·医学信息研究·

HIPAA 演变分析及其启示*

王冰倩 李亚子 李 娟 谢莉琴

(中国医学科学院 医学信息研究所/图书馆 北京 100020)

〔摘要〕 通过介绍 HIPAA 法案的主要内容及演变过程，提出我国应借鉴的先进经验：明确患者隐私信息的保护范围及安全标准，增强政策法规可问责性，细化侵权行为与具体惩罚措施，追求保护隐私与维护公益的价值平衡，进而为我国个人健康信息安全与隐私保护法律的制定提供参考。

〔关键词〕 健康保险携带与责任法案；隐私保护；演变；启示

〔中图分类号〕R-1 〔文献标识码〕A 〔DOI〕10.3969/j.issn.1673-6036.2016.02.010

HIPAA Evolution Analysis and Its Implication *WANG Bing-Qian, LI Ya-Zi, LI Juan, XIE Li-qin, Institute of Medical Information/ Medical Library, Chinese Academy of Medical Sciences, Beijing 100020, China*

〔**Abstract**〕 By introducing main contents of Health Insurance Portability and Accountability Act (HIPAA) and its evaluation process, the paper puts forward advanced experience which should be learnt by China. That is to clarify the protection scope of and security standards for patients´private information, strengthen the accountability of policies and regulations, detail infringement acts and specific punishment measures, and pursue the value balance between privacy protection and maintenance of public interest. Thus, it can provide reference for formulating laws on personal health information security and privacy protection in China.

〔**Keywords**〕 Health Insurance Portability and Accountability Act (HIPAA); Privacy protection; Evolution; Implication

1 引言

随着信息化技术的发展和管理意识的不断提高，我国卫生信息化的进程不断加快，使卫生机构之间个人健康信息的共享成为可能。然而，信息共享的程度越高，对其隐私性的威胁也越大。因此，在健康信息交换的过程中如何保护个人隐私已经成为卫生信息化发展过程中亟需解决的问题。

美国是世界上隐私权法律较为健全的国家，在卫生信息化环境下如何保护个人隐私的问题上，已经出台并实施了多项政策和法规并积累了丰富的实践经验，其中最具代表性的法规即《健康保险携带与责任法案》(Health Insurance Portability and Accountability Act, HIPAA)，HIPAA 法案是近 30 年来最彻底的医疗保健立法。而目前我国尚未建立起完整的病人隐私权立法体系，涉及健康信息隐私的相关法律法规与政策保障仍存在一定不足，尤其是隐私保护方面，我国应该借鉴美国先进的立法经验，切实推进立法及修法进度。

〔修回日期〕 2015-10-09

〔作者简介〕 王冰倩，在读硕士研究生；通讯作者，李亚子，博士，副研究员。

〔基金项目〕 协和青年基金课题“人口健康信息公开共享及安全隐私保护策略研究”(项目编号：33320140194)。

2 研究目的、资料与方法

2.1 目的

个人健康信息安全与隐私保护是近年来国内外卫生信息化研究领域的热点与难点议题，而我国对于个人健康信息安全与隐私保护的研究相对起步较晚，对 HIPAA 法案进行详细介绍和研究的文献几乎没有。本文通过详细介绍 HIPAA 法案的主要内容及演变过程，为我国个人健康信息安全与隐私保护法律的制定提供一些参考。

2.2 资料与方法

对于 HIPAA，国内文献一般直接称为 HIPAA 法案、健康保险携带和责任法案、医疗电子交换法案或义务型可携带式健康保险法案（台湾）。本文运用文献调研和综合对比研究等方法，通过检索美国卫生部门官方网站以及 PubMed、Science Direct、CNKI 和万方等国内外数据库，调研美国 HIPAA 法案的主要内容和演变过程，从患者隐私信息的保护范围及安全标准、政策法规的可问责性、侵权行为与惩罚措施的规定、保护隐私与维护公益的价值平衡4 个方面综合对比分析 HIPAA 法案和我国个人健康信息安全与隐私保护法律的建设现状与差异。

3 结果分析

3.1 HIPAA 的产生背景和主要内容

3.1.1 产生背景 随着医疗保健领域信息系统应用越来越广泛，医疗保健对信息系统的应用和依赖不可避免地带来相应的信息安全问题，如病人的病历保密问题[1]。美国医疗模式在 20 世纪 90 年代时发生了巨大变革，同时电子病历系统得到了广泛普及，美国国会意识到电子信息技术发展将对卫生信息隐私安全方面带来严峻挑战，针对病人隐私保护进行立法的需求也越发明显。1991 年美国卫生及公共服务部（United States Department of Health and Human Services，HHS）组建了电子数据交换工作组（The Workgroup on Electronic Data Interchange，WEDI）研究电子数据的交换问题。1992 年 WEDI 提交了一份关于医疗保险电子数据交换标准化的研究报告并于 1993 年发表。为提高医疗卫生保健系统的效率与有效性，实现电子健康数据标准性、隐私安全性，提高医疗保险覆盖率，1996 年比尔·克林顿总统签署了由美国国会通过的 HIPAA 法案。

3.1.2 主要内容 （1）法律保障医疗保险的覆盖率、移植性和连续性。修改美国《公共健康服务法》（Public Health Service Act，PHSA），《雇员退休收入保障法案》（the Employee Retirement Income Security Act，ERISA）及 1986 年的《国内税收法》（the Internal Revenue Code of 1986），通过限制以个人既存不利问题等因素导致的歧视排斥参保行为、提供个人前参保信用记录、保障小雇主保险覆盖、制定团体保险参保人丢失工作转为参加个体保险规定等方式提高团体和个人市场中医疗保险覆盖的可移植性和健康保险的连续性。（2）严防浪费、欺诈、滥用。打击在医疗保险和医疗保健服务供给过程中的浪费、欺诈和滥用行为。（3）缴费。推广使用医疗储蓄账户。（4）护理服务。改善长期护理服务准入机制并提高其覆盖率。（5）简化医疗保险的行政管理。HIPAA 中相关管理简化规定要求美国卫生部为电子卫生保健事务、代码集、唯一的健康标识符、信息安全（医疗费用电子支付、隐私保护）等方面制定国家标准。

3.2 HIPAA 的演变过程

3.2.1 概述 管理简化规定作为 HIPAA 法的重要内容，也是修改最为频繁的部分。管理简化规定总体可划分为事务和代码集标准、标识符标准、隐私规则、安全规则、执法规则、违约通知规则 6 个部分[2]，所以 HIPAA 法案的演变也可以从这 6 个方面进行梳理分析。1996 年 HIPAA 法案出台之后经历了6 次重要的演变，分别于 1998、1999、2003、2004、2009、2013 年充实完善：1998 年对管理简化规定中的事务和代码集标准、标识符标准和安全标准方面提出了相应的标准规范；1999 年提出了《HIPAA 隐私规则》，包含个体可识别健康信息隐私保护的标准，规范了相关信息的使用与披露；2003

年最终确定电子信息安全标准规范并发布了《民间资金惩罚》，对管理简化规定中的执法规则做出规定；2004 年发布《HIPAA 管理简化规定：为卫生保健提供者提供唯一的健康标识符标准》，规则最终确定标识符标准；2009 年发布《关于健康信息外泄通知义务》，完善违约通知规则；2013 年发布《关于 HIPAA 隐私、安全、执法、违约通知等规则的修改》，补充完善了相关规定。

3.2.2 事务和代码集标准 1996 年管理简化规定要求 HHS 制定一系列便于电子信息交换的标准，HHS 卫生保健财政管理局，1998 年发布一系列的规则制定建议通知（Notice of Proposed Rule Making，NPRM），提出 8 项电子交易标准规范，2000 年公布了一系列《事务和代码集标准》，如电子数据交换 EDI 837，835，834，820，270，271 等。2001 年的 107 届国会通过修正案，将标准化工作延期到 2004 年 10 月 16 日并要求联邦审计总署对 HIPPA 法实施及电子数据交换标准的实施效果进行评估，于 2003 年 10 月 31 日前向议会提交报告。

3.2.3 标识符标准 1998 年 HHS 卫生保健财政管理局在发布的 NPRM 中提出了国家卫生保健提供者和雇佣者标识符标准及其相关使用规范，2004 年 11 月医疗保险和医疗补助服务中心（Centers for Medicare & Medicaid Services，CMS）发布了《HIPAA 管理简化规定：为卫生保健提供者提供唯一的健康标识符标准》，规则最终确定了国家卫生保健提供者标识符标准并对 NPI 标准执行做了相关规定。

3.2.4 隐私规则 1996 年管理简化规定要求 HHS 秘书处向国会提交关于保护个体可识别健康信息的建议，以及关于健康隐私信息主体权利、行使权利的程序、隐私信息的使用与披露 3 方面的详细建议。1999 年隶属于 HHS 的负责规划和评估的助理部长办公室向国会提交《个人可识别健康信息的隐私标准》（建议稿），也称《HIPAA 隐私规则》（HIPAA Privacy Rule），提出了保护行政、金融事务中涉及到的个体可识别健康信息隐私保护的标准，保护信息主体人的权利，规范相关信息的使用与披露，提高公共、个人健康计划和卫生保健服务的效率和有效性[3]，这个规则完善了 1996 年 HIPAA 中关于隐私保护的规定内容，2000 年 8 月提交了《个人可识别健康信息的隐私标准》（最终稿），之后发布了其技术修订。2001 年 HHS 民权办公室修改《个人可识别健康信息的隐私标准》生效日期延迟至 2001 年 5 月 14 日，2002 年 3 月发布《个人可识别健康信息的隐私标准》，提出对个人隐私保护的相关规定的修改并对法规存在的一些误解进行阐释，消除产生的不利影响，减轻法规导致的管理负担，于 8 月发布了最终版，规定生效时间为 2002 年 10 月 15 日。

3.2.5 安全规则 1998 年 HHS 卫生保健财政管理局在发布的 NPRM 中提出了个体信息安全和电子签名相关信息安全标准等，之后于同年 8 月发布了《安全与电子签名标准》（建议稿），提出了个人电子健康信息以及电子签名安全问题的标准规范，补充了 1996 年 HIPAA 法案中管理简化规定的内容。2003 年 2 月 CMS 发布《医疗保险改革：安全标准》最终确定健康计划、卫生保健信息交换中心和特定的卫生保健提供者必须采用的相关电子信息安全标准规范。2010 年 5 月发布了隐私安全规则的系列修改：电子方式提交临床药品和生物制剂试验数据的规则；建立医疗器械独立标识系统的要求；进一步加强医疗服务提供者和服务计划商业联盟的责任和义务；限制受保护的健康信息出售；强化个人获取电子医疗记录以及防止重要信息泄漏的相关权益。

3.2.6 执法规则 2003 年 5 月 HHS 秘书室发布《民间资金惩罚》，规则提出了对违反 1996 年 HIPAA 法管理简化规定的实体进行处罚的相关程序。2005 年 5 月 HHS 秘书室发布《HIPAA 管理简化规定：执法规则》，修改了现有关于调查违反 HIPAA 管理简化规定的实体以及处罚的流程，于同年 9 月发布《民间资金惩罚》最终版，最终确立了关于违反 HIPAA 管理简化规定的实体的处罚流程，重新规定了法规的有效期。2006 年 2 月发布了《HIPAA 管理简化规定：执法规则》的最终版。

3.2.7 违约通知规则 2009 年 8 月 HHS 民权办公室发布《关于健康信息外泄通知义务》，要求 HIPAA 法覆盖的实体及其业务伙伴提供违反保护健

康信息的通知[4]。2013 年 HHS 发布了《关于 HIPAA 隐私、安全、执法、违约通知等规则的修改》，补充完善了《针对经济和临床医疗的卫生信息技术法案》（Health Information Technology for Economic and Clinical Health Act，HITECH Act）中的相关规定，修改个人健康信息的保护期限从无限到死后 50 年。

通过调研分析 HIPAA 法案的主要内容和演变过程可以看出，从 1996－2006 年 10 年间，每年都会针对 HIPAA 法案进行细化或修改，之后修改的频率会稍微低些，几经修改 HIPAA 法案比较完备地对医疗健康信息的保护做出了规定。

4 对我国的启示

4.1 概述

经过近 20 年的发展，我国卫生信息化建设，特别是医院信息系统、实验室信息系统、影像存储与传输系统等医疗信息系统建设已初具规模，各地电子健康档案、电子病历建设发展迅速[5]。然而在建设过程中，涉及健康信息隐私的相关法律法规与政策保障仍存在一定不足，尤其是隐私保护方面。虽然我国立法体系日趋完善，公众对健康信息隐私权保护的认识也不断加强，但是目前我国尚未建立完整的病人隐私权立法体系，多数涉及病人隐私权的法律规定常散见于法律、行政法规以及司法解释中，且缺乏层次性及统一性，如不尽快解决，势必会影响我国卫生信息化的发展。因此，我国应该借鉴他国先进立法经验，切实推进立法及修法进度。

4.2 明确患者隐私信息的保护范围及安全标准

HIPAA 要求 HHS 制定医疗信息传输过程中的相关安全标准，规定哪些授权部门参与管理，同时为每一位患者提供一个识别符，用于身份验证与识别，保证他人不会不正当地侵入、拦截、篡改存储患者隐私信息的系统，HIPAA 同时向患者明确其具有哪些权利，清晰易懂。然而，我国保护患者隐私的法律、法规所约束规制的主体多是医疗机构及其工作人员，内容也缺乏系统性，规定十分抽象、过于原则化、效力层级低、使用范围有限，使得医疗实践中对患者隐私权的保护缺乏实际操作性，对患者所具有的隐私保护范围也没有立法解释。我国立法机关可以在制定法规时借鉴 HIPAA 法案注重细节，易于操作的特点，推进立法。

4.3 增强政策法规的可问责性

当前我国卫生信息化环境下的信息安全隐忧之一是责任的确立，医疗全程电子化的实现，将使纸质医疗凭证转变为电子凭证，而电子数据很容易被修改、复制，难以明确医疗责任，而 HIPAA 法案规定患者能够主动地利用本人的医疗信息并能自助查询到这些医疗信息被哪些机构查阅和利用过，从而增强了可问责性。

4.4 细化侵权行为与具体惩罚措施

HIPAA 建立了保护病人隐私的法律框架和法律标准，提升了整个卫生行业的标准化水平，明确规定了侵犯病人隐私的行为应面临的法律责任，对违反 HIPAA 给出了具体的惩罚措施，如对公民的处罚 100 美元/人/违例，上限 25 000 美元/违例/年；对明知故犯或故意泄密者，50 000 美元加 1 年监禁等，彻底改变了医护人员在处理医疗实务所获取信息的方式[6]。然而，我国目前没有建立对个人医疗信息隐私保护的基本架构，对隐私权的侵害缺乏明确和严厉的法律责任的规定，惩罚措施也不明确。

4.5 努力追求保护隐私与维护公益的价值平衡

为追求保护隐私与维护公益的价值平衡，HIPAA 一方面确立医疗信息的使用和披露应当由患者同意或授权的基本原则，另一方面规定有 12 种为维护社会公共利益可以不经患者同意使用和披露患者医疗信息的情形[7]。而我国立法没有明确界定公共利益的具体范围，使医疗机构有机会以公共利益之名，有意无意侵害患者隐私而谋取利益，如为宣传性病、艾滋病防治而侵犯患者隐私的案例。

5 结语

通过对美国健康信息隐私立法情况进行较全面

的了解，可以看到涉及健康信息隐私相关的立法已成为美国政策和法律的重要议题，这不仅因为健康信息隐私保护所面临的严峻挑战已成为亟待解决的国际性难题，也因为其不仅仅属于技术层面的问题，还有赖于来自法律与社会伦理层面、管理层面的支持，只有法律理论与技术方法、管理策略密切结合才能发挥更好的隐私保护效果。

参考文献

1 谷丽华，徐玲，孟群. 欧美国家健康信息隐私保护立法情况探析及对我国立法的启示［J］. 中国卫生信息管理杂志，2013，(6)：520－524.

2 Kyusuk Chung, Dalsang Chung, Yanghee Joo. Overview of Administrative Simplification Provisions of HIPAA［J］. Journal of Medical Systems, 2006, 30 (1): 51－55.

3 Ness Roberta B. Influence of the HIPAA Privacy Rule on Health Research［J］. the Journal of the American Medical Association, 2007, 298 (4): 236－237.

4 Act R R. Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; other Modifications to the HIPAA Rules［J］. Federal Register, 2013, 78 (17): 5565－5702.

5 王才有. “十二五”卫生信息化发展规划研读［J］. 中国卫生信息管理杂志，2012，9 (2)：13－16.

6 Gebbie K M. Privacy: the patient's right［J］. American Journal of Nursing, 2001, (101): 69－71, 73.

7 孟群. 卫生信息化相关法律法规与政策研究［M］. 北京：人民卫生出版社，2012.

(上接第 39 页)

卡结算等日常操作。各药房发药员负责药费交费刷卡确认，各医生站和/或护士站负责各自病人的医疗交费刷卡确认。门诊部办公室负责监督、查询门诊医疗收费情况，住院部办公室负责监督、查询住院医疗收费和住院生活收费情况。后勤部各食堂售饭员和商店售货员负责日常售卖收费刷卡确认，后勤部充值员负责职工卡的发卡、所有消费者的充值、退卡结算等日常操作以及监督、查询售卖收费情况。后勤部水电管理员负责采集节能控制系统的消费数据；各订餐员负责营养餐订餐、统计和送餐。行政部门考勤员负责考勤数据的采集、统计。院办秘书负责会议签到系统的设置、统计。

4 结语

总之，患者医院一卡通规范医院财务流程关系，强化医院财务管理制度，实现医院财务管理现代化，信息实时化，提高服务的效率和质量，有效解决办事手续繁杂和效率低下的问题。规范化的管理、优质的服务推进医院管理一体化系统逐步完善，为提升医院的管理和科学决策水平发挥重要的作用。

参考文献

1 王波，黄米娜. 医院门户平台的需求分析与设计建设方法［J］. 现代电子技术，2014，(10)：64－67，70.

2 夏慧. 基于“银医一卡通”的门诊综合信息系统设计与实践［J］. 医学信息学杂志，2013，(2)：16－20.

3 白雪，湖北省医疗“一卡通”模式及信息平台研究［D］. 武汉：华中科技大学，2011.

4 李海军，数字化校园中一卡通建设的研究与实现［D］. 天津：天津大学，2007.

5 王波. 基于等级保护的医院信息网络平台安全体系设计与实现［J］. 医学信息学杂志，2014，35 (7)：30－32.

6 沈亚琴，刘雪梅. 基于电子认证服务的军队医院信息安全解决方案［J］. 医学信息学杂志，2014，35 (7)：37－41.