则在多处作出了定义性的规定，以便于对法律文本的理解和适用，定义部分的规定不仅丰富，而且极为详细，注意了其与法律文本的体系性、协调性。HIPAA 法案隐私规则在第 160 部分的 A 部分 103 节规定了 30 多个基础性定义，这些定义除了适用隐私规则外，还适用于其他管理要求。这些基础性定义主要有：管理简化条款、民事罚金、受管辖机构、电子媒体、家庭成员、遗传服务、遗传信息、团体健康信息、卫生保健、健康计划、实施规范、个人可识别性信息、症状、交易等。第 160 部分的 D 部分 401 节规定的定义有正当理由、合理注意、主观过错。HIPAA 法案隐私规则在第 164 部分的 E 部分 501 节规定了 10 多个定义，主要包括：矫正机构、数据聚集、指定记录集、直接治疗关系、卫生保健手术、卫生监督机构、间接治疗关系、囚犯、营销、报酬、心理治疗记录、公共卫生部门、研究等。HIPAA 法案隐私规则在其他部分也有相关定义的规定。另外，HIPAA 法案隐私规则将定义规定在各部分法条的相近位置，考虑了该定义与法条的相关性，如果该定义已经在其他法律有规定时也一并说明。丰富、具体的定义对于 HIPAA 隐私规则法律文本的理解和适用提供了便捷和帮助。

3. 受保护健康信息使用和公开具体标准分类多

HIPAA 法案隐私规则对于受保护健康信息隐私的保护标准的分类很多。

首先，在受保护健康信息使用和公开的一般规则中规定的标准就有十种，具体包括：受管辖机构及其商业伙伴使用和公开受保护健康信息标准、最低必要标准、限制性同意标准、可识别性受保护健康信息去除可识别性后的使用和公开标准、已故之人受保护健康信息使用和公开标准、因员工检举揭发和员工作为刑事受害人公开受保护健康信息标准等。其中，受管辖机构及其商业伙伴使用和公开受保护健康信息标准规定了受管辖机构及其商业伙伴对于受保护健康信息的许可使用和公开、被要求使用和公开、禁止使用和公开的情形。

其次，在受保护健康信息的使用和公开的一般规则之外，其他部分法条也有关于标准的规定，这些标准具体包括：受管辖机构商业伙伴合同标准，团体健康计划要求标准，复合功能实体要求标准，因治疗、付费或卫生健康手术需要使用和公开受保护健康信息标准；需授权使用和公开受保护健康信息标准，要求给予授权或给予个人同意或反对机会使用和公开受保护健康信息标准，无需授权或要求个人同意或反对使用和公开受保护健康信息标准，其他与使用和公开受保护健康信息相关的要求标准。

最后，隐私规则还在隐私实践通知、健康信息隐私保护请求权、受保护健康信息获取权、

受保护健康信息修改权、受保护健康信息公开报告、管理要求等相关条款中也有关于标准的规定。

（三）HIPAA 法案隐私规则具有可执行性

1. 健康信息使用和公开实施规范较为详细

HIPAA 隐私规则在受保护隐私使用和公开的标准之下，大多规定了相关的实施规范，以便对标准的进一步实施提供更为详尽的支持，增强了法条的可操作性。HIPAA 法案第 164 部分 502 节规定的是受保护健康信息使用和公开的一般规则，其中，个人代表标准实施规范中分别规定了针对成年人和独立的未成年人，未成年人，已故之人，家庭暴力、忽视和危险的实施规范。第 164 部分 504 节规定的是受保护健康信息使用和公开的组织性要求，在其商业伙伴合同标准之下规定的实施规范包括了商业伙伴合同、其他事项、合同和其他事项的其他要求、商业伙伴和其分包商合同等实施规范。第 164 部分 506 节规定了因治疗、付费或卫生保健手术需要使用和公开受保护健康信息实施规范。第 164 部分 508 节规定了需授权使用和公开受保护健康信息实施规范，具体包括有效授权、瑕疵授权、混合授权、限制授权的禁止、授权的撤回、文档化等实施规范，还规定了核心要素和要求实施规范，具体包括核心要素、要求性陈述、语言平实化实施规范。

2. 包含惩罚性条款的规定

惩罚性条款使得 HIPAA 法案隐私规则具有直接法律效力，避免了空洞的原则性规定和缺乏可诉性的宣示性规定的缺陷。HIPAA 法案第 160 部分的 D 部分为民事罚金的规定，该部分的规定具体详细，主要包括：定义部分、民事罚金使用基础性规定、民事罚金数额、民事罚金数额决定因素、积极抗辩、罚金通知、罚金收集等，具有较强的操作性。如果卫生部认为受管辖机构或其商业伙伴违反了管理简化条款，除具有积极抗辩事由外，卫生部可以对其处以民事罚金。HIPAA 法案第 160 部分 404 节和 406 节是有关于民事罚金的数额的规定，其数额因受管辖机构是否知情、履行了合理注意义务、具有主观过错等因素而不同。该部分内容对民事罚金金额做出了如下具体规定：2009 年 2 月 18 日之前的违法和 2009 年 2 月 18 之后的违法民事罚金数额不同。2009 年 2 月 18 日之前的违法，每次违法的罚金可达 100 美元，一年内（从元月 1 日至 12 月 31 日）对于相类似的违法，民事罚金总额可达 2500 美元；2009 年 2 月 18 日之后的违法，每次违法的罚金为 100 美元至 50000 美元或更多，一年内（从元月 1 日至 12 月 31 日）对于相类似的违法，民事罚金总额可达 1500000 美元。HIPAA 法案第 160 部分 408 节规定的是决定民事罚金数额的考虑因素，该节规定决定民事罚金数额时，卫生部将视以下情况减少或增加数额：一是违法性质和程度，包括受影响人数、违法行为发生的时间；二是因违法行为所产生的伤害的性质和程度，包括违法行为是否造成身体伤害，违法行为是否导致财产损害，违法行为是否导致个人名誉损害，违法行为是否阻碍了个人获得卫生保健的能力；三是遵守管理简化条款的历史情况，包括当前违法行为是否和先前违法行为相同或相似，受管辖机构或其商业伙伴是否改正，或改正违法行为的程度，受管辖机构或其商业伙伴如何回应卫生部关于遵守该法做出的努力的援助，受管辖机构或其商业伙伴如何回应此前的申诉；四是受管辖机构或其商业伙伴经济状况，包括是否有影响其执行能力的经济困难，处以民事罚金是否减损受管辖机构或其商业伙伴继续提供卫生保健或为卫生保健付费的能力，受管辖机构或其商业伙伴的规模大小。从以上规定可以看出，HIPAA 法案隐私规则对于民事罚金数额的规定具有可操作性。

（四）体现了平衡个人健康信息保护和社会利益之间的价值理念

HIPAA 法案隐私规则通过实现主体对于受保护健康信息的必要性自主控制和为了社会利益对于个人受保护健康信息进行必要性使用，试图努力平衡个人健康信息保护与有效利用和公开的矛盾，平衡个人健康信息保护和社会利益的矛盾，主要体现在以下方面：

1. 受保护健康信息有限保护与合理使用和公开的规定

HIPAA 法案第 164 部分 506 节是因治疗、

付费或卫生保健手术需要使用和公开受保护健康信息的规定；508 节是需授权使用和公开受保护健康信息的规定；510 节是要求给予授权或给予个人同意或反对使用或公开受保护健康信息的机会的规定，这几部分主要体现了健康信息主体对于健康信息的自主控制权。第 164 部分 512 节是无需授权或无需个人同意或反对的使用和公开受保护健康信息的规定，主要考虑了司法要求、守法监督等社会利益以及弱势群体和儿童利益的保护。从以上法条可以看出 HIPAA 法案隐私规则体现了受保护健康信息有限保护与合理使用和公开相结合的立法理念。

2. 受保护健康信息去可识别性后的使用和公开规定

HIPAA 法案隐私规则规定了受保护健康信息去可识别性后的使用和公开，具体内容包括：第一，受保护健康信息去可识别性后的使用和公开标准。该标准规定受管辖机构可以使用受保护健康信息来创造不具有个人可识别性的信息，或仅以此目的向其商业伙伴公开受保护健康信息，无论受管辖机构是否使用该去可识别性信息。第二，去可识别性信息的使用和公开。符合标准和实施规范的健康信息不被认为是个人可识别性健康信息，也就是说，已经去除可识别性。第三，受保护健康信息去可识别性标准。不能识别个人身份的信息和没有理由相信该相关信息能被用来识别个人身份的信息是个人非可识别性信息。受保护健康信息去可识别性要求实施规范规定：个人或其亲属、雇主、家庭成员的以下可辨别性信息应被去除：姓名，所有小于州的地理区划，包括街道地址、城市、县、选区、邮政编码等，直接与个人有关的日期，包括出生日期、入院日期、出院日期、死亡日期，89 岁以上的年龄以及此年龄的指示性日期构成成分，社会保障号码，证书或许可证号码，生物特征标识，全脸图像和任何类似图像等。受保护健康信息去可识别性要求规范规定的内容全面，保证了健康信息可识别性的彻底去除。

3. 最低必要标准及其实施规范规定

HIPAA 法案隐私规则规定了最低必要标准及其实施规范，规定了个人健康信息使用和公开的前提要求，即最低必要性，充分体现了个人健康信息保护和社会利益的平衡，具体包括：第一，最低必要标准。最低必要标准规定在 HIPAA 法案第 160 部分 502 节，属于受保护健康信息使用和公开的一般规则之一。该节规定：最低必要标准是指当使用和公开受保护健康信息，或从另一个受管辖机构或其商业伙伴获取受保护健康信息时，受管辖机构或其商业伙伴必须作出合理努力，为完成预期目的而使用、公开或获取受保护健康信息，并将必要性限制到最低。第二，最低必要标准除外性规定。最低必要标准不适用于以下情形：因治疗需要应卫生保健服务提供者请求向其公开、许可使用和公开、需要授权的使用和公开、因执行和调查需要向卫生部公开、因法律规定公开。第三，最低必要标准实施规范。HIPAA 法案第 160 部分 514 节规定了最低必要标准实施规范，包括：受保护健康信息最低必要使用实施规范、受保护健康信息最低必要公开实施规范、健康信息最低必要保护请求实施规范和其他要求实施规范。

五、HIPAA 法案健康信息隐私保护对我国的立法借鉴

（一）明确立法法理基础

在美国法的理论体系下，隐私权涵盖范围较广，包括个人健康信息在内的个人信息都可以在隐私权的框架下进行保护，再加上英美法系有重实用的传统，对于患者健康信息隐私的保护性立法相对灵活。HIPAA 法案隐私规则也在很多地方将患者健康信息直接称为患者健康信息隐私。大陆法系立法注重体系和形式，我国立法同样如此。因此，在我国，对于患者隐私权的立法保护考虑的首要问题就是明确患者健康信息隐私属于我国民法上的隐私。我国《侵权责任法》只是简单地承认了隐私权的概念，对于隐私权的内涵和外延没有明确的界定。有学者指出，隐私权可以进一步类型化为独处的权利、个人生活秘密的权利、通信自由、私人生活安宁、住宅隐私等，就私人生活秘密而

言，又可以进一步分类为身体隐私、家庭隐私、个人信息隐私、健康隐私、基因隐私等。甚至根据不同的场所，又可以分为公共场所隐私和非公共场所隐私等。[①] 应当明确，个人健康信息具有私密性，当属信息隐私，对于个人健康信息的保护是对隐私权的保护。另外，鉴于我国《侵权责任法》已经对患者隐私保护进行了初步规定，在今后的立法中，应当将个人信息中的健康信息加以明确化和具体化，明确个人健康信息应当包括患者姓名、住址、诊疗记录、基因信息等相关信息。我国《侵权责任法》对患者隐私的规定还需要其他法律法规的衔接和支持，需要进一步细化，在保证法律体系协调的前提下，可以考虑制定患者权利保护法、隐私权法或患者隐私权保护法等相关法律法规，作为患者隐私权保护的特别法，构建以侵权责任法为一般法的患者隐私权法律保护体系。

（二）明确健康信息隐私侵权主体

我国《侵权责任法》第六十二条规定：医疗机构及其医务人员应当对患者的隐私保密。泄露患者隐私或者未经患者同意公开其病历资料，造成患者损害的，应当承担侵权责任。《中华人民共和国性病防治管理办法》《中华人民共和国护士管理办法》《中华人民共和国执业医师法》《医疗机构病历管理规定》等法律法规中也对患者隐私保护有所规定，但适用主体单一，受管辖主体仅为医疗机构及其医务人员。因此，可以借鉴 HIPAA 法案隐私规则的规定，在立法中扩大患者健康信息隐私的侵权主体和责任主体，将可以接触到患者健康信息隐私的相关主体的侵权行为进行立法规制。实践中，可以直接接触到患者个人健康信息的主体主要是医务人员，包括医学专业实习人员，但也不能排除诸多医疗机构辅助工作人员，如：医院管理人员、病历管理人员、保洁人员、陪护人员等；可以间接接触到患者个人健康信息的主体相当广泛，包括医疗设施维护人员、医院后勤人员等医疗辅助人员，还包括药品生产供应商、医疗器械生产供应商、患者个人信息保存机构等和医院以及患者具有商业利益关系的企业与个人等。因此，在立法中，应当将这些机构或个人作为患者健康信息隐私侵权的主体。

（三）明确细化规定，增强可执行性

法律规范的可执行性是指通过立法活动创制的法律规范实现实施效果最优化所应具备的内在的和形式的立法技术要求。[②] 为了增强我国患者隐私权保护规则的可执行性，在今后的立法中应当做到：首先，在立法中明确患者隐私权的概念及具体类型，应当明确规定隐私权包括患者健康信息隐私权。HIPAA 法案中关于健康信息以及相关定义的规定都值得借鉴。如：健康信息、卫生保健服务提供者、最低必要标准等概念的定义丰富、具体，都具有极强的参考性。其次，增加患者健康信息隐私保护实施规范。可以适当借鉴 HIPAA 法案隐私规则的规定，制定以侵权责任主体为立法线索，适当列举的立法方式，来制定具体侵权行为实施规范，方便法律适用。再次，增加侵害患者健康信息隐私的具体惩罚机制。可以借鉴 HIPAA 法案隐私规则对于民事罚金数额的规定，适当考虑我国国情和地方差异，规定每次侵权的民事罚金的数额计算方法，适当考虑主观过错程度、改正其侵权行为的态度，还应适度考虑民事罚金对其为社会提供服务能力的影响。适当、科学地处以民事罚金，可以鼓励侵权主体自我改正，继续为社会提供必要的服务。最后，设立专门的健康信息隐私管理负责人员和联系人员。可以借鉴 HIPAA 法案隐私规则的相关规定，在包括医疗卫生机构等可以接触到患者健康信息的机构内设立健康信息隐私管理专门人员，进行专业化管理，并强化其责任。

（四）立法中应注意平衡个人健康信息保护和社会利益间的矛盾

HIPAA 法案隐私规则在保护个人健康信息的同时，力图维护个人健康信息隐私利益和社会公共利益之间的平衡。HHPAA 法案隐私规则在致力于保护个人健康信息的前提下，规定

① 王利明：《隐私权概念的再界定》，《法学家》2012 年第 1 期。

② 武志：《法律规范可执行性的理论诠释与实现路径》，《长春理工大学学报（社会科学版）》2015 年第 12 期。

卫生部可以适当使用个人健康信息，以实现其监管功能，体现了以社会利益为重的价值理念。在对受管辖机构遵守和实施隐私规则的管理和调查中，卫生部可以接触受管辖机构的设备、记录、账册和其他包括受保护健康信息在内的信息来源。在受保护健康信息去可识别性的规定，以及去可识别性后的使用和公开、最低必要标准和实施规范等特色性规定中，也体现了力图实现个人健康信息隐私利益和社会公共利益之间达到平衡的理念。今后我国患者信息隐私保护立法中，可以赋予监管机构更多的权利，以实现其监管职能的实现。可以充分借鉴 HIPAA 法案隐私规则对于可识别性信息去可识别性的详细规定，做到彻底去除可识别性，充分保护患者健康信息隐私；同时促进健康信息的合理使用和公开，促进医学发展和社会进步，促进和保障全民健康水平不断提高。

（五）赋予个人更多有关个人健康信息相关的自主权利

HIPAA 法案隐私规则还赋予了个人对于其个人健康信息使用和公开的自主性权利，主要有获得通知权、受保护健康信息获取权、受保护健康信息更正权、受保护健康信息公开报告接收权等。获得通知权是指个人对于受管辖机构使用和公开受保护健康信息时获得充分通知的权利、充分获知其享有个人权利和受管辖机构负有法律义务的权利。受保护健康信息获取权是指个人有权查验和获得指定记录集记录的健康信息的权利。受保护健康信息更正权是指个人有权要求受管辖机构更正其保存在指定记录集的受保护健康信息的权利。受保护健康信息公开报告接收权是指个人有权就受管辖机构在受保护健康信息公开报告被要求做出之日起 6 年内接收保护健康信息公开报告的权利。HIPAA 法案隐私规则规定的个人健康信息自主性权利是个人信息隐私权的重要相关权利，对于我国健康信息保护立法具有积极指导作用，在我国患者隐私权法律保护的立法中，应当采纳、补充和完善这些自主性权利。

本文作者：蔡宏伟是甘肃中医药大学定西校区人文教学部讲师，中国社会科学院研究生院法学系 2015 级博士研究生；龚赛红是中国社会科学院研究生院教授、博士生导师

责任编辑：周勤勤

A Study on References to the Protection of Patient Privacy Rights of HIPAA

Cai Hongwei　Gong Saihong

Abstract：The legislation of patient privacy rights of China should be further improved. The provisions of Privacy Rule in Health Insurance Portability and Accountability Act（HIPAA）are detailed，exercisable and systematic，and can serve as references. In legislation，the legal basis should be clear，the subject of torts should be definite，the specification should be detailed to improve enforcement，the protection of health information and social interests should be balanced and more individual dominant rights should be authorized to the individuals.

Keywords：patient privacy right；HIPAA；social interests；dominant rights