I/S: A JOURNAL OF LAW AND POLICY FOR THE INFORMATION SOCIETY

CICELY N. TINGLE*

Developments in HIPAA and Health Information Technology

Abstract: This note provides an overview of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and its Privacy Rule. It then provides background into the controversy of the lack of enforcement by the Department of Health and Human Services ("HHS") Office of Civil Rights and updates the Department of Justice's criminal enforcement of HIPAA. The second half of this article focuses specifically on health information technology ("HIT") and provides an update on HHS' four HIT contracts, the Government Accountability Office's assessment of HHS' information technology and privacy efforts, currently pending HIT legislation, and a brief explanation of the debate concerning HIT legislation and preemption of state privacy laws.

* Cicely N. Tingle is a J.D./M.H.A. graduate of The Ohio State University Moritz College of Law, class of 2007. She received a B.A. in biological sciences from Northwestern University.

I. INTRODUCTION

This note examines important topics relating to the development of health care privacy in the past year. With many of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA")[1] regulations published as final rules, there is now greater attention to the enforcement of these rules. Another major topic examined in this note is the Department of Health and Human Services' ("HHS") role in helping to spread the use of health information technology to increase the safety and efficiency of the U.S. health care system. This note provides a brief overview of HIPAA and its Privacy Rule, along with recent developments in enforcement of HIPAA, including new indictments by the Department of Justice. The note then examines the government's participation in the development of health information technology throughout the past year in an effort to achieve President Bush's goal of electronic health records for most Americans by 2014.[2]

II. HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996

A. OVERVIEW

HIPAA was created to serve many purposes.[3] A few of the goals of HIPAA are "to improve portability and continuity of health insurance coverage in the group and individual markets, to combat waste, fraud, and abuse in health insurance and health care delivery, to promote the use of medical savings accounts, to improve access to long-term care services and coverage, [and] to simplify the administration of health insurance."[4] This last purpose, "to simplify the administration of health insurance," comprises a key element of HIPAA commonly referred to as the "Administrative Simplification"

---

[1] Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), Pub. L. 104-191, 110 Stat. 1936 (1996).

[2] Department of Health and Human Services, American Health Information Community: Background, http://www.hhs.gov/healthit/community/background/ (last visited Jan. 22, 2008).

[3] A more detailed discussion of HIPAA is provided in Elizabeth Hutton & Devin Barry, *Privacy Year in Review: Developments in HIPAA*, 1 ISJLP 347 (2005).

[4] *Id.*

provision.[5] The goal of the Administrative Simplification provisions is to "encourag[e] the development of a health information system through the establishment of standards and requirements for the electronic transmission of certain health information."[6] These provisions only apply to health plans, health care clearinghouses, and certain health care providers.[7]

In addition, the Administrative Simplification provisions require the Secretary of HHS to adopt standards for electronic exchange transactions, unique health identifiers, code sets, security, electronic signatures, and transfer of data elements.[8] HIPAA requires the Secretary of HHS to establish monetary penalties for those persons who fail to comply with the established standards.[9] HIPAA also provides criminal penalties for the "wrongful disclosure of individually identifiable health information."[10] As a result of this provision, HHS promulgated the Privacy Rule,[11] which will be discussed further below. To date, HHS has published final rules for Transactions and Code Sets,[12] Security,[13] Privacy,[14] Employee Identifiers,[15] and Enforcement.[16]

---

[5] HIPAA, Pub. L. No. 104-191, 110 Stat. 1936, 2021–2034 (codified at 42 U.S.C. §§ 1320d-1320d-8 (2006)).

[6] HIPAA, 42 U.S.C. § 1320d, Historical and Statutory Notes (2006).

[7] HIPAA, 42 U.S.C. §§ 1320d-(a)(1)–320d01(a)(3). The health care providers subject to HIPAA's Administrative Simplification provisions are those "who transmit[] any health information in electronic form in connection with a transaction referred to in section [42 U.S.C. § 1320-2(a)(1)]." HIPAA, 42 U.S.C. § 1320d-1(a)(3). The section 1320d-2(a)(1) transactions are described in section 1320d-1(a)(2) as: "(A) Health claims or equivalent encounter information; (B) Health claims attachments; (C) Enrollment and disenrollment in a health plan; (D) Eligibility for a health plan; (E) Health care payment and remittance advice; (F) Health plan premium payments; (G) First report of injury; (H) Health claim status; (I) Referral certification and authorization."

[8] HIPAA, 42 U.S.C. §§ 1320d-2(a)–1320d-2(f) (2006).

[9] HIPAA, 42 U.S.C. § 1320d-5(a) (2006).

[10] HIPAA, 42 U.S.C. § 1320d-6 (2006).

[11] Standards for Privacy of Individually Identifiable Health Information, 67 Fed. Reg. 53,182 (Aug. 14, 2002) (to be codified at 45 C.F.R. pts. 160 and 164).

[12] 45 C.F.R. pt. 162 (2003), *available at* http://www.cms.hhs.gov/transactioncodesetsStands/02_TransactionsandCodeSetsRegulations.asp.

[13] Health Insurance Reform: Security Standards, 68 Fed. Reg. 8334 (Feb. 20, 2003) (to be codified at 45 C.F.R. pts. 160, 162, and 164).

B. PRIVACY RULE

The Privacy Rule is of particular relevance to this note.[17] The Standards for Privacy of Individually Identifiable Health Information ("IIHI"), or the "Privacy Rule," provides standards to protect an "individual's health information . . . while allowing the flow of health information needed to provide and promote high quality health care and to protect the public's health and well being."[18] IIHI, sometimes referred to as protected health information ("PHI"), includes demographic data, information on an individual's "physical or mental health condition," information on the health care received by an individual, information related to payment for health care provided—or to be provided—to the individual, and information that identifies the individual.[19] The establishment of standards to protect IIHI also facilitates the use of electronic health care transactions and, consequently, supports health information technology ("HIT").[20] The basic principle of the Privacy Rule is that "a covered entity may not use or disclose protected health information, except either: (1) as the Privacy Rule permits or requires, or (2) as the individual who is the subject of the information (or the individual's authorized representative) authorizes in writing."[21] The imposition of a civil

---

[14] Standards for Privacy of Individually Identifiable Health Information, 67 Fed. Reg. 53,182 (Aug. 14, 2002) (to be codified at 45 C.F.R. pts. 160 and 164).

[15] Health Insurance Reform: Standard Unique Employer Identifier, 67 Fed. Reg. 38,009 (May 31, 2002) (to be codified at 45 C.F.R. pts. 160 and 162).

[16] HIPAA Administrative Simplification: Enforcement, 71 Fed. Reg. 8390 (Feb. 16, 2006) (to be codified at 45 C.F.R. pts. 160 and 164).

[17] For a more detailed discussion of the Privacy Rule, *see* Nusrat Rahman, *Reflections on Privacy: Recent Developments in HIPAA Privacy Rule,* 2 ISJLP 685 (2006).

[18] HHS OFFICE FOR CIVIL RIGHTS ("OCR"), SUMMARY OF THE HIPAA PRIVACY RULE 1 (2003), *available at* http://www.hhs.gov/ocr/privacysummary.pdf.

[19] *Id.* at 4.

[20] HHS Office of Civil Rights, *General Overview of Standards for Privacy of Individually Identifiable Health Information*, OCR HIPAA PRIVACY, Apr. 3, 2003, *available at* http://www.hhs.gov/ocr/hipaa/guidelines/overview.pdf.

[21] SUMMARY OF THE HIPAA PRIVACY RULE, *supra* note 18, at 4. SUMMARY OF THE HIPAA PRIVACY RULE also provides an overview of the permitted uses and disclosures, required disclosures, authorized uses and disclosures, and the limiting of uses and disclosures to the minimum necessary under the Privacy Rule. *Id.* at 4–11.

monetary penalty by HHS can result if a covered entity fails to comply with the Privacy Rule.[22]

C. UPDATES ON ENFORCEMENT

The Enforcement Rule, which became effective March 16, 2006, set the standard for civil monetary penalties and noncompliance.[23] The final rule expanded upon the previous rules regarding "the investigation of noncompliance to make them apply to all of the HIPAA Administrative Simplification rules, rather than exclusively to the privacy standards."[24] This section discusses recent developments in enforcement of HIPAA.

1. CIVIL ENFORCEMENT

The Office of Civil Rights ("OCR") within HHS is responsible for the civil enforcement of HIPAA. Under the Enforcement Rule, HHS has the authority to levy fines up to $100 per violation, but not to exceed $25,000 total, for identical violations committed during a calendar year.[25] Instead of enforcement through monetary penalties, however, HHS first looks for voluntary compliance from non-compliant entities, a practice which the Director of OCR, Winston Wilkinson, believes is working well.[26] Since the adoption of the HIPAA complaint system in July 2003, there has been little enforcement for noncompliance with HIPAA regulations.[27] As of August 31, 2007, even though there have been a total of 29,994 complaints filed with OCR, no fines have been issued to noncompliant

---

[22] *Id.* at 17; *see also* Rahman, *supra* note 17, for a discussion of civil money penalty and the final Enforcement Rule.

[23] HIPAA Administrative Simplification: Enforcement, 71 Fed. Reg. 8390 (Feb. 16, 2006) (to be codified at 45 C.F.R. pts. 160 and 164).

[24] *Id.*

[25] *Id.* at 8427 (to be codified at 45 C.F.R. § 160.404(b)).

[26] Rob Stein, *Medical Privacy Law Nets No Fines: Lax Enforcement Puts Patients' Files at Risk, Critics Say*, WASH. POST, June 5, 2006, at A01.

[27] Dennis Melamed, *Little Change in OCR Enforcement*, HEALTH INFO. PRIVACY/SEC. ALERT, Nov. 2006, at 4.

covered entities.[28] The most common complaints received by HHS include situations where "personal medical details were wrongly revealed, information was poorly protected, more details were disclosed than necessary, proper authorization was not obtained or patients were frustrated getting their own records."[29]

Dennis Melamed, publisher of the Health Information Privacy/Security Alert newsletter, believes that OCR deserves credit for providing statistics,[30] but he also believes that the statistics raise a new set of questions:

> [D]oes this mean that concerns over medical privacy are overblown? Or does it mean that the HIPAA privacy rule does not cover everyone it should? Or does it mean that the country got lucky and that the healthcare community has been protecting patient confidentiality but just didn't have a way to prove it until HIPAA came along? We just don't know. . . .[31]

Critics of HHS believe that these statistics, demonstrating a lack of enforcement, weaken compliance with HIPAA. Health care consultants find that many hospitals and other providers are taking the stance that "HHS really isn't doing anything, so why should I worry?"[32] Columbia University health privacy expert Janlori Goldman states that "[OCR has] done almost nothing to enforce the law or make sure people are taking it seriously . . . . [W]e're dangerously close to having a law that is essentially meaningless."[33]

---

[28] Dennis Melamed, *Private Practices Frequent Target of HIPAA Privacy Action*, HEALTH INFO. PRIVACY/SEC. ALERT, Sept. 2007, at 6 [hereinafter *Melamed Private Practice*]. Only about 5400, or 23.8%, of complaints (as of Sept. 30, 2006) received further investigation or action. HIPAAdvisory, *Less than 25% of Medical Privacy Complaints Merit HHS Investigation Melamedia Seminar Reveals*, HIPAA NEWS, Dec. 13, 2006, *available at* http://www.hipaadvisory.com/news/newsarchives/2006/1213mela.htm. As of Aug. 31, 2007, the number of total complaints increased to 7,550, or 25.2% of complaints. *Melamed Private Practice*, *supra* note 28.

[29] Stein, *supra* note 26.

[30] HIPAAdvisory, *supra* note 28

[31] *Id.*

[32] Stein, *supra* note 26 (quoting Chris Apgar of Apgar & Associates).

[33] *Id.* Similarly, Ohio State University law professor Peter Swire states that "lack of enforcement undermines compliance because privacy officers don't get budget and

On the other hand, because the rules are "complicated and relatively new," the entities covered by HIPAA—health plans, insurance companies, and providers—agree with HHS' voluntary compliance stance.[34]

2. CRIMINAL ENFORCEMENT

The statistics for the criminal enforcement of HIPAA are just as sparse. The U.S. Department of Justice ("DOJ") handles the criminal enforcement of HIPAA.[35] Until September 2006, there had only been two criminal prosecutions under HIPAA: *United States v. Gibson*[36] and *United States v. Ramirez*.[37]

Since September 2006, the DOJ has prosecuted two additional cases, *United States v. Ferrer*[38] and *United States v. Williams*,[39] which are now the third and fourth HIPAA prosecutions by the DOJ, respectively. On September 8, 2006, two individuals were indicted in Florida on eight counts, including "violating [HIPAA], through their wrongful disclosure of individually identifiable health information in violation of 42 U.S.C. § 1320d-6(a)(2) . . . ."[40] One of the individuals

---

management attention unless they can show that the rules have teeth." Deborah Gage & Kim S. Nash, *A Tenuous Grip on Data*, BASELINE, Dec. 8, 2006, http://www.baselinemag.com/article2/0,1540,2070225,00.asp. *See also*, Theo Francis, *Medical Dilemma: Spread of Records Stirs Patient Fears of Privacy Erosion*, WALL ST. J., Dec. 26, 2006, at A1.

[34] Stein, *supra* note 26.

[35] *Id.*

[36] United States v. Gibson, No. CR04-0374RSM, 2004 WL 2188280 (W.D. Wash. Aug. 19, 2004). *See* Hutton & Barry *supra* note 3, at 359 for further discussion.

[37] United States v. Ramirez, No. 7:05CR00708 (S.D. Tex. Aug. 30, 2005). *See* Rahman, *supra* note 17 for a discussion of U.S. v. Ramirez.

[38] The indictment of Ferrer and Machado can be found at http://www.usdoj.gov/usao/fls/PressReleases/Attachments/060908-01-Indictment.pdf (last visited Jan. 22, 2008).

[39] Press Release, The United States Attorney's Office, District of Delaware, Former Medical Biller Accused of Stealing Patients' Identities (Nov. 17, 2006), *available at* http://www.usdoj.gov/usao/de/press/2006/11_17_06_medicalidtheft.pdf.

[40] Press Release, The United States Attorney's Office, Southern District of Florida, Two Charged in Computer Fraud, Identity Theft and Health Care Fraud Conspiracy (Sept. 8, 2006) [hereinafter *Computer Fraud*], *available at* http://miami.fbi.gov/dojpressrel/pressrel06/mm20060908.htm.

charged, Isis Machado, was the front desk coordinator of the Cleveland Clinic's Weston Office in the Miami, Florida, area.[41] The indictment alleges that "Machado . . . wrongfully accessed the Cleveland Clinic's computerized patient files and downloaded the personal identification information of more than 1,100 patients."[42] She then sold the patient information to her cousin, Fernando Ferrer, Jr., "who caused the stolen patient information to be used in connection with the submission of approximately $2.8 million in false claims to Medicare."[43]

Linda Danyell Williams was indicted in Delaware on November 16, 2006. Williams, an employee of Hospital Billing & Collection Services, Ltd. ("HBCS"), a health care clearinghouse, "accessed the identities of [over 400] patients through HBCS' computers" and supplied her accomplice, Richard Yaw Adjei, with personal health information.[44] A portion of the stolen identities were then used by Adjei in a tax fraud scheme.[45] Williams was charged with, among other things, "wrongfully obtaining individually identifiable health information . . . ."[46]

A key point to note is that, although Machado and Williams were employees of HIPAA-covered entities, neither employer has been charged with a privacy violation.[47] One health care law practitioner noted that government officials are specifically targeting the wrong-doers and are willing to work with the employer-providers that cooperate with the officials and that have systems in place to notify affected patients.[48] While a 2005 Justice Department memo indicated that "HIPAA criminal penalties for unauthorized disclosure apply

---

[41] *Id.*

[42] *Id.*

[43] *Id.*

[44] Press Release, The United States Attorney's Office, District of Delaware, *supra* note 39.

[45] *Id.*

[46] *Id.*

[47] Amy Lynn Sorrel, *3rd HIPAA Criminal Case Hints at Federal Tactics*, AMEDNEWS.COM, Oct. 16, 2006, http://www.ama-assn.org/amednews/2006/10/16/gvsb1016.htm. The District of Delaware press release does not mention any indictments against HBCS.

[48] *Id.* (citing Jacqueline M. Darrah, health care lawyer and HIPAA compliance specialist for Halleland Lewis Nilan & Johnson PA, in Minneapolis).

directly to covered entities . . . but not to their employees," an employer has yet to be charged in such a case.[49] The industry wonders whether this could be an emerging trend, particularly since the first two criminal prosecutions by the DOJ, *Gibson* and *Ramirez*, also concerned prosecution of the employee but not the employer.[50]

Assistant U.S. Attorney Peter A. Winn explained in a United States Attorneys' Bulletin article, "Criminal Prosecutions under HIPAA," that a possible theory of criminal liability for employees under HIPAA can be derived indirectly through 18 U.S.C. § 2(b).[51] The Justice Department memo, issued as an opinion by the Office of Legal Counsel of the Department of Justice ("OLC"), discusses "who can be prosecuted for *directly* violating [the HIPAA criminal statute, 42 U.S.C. § 1320d-6] . . . ."[52] The OLC opinion "concludes that 'liability under Section 1320d-6 must begin with covered entities, the only persons to whom the standards apply.'"[53]

Winn notes, however, that the OLC opinion "leaves open the possibility that employees and business associates could still be prosecuted" indirectly, under 18 U.S.C. § 2(b).[54] Title 18 U.S.C. § 2(b) states: "Whoever willfully causes an act to be done which if directly performed by him or another would be an offense against the United States, is punishable as a principal."[55] As a result, if an action performed by an employee or business associate would have violated section 1320d-6 if performed by the covered entity, then the employee or business associate is liable as if it were the principal.[56] Winn's section 2(b) theory, therefore, explains how in these recent criminal

---

[49] *Id.*

[50] *Id.* In both *Gibson* and *Ramirez*, the defendants pleaded guilty, so the court did not get the opportunity to answer the question of whether the employer should have been charged. *Id.*

[51] *See* Peter A. Winn, *Criminal Prosecutions under HIPAA*, 53 U.S. ATT'YS BULL. 21 (Sept. 2005), *available at* http://www.usdoj.gov/usao/eousa/foia_reading_room/usab5305.pdf.

[52] *Id.* at 23. The Office of Legal Counsel Opinion, "Scope of Criminal Enforcement Under 42 U.S.C. § 1320d-6," can be found at http://www.usdoj.gov/olc/hipaa_final.htm (last visited Jan. 22, 2008).

[53] *Id.*

[54] *Id.*

[55] 18 U.S.C. § 2(b) (2007).

[56] Winn, *supra* note 51, at 25.

enforcement cases the employee has been held criminally liable, while the employer has not.

III. PRIVACY AND HEALTH INFORMATION TECHNOLOGY

Despite the lack of enforcement, the HIPAA Privacy Rule has provided a baseline level of protection for health information and is therefore providing the framework for the necessary safeguards for implementation of health information technology. In order for advancement in the use of electronic health records ("EHR") and a nationwide health information network ("NHIN"), standards and procedures must be established so that IIHI can be protected as required by the Privacy Rule. Through contracts provided by HHS and possible legislation introduced by Congress, the government and private sectors continue to take steps to provide these standards and ease the implementation of HIT nationwide.

A. HEALTH INFORMATION TECHNOLOGY

In April 2004, President Bush "announced the goal of assuring that most Americans have electronic health records within the next 10 years."[57] The EHR will be able to "share information privately and securely among health care providers when authorized by the patient."[58] Executive Order 13,335 created the Office of the National Coordinator ("ONC") for Health Information Technology under the Secretary of HHS and charged the ONC with "developing a nationwide interoperable health information technology infrastructure."[59]

1. UPDATE ON HIT CONTRACTS AWARDED BY HHS

HHS awarded four contracts in the fall of 2005 that collectively provide a framework for implementing health information technology

---

[57] Press Release, The White House, Fact Sheet: Transforming Health Care for All Americans (May 24, 2004), *available at* http://www.whitehouse.gov/news/releases/2004/05/20040527-2.html.

[58] *Id.*

[59] Exec. Order No. 13,335, 69 Fed. Reg. 24059, 24059 (Apr. 30, 2004).

("HIT") nationwide.[60] This section provides an update on these contracts.

A. STANDARDS–ANSI

In October 2005, HHS awarded a contract to the American National Standards Institute ("ANSI"), which had partnered with the Healthcare Information and Management Systems Society ("HIMSS"), the Advanced Technology Institute ("ATI") and Booz Allen Hamilton, to form the Healthcare Information Technology Standards Panel ("HITSP").[61] HITSP seeks to "bring together a wide range of stakeholders to identify, select, and harmonize standards for communicating data throughout the healthcare spectrum."[62]

Since the award of the initial contract, HITSP has:

- approved an initial set of high-level standards that will help to communicate data in a nationwide health information network for the United States;[63]
- identified . . . an initial set of standards to facilitate the secure exchange of patient data in a new nationwide health information network ("NHIN");[64] and

---

[60] *See* Kirk Benton Koehler, *Toward Implementation of Electronic Health Records: Justification, Action, and Barriers to Adoption*, 2 ISJLP 651 (2006) for an overview of the initial HHS HIT contracts.

[61] Press Release, American National Standards Institute ("ANSI"), New Healthcare Information Technology Standards Panel Formed Under Contract from DHHS: ANSI partners with HIMSS, ATI and Booz Allen Hamilton to Lead Initiative (Oct. 6, 2005) [hereinafter *Technology Standards Panel*], *available at* http://www.ansi.org/news_publications/news_story.aspx?menuid=7&articleid=1054.

[62] *Id.*

[63] Press Release, American National Standards Institute ("ANSI"), HITSP Takes Another Step to Advance the NHIN (June 16, 2006) [hereinafter *HITSP Takes Another Step*], *available at* http://www.ansi.org/news_publications/news_story.aspx?menuid=7&articleid=1254.

[64] Press Release, American National Standards Institute ("ANSI"), Panel Recommends Initial Standards to Support Nationwide Health Information Network (June 30, 2006) [hereinafter *Panel Recommends Initial Standards*], *available at* http://www.ansi.org/news_publications/news_story.aspx?menuid=7&articleid=1262.

- recommended . . . three interoperability specifications in the areas of electronic health records, biosurveillance, and consumer empowerment.[65]

B. EHR CERTIFICATION–CCHIT

The Certification Commission for Healthcare Information Technology ("CCHIT") also received a contract from HHS in October 2005. The purpose of this contract is "to develop, create prototypes for, and evaluate the certification criteria and inspection process for electronic health records."[66] This three-year contract focuses on the certification of "ambulatory EHRs, inpatient EHRs, and the infrastructure components through which they interoperate."[67]

On April 30, 2007, CCHIT announced the certification of thirty additional ambulatory EHR products for a total of eighty-one overall.[68]

---

[65] Press Release, American National Standards Institute ("ANSI"), Standards Panel Delivers Interoperability Specifications to Support Nationwide Health Information Network: Implementation Testing to Begin on Biosurveillance, Electronic Health Records, and Consumer Empowerment (Nov. 1, 2006) [hereinafter *Interoperability Specifications*], *available at* http://www.ansi.org/news_publications/news_story.aspx?menuid=7&articleid=1361. Requirements for data exchange are as follows:

> The HITSP Biosurveillance Interoperability Specification defines specific standards that promote the exchange of biosurveillance information among health care providers and public health authorities.
>
> The HITSP Electronic Health Record ("EHR") Interoperability Specification details specific standards to support the interoperability between electronic health records and laboratory systems and secure access to laboratory results and interpretations in a patient-centric manner.
>
> The HITSP Consumer Empowerment Interoperability Specification identifies the standards needed for patients to exchange data with their caregivers. *Id.*

[66] Press Release, Certification Commission for Healthcare Information Technology, CCHIT Awarded HHS Contract for Health IT Product Certification: Collaborative Certification Effort Gains Funding, Momentum (Oct. 6, 2005), *available at* http://www.cchit.org/media/press+releases/CCHIT+Awarded+HHS+Contract+for+Health+IT+Product+Certification.htm.

[67] *Id.*

[68] Press Release, Certification Commission for Healthcare Information Technology, Certification Commission Announces New Certified Products (Apr. 30, 2007), *available at* http://www.cchit.org/about/news/releases/Certification-Commission-Announces-New-

CCHIT has published over 200 criteria, all of which must be met in order to achieve CCHIT Certified[SM] status.[69] These criteria "ensure that products provide a broad foundation of functionality, will evolve to be interoperable with other systems, and include security features that protect the privacy of personal health information."[70]

C. PRIVACY AND SECURITY SOLUTIONS–RTI INTERNATIONAL

The third HHS contract was awarded to RTI International ("RTI"). RTI contracted "to work with the Office of the National Coordinator for Health Information Technology (ONC) and the Agency for Healthcare Research and Quality (AHRQ) to identify best practices and develop solutions to overcome variances in laws and business practices that prevent the nationwide sharing of electronic health information."[71] The eighteen month contract calls for the formation of the Health Information Security and Privacy Collaboration ("HISPC"), which will "help assess and develop plans to address variations in organization-level business policies and state laws that affect privacy and security practices that may pose challenges to interoperable health information exchange."[72]

In August 2006, thirty-three states and Puerto Rico subcontracted with RTI and the HISPC project "to address privacy and security policy questions affecting interoperable health information

---

Certified-Products.asp. For more information on Certified Electronic Health Products, see also Press Release, Certification Commission for Healthcare Information Technology, CCHIT Announces New Certified Electronic Health Products (Oct. 23, 2006), *available at* http://www.cchit.org/media/press+releases/CCHIT+Announces+New+Certified+Electronic+Health+Record+Products.htm.

[69] *Id.*

[70] Press Release, Certification Commission for Healthcare Information, CCHIT Announces First Certified Electronic Health Record Products (July 18, 2006), *available at* http://www.cchit.org/media/press+releases/CCHIT+Announces+First+Certified+Electronic+Health+Record+Products.htm.

[71] Press Release, RTI International, RTI International to Support National Health Information Security and Privacy Collaboration ("HISPC") (Oct. 12, 2005) [hereinafter *RTI to Support HISPC*], *available at* http://www.rti.org/newsroom/news.cfm?nav=92&objectid=0AD0F1AC-B38F-4286-92481FDE5E224511.

[72] *Id.* The HISPC consists of privacy, security law, and health care management experts, the National Governors Association, and state governments. *Id.*

exchange."[73] These states were responsible for "bringing together a broad range of stakeholders to develop consensus-based solutions to problematic variations in privacy and security business policies, practices and state laws within their states."[74] RTI announced the completion of three final reports submitted to AHRQ and ONC on August 1, 2007.[75]

D. DEVELOPMENT OF A NATIONWIDE HEALTH INFORMATION NETWORK PROTOTYPE–ACCENTURE, CSC, IBM, AND NORTHROP GRUMMAN

On November 10, 2005, HHS awarded a fourth contract. This contract was awarded to "four groups of health care and health information technology organizations to develop prototypes for a Nationwide Health Information Network (NHIN) architecture."[76] The contract designated Accenture, Computer Science Corporation

---

[73] Press Release, RTI International, 34 States, Territories Join National Health Information Security and Privacy Collaboration (Aug. 2, 2006) [hereinafter *34 States Join HISPC*], *available at* http://www.rti.org/page.cfm?objectid=BCE53731-9277-4FF2-B3A70BBBAB6B1E82. The participants include: Alaska, Arkansas, Arizona, California, Colorado, Connecticut, Florida, Iowa, Illinois, Indiana, Kansas, Kentucky, Louisiana, Massachusetts, Maine, Michigan, Minnesota, Mississippi, New Hampshire, New Jersey, New Mexico, North Carolina, New York, Ohio, Oklahoma, Oregon, Rhode Island, Utah, Vermont, Washington, Wisconsin, West Virginia, Wyoming, and Puerto Rico. *Id.*

[74] *Id.*

[75] Press Release, RTI International, States and Territories Begin to Reduce Challenges to Electronic Health Information Exchange (Aug. 1, 2007). *See id.* for summary of the reports. Links to the three reports are available on RTI's website:

- Final Assessment of Variations and Analysis of Solutions, *available at* http://www.rti.org/pubs/ avas.pdf.
- Final Implementation Plan Report, *available at* http://www.rti.org/pubs/final_implementation_plans.pdf.
- NATIONWIDE SUMMARY REPORT, PRIVACY AND SECURITY SOLUTIONS FOR INTEROPERABLE HEALTH INFORMATION EXCHANGE, (2007) *available at* http://www.rti.org/pubs/nationwide_ summary.pdf.

[76] Press Release, Department of Health and Human Services, HHS Awards Contract to Develop Nationwide Health Information Network (Nov. 10, 2005), *available at* http://www.hhs.gov/news/press/2005pres/20051110.html.

("CSC"), International Business Machines ("IBM"), and Northrop Grumman to each lead a consortium that consisted of "a partnership between technology developers and health care providers in three health care markets."[77] The contract gave each group one year to "develop an architecture and prototype network for secure information sharing," and the groups were to "ensure that information [could] move seamlessly between each of the four networks to be developed."[78] In June 2006, each consortium presented its initial approach to NHIN architecture at the First Nationwide Health Information Network Forum: Functional Requirements.[79]

---

[77] *Id.* These consortia are:

- Accenture, working with Apelon, Cisco, CGI-AMS, Creative Computing Solutions, eTech Security Pro, Intellithought, Lucent Glow, Oakland Consulting Group, Oracle, and Quovadx. This group will work with the following health market areas: Eastern Kentucky Regional Health Community (Kentucky); CareSpark (Tennessee); and West Virginia eHealth Initiative (West Virginia).

- CSC, working with Browsersoft, Business Networks International, Center for Information Technology Leadership, Connecting for Health, DB Consulting Group, eHealth Initiative, Electronic Health Record Vendors Association, Microsoft, Regenstrief Institute, SiloSmashers, and Sun Microsystems. This group will work with the following health market areas: Indiana Health Information Exchange (Indiana); MA-SHARE (Massachusetts); and Mendocino HRE (California).

- IBM, working with Argosy Omnimedia, Business Innovation, Cisco, HMS Technologies, IDL Solutions, Ingenium, and VICCS. This group will work with the following health market areas: Taconic Health Information Network and Community (New York); North Carolina Healthcare Information and Communications Alliance (Research Triangle, North Carolina); and North Carolina Healthcare Information and Communications Alliance (Rockingham County, North Carolina).

- Northrop Grumman, working with Air Commander, Axolotl, Client/Server Software Solutions, First Consulting Group, SphereCom Enterprises, and WebMD. This group will work with the following health market areas: Santa Cruz RHIO (Santa Cruz, California); and HealthBridge (Cincinnati, Ohio); University Hospitals Health System (Cleveland, Ohio). *Id.*

[78] *Id.*

[79] The agenda for this First Nationwide Health Information Network Forum is available at http://www.hhs.gov/healthit/nhin/forum_june2006.html (last visited Jan. 22, 2008). Each consortia's presentation is also provided:

- Accenture, http://www.hhs.gov/healthit/documents/AccenturePresentation.pdf (last visited Jan. 22, 2008)

- CSC, http://www.hhs.gov/healthit/documents/CSCForumslides.pdf (last visited Jan. 22, 2008)

IBM announced the completion of its NHIN technology in a January 2007 press release.[80] The technology, which is a "standards-based system, based on a service oriented architecture (SOA) to connect information," allows for "secure access to healthcare data and real time information sharing and exchange of healthcare data among physicians, patients, hospitals, laboratories, and pharmacies, regardless of where the medical data is located."[81] All four consortia presented their final architectures in January 2007 at the Third Annual Nationwide Health Information Network Forum in Washington, D.C.[82]

2. HHS' NEXT STEPS IN NATIONWIDE HEALTH INFORMATION NETWORKS

In December 2006, HHS announced its support of trial NHIN implementations.[83] Through this next step, HHS intends to produce a "network of networks" by using the "technical expertise that the consortia developed . . . together with state and regional information exchanges . . . to knit together these different exchanges into an NHIN."[84] John Loonsk, ONC director of interoperability and

---

- IBM, http://www.hhs.gov/healthit/documents/IBM_NHIN_Forum.pdf (last visited Jan. 22, 2008)

- Northrop Grumman, http://www.hhs.gov/healthit/documents/NGC_NHIN_Forum.pdf (last visited Jan. 22, 2008).

[80] Press Release, IBM, IBM Propels Nationwide Health Information Network (Jan. 23, 2007), *available at* http://www-03.ibm.com/press/us/en/pressrelease/20955.wss.

[81] *Id.*

[82] Press Release, Department of Health and Human Services, HHS Advances Nationwide Health Information Network Initiative (Dec. 8, 2006), *available at* http://www.hhs.gov/news/press/2006pres/20061208.html. Summaries of the consortia's prototype demonstrations and links to their presentations introducing the prototype demonstrations are available at http://www.hhs.gov/healthit/healthnetwork/forum_jan2007.html (last visited Jan. 22, 2008). *See also* WES RISHEL, VIRGINIA RIEHL & CATHLEEN BLANTON (GARTNER, INC.), SUMMARY OF THE NHIN PROTOTYPE ARCHITECTURE CONTRACTS: A REPORT FOR THE OFFICE OF THE NATIONAL COORDINATOR FOR HEALTH IT (2007), http://www.hhs.gov/healthit/healthnetwork/resources/summary_report_on_nhin_Prototype_architectures.pdf.

[83] *Id.*

[84] Heather Havenstein, *Q&A: U.S. Health IT Exec Details 'Trial' Nationwide Networks*, COMPUTERWORLD GOV'T, Dec. 12, 2006, *available at* http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9005875.

standards, notes that a potential challenge, however, will be "ensur[ing] the secure exchange of data."[85]

B. GAO'S ASSESSMENT OF HHS AND ITS IT AND PRIVACY EFFORTS

The U.S. Government Accountability Office ("GAO"), in a February 2006 report, found several weaknesses in HHS, specifically the Centers for Medicare and Medicaid's ("CMS") information security controls.[86] Some of the weaknesses cited included: inconsistent electronic access controls to sensitive data; electronic access control vulnerabilities to computer networks; and poor controls for "physically secure[ing] computer resources, conduct[ing] suitable background investigations, segregat[ing] duties appropriately, and prevent[ing] unauthorized changes to application software."[87]

The GAO report identifies a lack of program implementation as the reason for inadequate information security.[88] The information security elements not implemented were "related to (1) risk assessments, (2) policies and procedures, (3) security plans, (4) security awareness and training, (5) tests and evaluations of control effectiveness, (6) remedial actions, (7) incident handling, and (8) continuity of operations plans."[89] As a result of the study, GAO recommended full implementation of HHS' information security program.[90]

In September 2006, the Workforce Subcommittee of the House Government Reform Committee requested GAO to provide an assessment of the HHS' health information technology efforts.[91]

---

[85] *Id.*

[86] GAO Report to the Chairman, Committee on Finance, U.S. Senate, *Information Security: Department of Health and Human Services Needs to Fully Implement Its Program*, GAO-06-267 (Feb. 2006) [hereinafter *Information Security*].

[87] *Id.* at 2–3.

[88] *Id.*

[89] *Id.*

[90] *Id.*

[91] David A. Powner, Health Information Technology: HHS is Continuing Efforts to Define Its National Strategy, Testimony Before the House Subcomm. on Federal Workforce and Agency Organization, Comm. on Gov't Reform, GAO Report No. GAO-06-1071T at 2–3 (Sept. 11, 2006), *available at* http://www.gao.gov/new.items/d061071t.pdf.

David Powner noted several of HHS' achievements in his testimony before the Federal Workforce and Agency Organization Subcommittee, including: the creation of certification criteria for ambulatory electronic health record and resultant certification of vendors; selection of ninety interoperability standards; and workgroup formation to "address confidentiality and security issues relevant to a nationwide health information exchange."[92] Powner is concerned, however, that "while HHS has made progress in these areas, it still lacks detailed plans, milestones, and performance measures for meeting the President's goals."[93]

The GAO echoed this concern in a written statement by Linda D. Koontz, Director of Information Management Issues, and Valerie C. Melvin, Director of Human Capital and Management Information Systems Issues.[94] Koontz and Melvin stated that "HHS's approach for addressing privacy and security did not address elements that should be included in a comprehensive privacy approach, such as milestones for integration, identification of the entity responsible for integrating the outcomes of privacy-related initiatives, and plans to address key privacy principles and challenges."[95] Commentators note that "[t]he [GAO] reports underscore the difficulties HHS faces with its ambitious plans to revamp healthcare through broader use of

---

[92] *Id.*

[93] *Id.*

[94] Linda D. Koontz & Valerie C. Melvin, *Health Information Technology: Efforts Continue but Comprehensive Privacy Approach Needed for National Strategy*: Testimony Before the House Subcomm. on Information Policy, Census, and National Archives, Comm. on Oversight and Gov't Reform, GAO Report No. GAO-07-988T (June 19, 2007), *available at* http://www.gao.gov/cgi-bin/getrpt?GAO-07-988T.

[95] *Id.* at 4. For additional GAO reports on HHS's HIT and privacy efforts, see U.S.Gov't Accountability Office, *Health Information Technology: Early Efforts Initiated but Comprehensive Privacy Approach Needed for National Strategy*. GAO REPORT NO. GAO-07-238 (Jan. 2007), *available at* http://www.gao.gov/new.items/d07238.pdf; Linda D. Koontz & David A. Powner, *Health Information Technology: Early Efforts Initiated but Comprehensive Privacy Approach Needed for National Strategy*, Testimony Before the Senate Subcomm. on Oversight of Government Management, the Federal Workforce, and the District of Columbia, Comm. on Homeland Security and Governmental Affairs (Feb. 1, 2007), *available at* http://www.gao.gov/new.items/d07400t.pdf; U.S. Gov't Accountability Office, *Information Security: Dept. of Health and Human Services Needs to Fully Implement Its Program*, GAO REPORT NO. GAO-06-267, *available at* http://www.gao.gov/new.items/d06267.pdf (last visited Jan. 22, 2008).

technology, improved efficiency and more transparency, but while not necessarily dictating how the plans should work."[96]

Further evidence of HHS's lack of progress manifested itself in late February 2007 with the resignation of Paul Feldman, co-chair of the American Health Information Community ("AHIC"), a workgroup that provides recommendations to HITSP in its development of standards.[97] According to Feldman "[AHIC's] efforts to establish standards for the nation's developing healthcare IT network, are 'a far cry from a comprehensive and timely approach that would give privacy policy equal and necessary footing with interoperability and systems development efforts.'"[98]

C. HIT LEGISLATION LEFT PENDING BY THE 109TH CONGRESS

The 109th Congress introduced several bills related to health information technology,[99] but none were reconciled or passed before the end of the term. The most promising bills were Senate Bill 1418, Wired for Health Care Quality Act of 2005, and House Bill 4157, Health Information Technology Promotion Act of 2006. This section summarizes a few of the key provisions of these bills.

---

[96] Andis Robeznieckes & Joseph Conn, *GAO Blasts HHS on IT, Privacy*, MODERN HEALTHCARE, Sept. 11, 2006, at 8.

[97] Diana Manos, *Privacy Advocate Quits AHIC Workgroup*, HEALTHCARE IT NEWS, Mar. 1, 2007, *available at* http://www.healthcareitnews.com/story.cms?id=6553. *See* section 1A *supra* of Part III of this article for a brief discussion of HITSP. For background information on AHIC, see U.S. Dep't of Health and Human Services, *American Health Information Community*, http://www.hhs.gov/healthit/community/background/ (last visited Jan. 22, 2008).

[98] Manos, *supra* note 97. *See also* Todd Sloane, *Privacy Could Be IT Standards' Deal-Breaker*, MODERN HEALTHCARE, Mar. 9, 2007, http://www.modernhealthcare.com/apps/pbcs.dll/article?AID=/20070309/FREE/70308003/0/FRONTPAGE. For a copy of Mr. Feldman's resignation letter, co-signed by Janlori Goldman, Director of the Health Privacy Project (HPP), see Letter from Janlori Goldman, Director, HPP & Paul Feldman, Deputy Director, HPP, to Robert Kolodner, M.D., Interim Nat'l Coordinator for Health Info. Tech., Dep't of Health and Human Services, *available at* http://www.healthprivacy.org/info-url_nocat2303/info-url_nocat_show.htm?doc_id=465343.

[99] *See* John Monroe, *Kennedy to Introduce Personal Health Records Bill*, GOV'T HEALTH IT, Sept. 26, 2006, http://govhealthit.com/article96235-09-26-06-Web; *see also* Nancy Ferris, *House Subcommittee Passes Bill on EHRs for Feds*, GOV'T HEALTH IT, Sept. 14, 2006, http://govhealthit.com/article96068-09-14-06-Web.

1. WIRED FOR HEALTH CARE QUALITY ACT OF 2005

The Wired for Health Care Quality Act of 2005 ("WHCQ Act"), sponsored by Senator Michael B. Enzi (R-WY), "[establishes] the Office of the National Coordinator of Health Information Technology to coordinate . . . and oversee [the development of] a nationwide interoperable health information technology infrastructure."[100] WHCQ was passed in the Senate, as amended, on November 18, 2005 and referred to the House Subcommittee on Health in December 2005.[101]

The WHCQ Act provides the National Coordinator with several responsibilities, requiring the National Coordinator to:

1. serve as the principal advisor to the Secretary of Health and Human Services (the Secretary) concerning the development, application, and use of health information technology and to coordinate and oversee the health information technology programs of the Department of Health and Human Services (HHS);

2. facilitate the adoption of a nationwide, interoperable system for the electronic exchange of health information;

3. ensure the adoption and implementation of standards for such exchange.[102]

The WHCQ Act also requires the HHS Secretary to:

- establish the public-private American Health Information Collaborative to:

    1. advise the Secretary and recommend actions to achieve a nationwide interoperable health information technology infrastructure;

---

[100] Wired for Health Care Quality Act of 2005, S. 1418, 109th Cong., 1st Sess. (2005), CRS Summary, http://thomas.loc.gov/cgi-bin/bdquery/z?d109:SN01418:@@@D&summ2=m&.

[101] *Id.*

[102] *Id.*

2. serve as a forum for the participation of a broad range of stakeholders to provide input on achieving the interoperability of health information technology; and

3. recommend standards for the electronic exchange of health information by the federal government and private entities.

- develop criteria to:

1. ensure uniform and consistent implementation of any standards voluntarily adopted by private entities; and

2. ensure and certify hardware, software, and support services compliance with applicable adopted standards.

- develop measures of the quality of care patients receive and ensure that such measures:

1. are evidence-based, reliable, and valid;

2. are consistent with the purposes of developing a nationwide interoperable health information technology infrastructure;

3. include measures of clinical processes and outcomes, patient experience, efficiency, and equity; and

4. include measures of overuse and underuse of health care items and services.

- carry out a study that examines the impact that variations among state laws relating to licensure, registration, and certification of medical professionals have on the secure electronic exchange of health information.[103]

---

[103] *Id.*

2. HEALTH INFORMATION TECHNOLOGY PROMOTION ACT OF 2006

Similar to the WHCQ Act, the Health Information Technology Promotion Act of 2006 ("HITP Act") "[e]stablishes within the HHS an Office of the National Coordinator for Health Information Technology."[104] Representative Nancy L. Johnson (R-CT) introduced the HITP Act, and the bill passed the House, as amended, on July 27, 2006.[105]

The HITP Act permits the HHS Secretary to:

- study and report to Congress on the impact of variation and commonality in state laws, as well as current federal standards, for security and confidentiality upon the timely exchange of health information in order to ensure the availability of information necessary to make medical decisions at the location in which the medical care is provided.[106]

The HITP Act also instructs the National Coordinator to:

- provide for a strategic plan for nationwide implementation of interoperable health information technology in both the public and private health care sectors; and

- collaborate with the Agency for Healthcare Research and Quality and the Health Services Resources Administration and other federal agencies to support technical assistance and resource development for such medically underserved communities, particularly those seeking to establish electronic health information networks across providers.[107]

---

[104] Health Information Technology Promotion Act of 2006, H.R. 4157, 109th Cong., 2d Sess. (2006), CRS Summary, *available at* http://thomas.loc.gov/cgi-bin/bdquery/z?d109:HR04157:@@@D&summ2=m& [hereinafter *H.R. 4157 CRS Summary*].

[105] *Id.*

[106] *Id.*

[107] *Id.*

This Act also "amends [the Social Security Act] title XI to create safe harbors from civil and criminal penalties in current anti-kickback laws for providing certain health information technology and training services."[108]

It is important to note that the version of the bill passed by the House emphasizes the fact that "nothing in [the HITP] Act shall be construed to affect the scope, substance, or applicability of the Health Insurance Portability and Accountability Act of 1996 (HIPAA, or HIPPA [sic]) and any related regulation regarding the privacy of individually identifiable health information, particularly the non-preemption of more stringent state law."[109]

3. TRANSITION TO THE 110TH CONGRESS

As predicted, the House and Senate were unable to reconcile the bills before the 2006 mid-term elections.[110] As one commentator noted, "[a]mong issues that might get left behind or pushed into the 110th Congress are a Medicare physician fee adjustment, health IT legislation, reauthorization of the Magnuson-Stevens fisheries law and the Water Resources Development Act and an attempt to overhaul the United States Postal Service."[111] An interesting possible outcome that follows from the lack of performance by Congress is that CMS may "pursue new forms of administrative action to advance the [health IT] field."[112]

In addition, while the 110th Congress includes HIT on their agenda, it was not a part of the legislation voted on by the House of

---

[108] *Id.*

[109] *Id.*

[110] *Capitol Hill Watch: Prospect for Passage of Final Health Care Information Technology Bill Uncertain*, KAISERNETWORK.ORG (DAILY HEALTH POLICY REPORT), Sept. 12, 2006, http://www.kaisernetwork.org/daily_reports/rep_index.cfm?hint=3&DR_ID=39758.

[111] Martin Vaughan**,** *Lame Duck: List is Long, Time is Short*, NATIONAL J. CONGRESSDAILY, Nov. 13, 2006.

[112] John Reichard, *Acting CMS Head Promotes Health Information Technology: Leslie Norwalk, Style and Substance*, CQ HEALTHBEAT NEWS, November 1, 2006, *available at* http://coburn.senate.gov/ffm/index.cfm?FuseAction=LatestNews.NewsStories&ContentRecord_id=a9c02d9f-802a-23ad-469e-b019da2ebcb3 (quoting Leslie Norwalk, CMS Acting Administrator).

Representatives' first 100 legislative hours.[113] President Bush, however, mentioned HIT for the fourth consecutive year in his State of the Union address on January 23, 2007, stating, "we need to reduce costs and medical errors with better information technology."[114] Therefore, this is an indication that President Bush is still giving high priority to HIT.

As of early August 2007, the Senate does seem to be moving forward with HIT legislation. Another version of the Wired for Health Care Quality Act (Senate Bill 1693) was introduced by Senator Edward E. Kennedy (D-MA) on June 26, 2007.[115] A substitute bill was reported in the Senate and placed on the Senate Legislative Calendar on August 1, 2007, by the Committee on Health, Education, Labor, and Pensions.[116]

Senate Bill 1693 seeks to support the adoption of health information technology by:

- codifying the establishment and the responsibilities the Office of the National Coordinator for Health Information Technology (ONCHIT), the American Health Information Community (AHIC), and the Partnership for Health Care Improvement;

- requiring the development of a Health Information Technology Resource Center to provide technical assistance and develop best practices to support adoption of interoperable health information technology;

- authorizing grants to promote the widespread adoption of interoperable health information technology; and

---

[113] *See* Christopher Lee, *Shift in Congress Puts Health Care Back on the Table*, WASH. POST, Dec. 25, 2006, A12, *available at* http://www.washingtonpost.com/wp-dyn/content/article/2006/12/24/AR2006122400589.html; *see also* Speaker Nancy Pelosi's Web site, http://www.speaker.gov/legislation/clock (last visited Jan. 22, 2008), for an overview of the legislation passed by the 110th Congress in its first 100 hours.

[114] *President's State of the Union Address is a Home Run for Harnessing Information Technology to Transform Healthcare*, HIMSS NEWS, Jan. 24, 2007, *available at* http://www.himss.org/ASP/ContentRedirector.asp?ContentId=66451&type=HIMSSNewsItem.

[115] Wired for Health Care Quality Act, S. 1693, 110th Cong., 1st Sess. (2007).

[116] *Id.*

- deeming an operator of a health information electronic database to be a covered entity under HIPAA.[117]

D. FEDERAL PRIVACY PREEMPTION

A discussion on the national push for health information technology must also consider the issue of federal preemption of state privacy laws. This section will provide a brief overview of HIPAA preemption and then discuss federal privacy preemption in the context of health information technology legislation.

1. HIPAA PREEMPTION OVERVIEW

The Privacy Rule was meant to provide a federal floor of privacy standards. 45 C.F.R. § 160.203 states, "[a] standard, requirement, or implementation specification adopted under this subchapter that is contrary to a provision of State law preempts the provision of State law."[118] An exception to this rule applies, however, when a "provision of State law relates to the privacy of individually identifiable health information and is more stringent than a [HIPAA] standard, requirement, or implementation specification."[119] Therefore, "any provision of state law that 'relates' to the privacy of health information and is both 'contrary' to, and is 'more stringent' than, a provision of HIPAA will not be preempted by HIPAA."[120]

To state it another way, "[HIPAA] specifically empowered states to keep or pass their own privacy laws if they contained more stringent privacy protections."[121] This issue of preemption, or lack of preemption, becomes of particular concern when discussing the framework necessary for national, interoperable HIT, because states have varying levels of privacy protection.

---

[117] CONGRESSIONAL BUDGET OFFICE, COST ESTIMATE: S. 1693 WIRED FOR HEALTH CARE QUALITY ACT (2007), *available at* http://www.cbo.gov/ftpdocs/84xx/doc8457/s1693.pdf.

[118] 45 C.F.R. § 160.203 (2006).

[119] 45 C.F.R. § 160.203(b) (2006).

[120] Christopher C. Gallagher, *Health Information Privacy: The Federal Floor's States Elevator*, Glasser LegalWorks Conference "HIPAA Privacy Compliance," July 25, 2001, Washington, D.C., Sept. 20–21, Chicago, Illinois, *available at* http://www.gcglaw.com/resources/healthcare/healthprivacy.pdf (emphasis in original).

[121] Joseph Conn, *HIPAA, 10 Years After*, MODERN HEALTHCARE, Aug. 7, 2006 at 26.

2. HEALTH INFORMATION TECHNOLOGY LEGISLATION AND PREEMPTION

The debate concerning federal preemption of state privacy law was highlighted when "[e]arlier versions of the [HITP Act] contained a provision that would have, in effect, modified HIPAA by authorizing the HHS secretary to pre-empt any state privacy laws deemed as barriers to interoperability [of HIT]."[122] This provision was of major concern because HIPAA does not differentiate between "the type and sensitivity of health information . . . , [while states] demand more rigorous protection of certain types of medical data, including information about genetics, mental health, substance abuse and developmental disabilities."[123] However, after much outcry by privacy advocates, the preemption provision was removed from the final version, which passed in the House on June 27, 2006.[124]

Still, HHS is attempting to alleviate the problem of varying levels of privacy protection through its contract with, and resulting study by, RTI. [125] Using the results of its study, RTI is "develop[ing] solutions to overcome variances in laws and business practices that prevent the nationwide sharing of electronic health information."[126]

Privacy advocates still argue, however, "that state laws that have protections not included in federal statutes should be preserved—and not immediately pre-empted—to facilitate the exchange of electronic

---

[122] *Id.*

[123] John Pulley, *Untying the Privacy Knot*, GOV'T HEALTH IT, Aug. 14, 2006, http://www.govhealthit.com/print/3_17/features/95583-1.html. Pulley notes that there is an exception under HIPAA for psychotherapy notes. *See also* National Association of Social Workers, *Federal Legislation Threatens Health Care Privacy Rights*, June 20, 2006, http://www.socialworkers.org/advocacy/alerts/2006/062006.asp:

> H.R. 4157 profoundly undermines current patient privacy rights, such as state social worker-patient confidentiality and privilege laws, without providing any new federal protections. Preemption of state and local privacy laws is strongly opposed by NASW and other advocates of health privacy rights because it eliminates critical privacy laws that protect patient/therapist confidentiality and other key protections, without ensuring their replacement by strong federal privacy protections . . . .

[124] Conn, *supra* note 121; *see also H.R. 4157 CRS Summary*, *supra* note 104.

[125] *RTI to Support HISPC*, *supra* note 71.

[126] *Id.*

medical records."[127] Similarly, other privacy advocates believe that "without basic privacy protections built into the legislation up front, Congress will create an electronic superhighway system for others to misuse, data mine and steal the nation's medical records."[128]

IV. CONCLUSION

The efforts to improve the effectiveness and efficiency of health care through health information technology are increasing. Familiarity and compliance with the Privacy Rule adds to the likelihood that electronic health records and a nationwide health information network will be successful. But the use of this health information technology to improve health care will only be effective if the individually identifiable health information contained in electronic health records can remain secure. As a result, the HIPAA Privacy Rule and state privacy laws have a large impact on the implementation of HIT.

---

[127] Pulley, *supra* note 123 (citing Janlori Goldman).

[128] Monya L. Baker, *House Passes Health IT Bill*, EWEEK.COM, July 28, 2006, http://www.eweek.com/article2/0,1895,1995791,00.asp (citing Deborah Peel, chairman of the Patient Privacy Rights Foundation).