Pandora's Box: Can HIPAA Still Protect Patient Privacy Under a National Health Care Information Network?

Sean T. McLaughlin*

TABLE OF CONTENTS

I. INTRODUCTION 30
II. ELECTRONIC HEALTH RECORDS AND MOMENTUM TOWARD A NATIONAL HEALTH CARE INFORMATION NETWORK 32
III. THE COMPUTER NETWORK CONCEPT 35
IV. HIPAA AND CREATING A SUCCESSFUL NHIN FRAMEWORK 37
A. *HIPAA's Privacy Rule* 39
1. Protected Health Information 39
2. Covered Entities 40
3. Business Associates 43
4. Authorization and Treatment, Payment, and Health Care Operations 44
6. The "Minimum Necessary" Standard 47
7. Patient Rights 49
a. Individual Right to PHI Access 50
b. Individual Right to PHI Amendments 51
c. Individual Right to PHI Accounting and Restrictions 52
8. HIPAA Preemption and State Medical Privacy Law 53
B. *HIPAA's Security Rule* 55
1. Administrative Safeguards 56
2. Physical and Technical Safeguards 58
V. CONCLUSION 60

*. J.D., Notre Dame Law School. In addition to academic mentors past and present, the author would like to thank Mr. Mike Piper, Mrs. Cheri Dolezal, Mr. Jerry Dolezal, and Mr. Ron Curtin for providing the opportunity to make this article possible.

I. INTRODUCTION

In an attempt to address the rising costs of health care,[1] the Bush administration seeks to fully usher American medicine into the digital age.[2] The Federal Health Architecture[3] is currently coordinating its practice toward electronic health care.[4] Serving as models for the private sector, the U.S. Department of Defense and Veteran's Administration both continue to develop policies and procedures to safeguard electronic medical privacy and security.[5] Most importantly, the U.S. Department of Health and Human Services ("HHS") has laid the foundation for a national health care information network.[6]

---

1. The Office of the Actuary at the Centers for Medicare and Medicaid Services estimates that yearly U.S. health care costs will reach $3.4 trillion dollars by 2013. Growing at an annual rate of 7.3%, health care expenditures will ultimately account for 18.4% of the nation's gross domestic product. *See* CENTERS FOR MEDICARE AND MEDICAID SERVICES, NATIONAL HEALTH CARE EXPENDITURE PROJECTIONS: 2002-2013 (2005), http://www.cms.hhs.gov/NationalHealthExpendData/downloads/nheprojections2003-2013.pdf.

2. *See* President George W. Bush, Address Before a Joint Session of the Congress on the State of the Union (Jan. 31, 2006) 42 Weekly Comp. Pres. Doc 5 ("We will make wider use of electronic records and other health information technology, to help control costs and reduce dangerous medical errors"). *See generally* Mike Allen, *Bush Touts Plan for Electronic Medicine*, WASH. POST, May 28, 2004, at A08 (reporting on electronic health care innovation as a centerpiece in President Bush's 2004 re-election campaign). *See generally* TRANSFORMING HEALTH CARE: THE PRESIDENT'S HEALTH INFORMATION TECHNOLOGY PLAN (2004), http://www.whitehouse.gov/infocus/technology/economic_policy200404/chap3.html [hereinafter PRESIDENT BUSH'S HEALTH INFORMATION TECHNOLOGY PLAN].

3. The Federal Health Architecture, led by the Department of Health and Human Services, the Department of Defense, and the Department of Veterans Affairs, includes 35 administrative offices and agencies. *See* United States Dep't of Health and Human Services: Federal Health Architecture, http://www.hhs.gov/fedhealtharch/members.html (last visited Oct. 7, 2006).

4. *See* DEPARTMENT OF HEALTH AND HUMAN SERVICES, THE DECADE OF HEALTH INFORMATION TECHNOLOGY: DELIVERING CONSUMER-CENTRIC AND INFORMATION-RICH HEALTH CARE 37-38 (July 2004), http://www.hhs.gov/healthit/documents/hitframework.pdf [hereinafter HHS REPORT].

5. This inter-agency effort is part of the Coordinated Health Infomatics (CHI). CHI continues to formulate a broad strategy to standardize data, communications, security, and health information systems throughout the federal government. *See id.* at 15, 19. "Outside of HHS, the Department of Veterans Affairs (VA) and the Department of Defense (DOD) are considered by experts to be leaders in the use of health IT, particularly in the adoption of EHR systems for their constituents." GENERAL ACCOUNTING OFFICE, HHS'S EFFORTS TO PROMOTE HEALTH INFORMATION TECHNOLOGY & LEGAL BARRIERS TO ITS ADOPTION, n.3 (Aug. 13, 2004), http://www.gao.gov/atext/d04991r.pdf [hereinafter GAO REPORT].

6. *See* Request for Information (RFI), 69 Fed. Reg. 65,599 (Nov. 15, 2004) (evaluating the legal and regulatory viability of President Bush's proposal); *See also* DEP'T OF HEALTH & HUMAN SERV., SUMMARY OF NATIONWIDE HEALTH INFORMATION NETWORK (NHIN) REQUEST FOR INFORMATION RESPONSES (RFI) (June 2005), http://www.hhs.gov/healthit/rfisummaryreport.pdf [hereinafter HHS RFI] (highlighting feedback received regarding a variety of issues pertaining to

Establishing a national health care information network continues to build momentum within Congress. Members of the U.S. Senate[7] and U.S. House of Representatives[8] recently introduced bi-partisan legislation empowering HHS to fund pilot projects. Both bills provide for regional grants that encourage increased use of electronic medical records. Each includes financial incentives to develop experimental computer networks capable of securely and efficiently exchanging electronic health care information.[9]

Ideally, a nationally accessible network will allow the health care industry to improve efficiency and quality, while reducing costs and errors.[10] Yet, the decisions facing the Bush administration in devising and implementing the network will have profound implications for how U.S. health care functions in the 21st century. To succeed in digitalizing American medicine, the Bush administration must first inspire the trust and confidence of lawmakers, patients, and other health care participants.[11] While providing participatory incentives to the health care industry, the federal government also needs to vigilantly protect individual privacy against foreseeable abuse and threats. Specifically, any national health care network must adhere to medical privacy and security protections mandated under the "Health Insurance Portability and Accountability Act" ("HIPAA").[12]

---

network development, including viability, structure, governance, security, and patient privacy). *See generally* HHS REPORT, *supra* note 4.

7. *See* Health Technology to Enhance Quality Act of 2005, S. 1262, 151 CONG. REC. 80, S6752-54 (daily ed. June 16, 2005) (introduced by Senate Majority Leader William H. Frist (R-TN) and Sen. Hillary Clinton (D-NY)). *See also* Wired for Health Care Quality Act, S. 1418, 151 CONG. REC. 97, S8420-26 (daily ed. July 18, 2005) (directing the HHS Secretary to establish the public-private "American Health Information Collaborative" in order to collect input regarding network feasibility, develop security standards, and recommend specific actions for implementation).

8. *See* 21st Century Health Information Act of 2005, H.R. 2234, 151 CONG. REC. 60, H3112 (daily ed. May 10, 2005) (introduced by Rep. Tim Murphy (R-PA) and Rep. Patrick Kennedy (D-RI)). *See also* National Health Information Incentive Act of 2005, H.R 747, 151 CONG. REC. 14, H581-82 (daily ed. Feb. 10, 2005) (directing the HHS Secretary to develop pilot programs to test safety and security standards for nation-wide electronic health information use and exchange).

9. *See generally* H.R. 2234, 109th Cong. § 3 (2005); S. 1262, 109th Cong. § 2906, 2908 (2005).

10. *See* Sen. William H. Frist, *Why We Must Invest in Electronic Medical Records*, S.F. CHRONICLE, July 24, 2005, at C-5. *See generally* PRESIDENT BUSH'S HEALTH INFORMATION TECHNOLOGY PLAN, *supra* note 2; HHS REPORT, *supra* note 4.

11. Events such as the recent theft of 26.5 million Americans' personal information from the Veteran's Administration can only make this task increasingly difficult. *See* Christopher Lee & Steve Vogel, *Personal Data on Veterans is Stolen*, WASH. POST, May 23, 2006, at A01.

12. Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (1997) [hereinafter HIPAA] (codified as amended in various sections of 42 U.S.C.) . While the federal government has enacted privacy protections regarding substance abuse records, HIPAA is the first federal statute specifically pertaining to a patient's entire medical history. *See* 42 U.S.C. § 290dd-2 (1994); S*ee generally* Freedom of Information Act of 1966, 5 U.S.C. §§ 552(b)(1)-(3) & (6) (1988); Privacy Act of 1974, 5 U.S.C. § 552a (1994); Americans with

While criticism of HIPAA's legality and effectiveness[13] may serve a vital function in debating the best approach to safeguard medical privacy, federal involvement is here to stay.[14] A more critical issue is how HIPAA will function in an age where evolving computer technology continues to empower the rapid accumulation and dissemination of information.

This article focuses on the key medical privacy questions surrounding the Bush administration's national health care information network. Part II examines the Administration's proposal, including the adoption of electronic medical records. Part III highlights the operational technology available to network architects. Part IV details how the Bush administration should direct HHS to devise and manage the network in order to uphold and empower HIPAA's medical privacy and security regulations.

II. ELECTRONIC HEALTH RECORDS AND MOMENTUM TOWARD A NATIONAL HEALTH CARE INFORMATION NETWORK

Inconsistencies regarding non-electronic medical information continue to plague the U.S. health care system.[15] Data is routinely stored in disparate locations. Most health records often remain compartmentalized by issues pertaining to treatment, research, administration, or payment.[16] Further, transferring and utilizing non-electronic health information often proves slow, expensive, and inaccurate.[17]

In April 2004, President George W. Bush issued an executive order[18] urging the health care industry to implement and utilize electronic health records ("EHRs").[19]

Disabilities Act, 42 U.S.C. §§ 12101-213 (1994); Electronic Communications Privacy Act, 18 U.S.C. §§ 2701-2707 (2004).

13. Although too voluminous to cite in full, for a sample of recent scholarship regarding HIPAA's legality and effectiveness see infra notes 25, 55, & 198 (citations omitted).

14. *See* HHS RFI, *supra* note 6, at 12 (noting widespread opinion that the "federal government is the best candidate to facilitate a nationwide consensus and serve as an impartial convener of a broad range of stakeholders").

15. *See* Mitchelle C. Pierre, *New Technology, Old Issues: The All-Digital Hospital and Medical Information Privacy,* 56 RUTGERS L. REV. 541, 544-45 (2004). *See also* GAO REPORT (citing INSTITUTE OF MEDICINE, CROSSING THE QUALITY CHASM: A NEW HEALTH SYSTEM FOR THE 21ST CENTURY (2001)); PRESIDENT BUSH'S HEALTH INFORMATION TECHNOLOGY PLAN, *supra* note 2 ("The Institute of Medicine estimates that between 44,000 and 98,000 Americans die each year from medical errors").

16. *See id.*

17. *See id.*

18. Exec. Order No. 13,335, 69 Fed. Reg. 24,059 (Apr. 30, 2004). The Bush administration currently foresees a ten-year timeline for full EHR adoption. *See* PRESIDENT BUSH'S HEALTH INFORMATION TECHNOLOGY PLAN, *supra* note 2.

19. "An electronic health record is a digital collection of a patient's medical history and could include items like diagnosed medical conditions, prescribed medications, vital signs, immunizations, lab results, and personal characteristics like weight and age." Press Release,

Initially proposed in 1992 by the Institute of Medicine,[20] EHRs include a patient's entire medical history.[21] Allowing for convenient access and organization, EHRs should greatly enhance information accuracy and health care delivery.[22] Shifting toward electronic use and storage will also empower researchers and public health officials to more efficiently accumulate and analyze data.[23] While the protracted benefits appear to greatly outweigh transition costs,[24] utilizing EHRs also raises important patient privacy concerns.[25]

In July 2004, HHS released: *The Decade of Health Information Technology: Delivering Consumer-centric and Information-rich Health Care.*[26] To help enact President Bush's vision for twenty-first century medicine, the Department outlined four main goals: to inform clinical practice, to interconnect clinicians, to personalize health care, and to improve population health.[27] While upholding federal medical

---

Department of Health and Human Services, Secretary Leavitt Takes New Steps to Advance Health IT (June 6, 2005), http://www.hhs.gov/news/press/2005pres/20050606.html.

20. *See* Pierre, *supra* note 15, at 546-47 (citing AMITAI ETZIONI, THE LIMITS OF PRIVACY 142 (1999)).

21. *See* Press Release, *supra* note 19. *See also* PRESIDENT BUSH'S HEALTH INFORMATION TECHNOLOGY PLAN *supra* note 2; Phillip C. Butell, *The Privacy and Security of Health Information in the Electronic Environment Created by HIPAA*, 10 KAN. J.L. & PUB. POL'Y 399, 405-06 (2001); Amy M. Jurevic, *When Technology and Health Care Collide: Issues with Electronic Medical Records and Electronic Mail*, 66 UMKC L. REV. 809, 810-12 (1998).

22. *See* Press Release, *supra* note 19; PRESIDENT BUSH'S HEALTH INFORMATION TECHNOLOGY PLAN, *supra* note 2; Butell, *supra* note 21, at 405-06; Jurevic, *supra* note 21, at 810-12.

23. *See* Press Release, *supra* note 19; PRESIDENT BUSH'S HEALTH INFORMATION TECHNOLOGY PLAN, *supra* note 2; Butell, *supra* note 21, at 405-06; Jurevic, *supra* note 21, at 810-12.

24. Similar to a National Identification System, HHS's network may cost up to $30 billion to implement, and an additional $3-6 billion per year to operate. *See* Richard Sobel, *The Degradation of Political Identity Under a National Identification System*, 8 B.U. J. SCI. & TECH. L. 37, 62 (2002) (citing John J. Miller & Stephen Moore, *A National ID System: Big Brother's Solution to Illegal Immigration*, CATO POLICY ANALYSIS, No. 237, Sept. 7, 1995, http://www.cato.org/pubs/pas/pa237.html). *But see* HHS RFI, *supra* note 6, at 1 (citing Jan Walker et. al., *The Value of Health Care Information Exchange and Interoperability*, HEALTH AFFAIRS, Jan. 19, 2005, http://content.healthaffairs.org/cgi/reprint/hithaff.w5.10v1) (stating the adoption of a national health care network could reduce annual U.S. health care expenditures by nearly five percent).

25. *See* Butell, *supra* note 21, at 405-06; Jurevic, *supra* note 21, at 810-12. Some also contend that privacy anxiety impairs patient-provider relationships, treatment advances, and trust in the health care system. *See* Mike Hatch, *HIPAA: Commercial Interests Win Round Two*, 86 MINN. L. REV. 1481, 1486-90 (2002); Sharon J. Hussong, *Medical Records and Your Privacy: Developing Federal Legislation to Protect Patient Privacy Rights*, 26 AM. J.L. & MED. 453, 455-57 (2000). *See also* Gina Kolata, *When the Doctor Is In, But You Wish He Weren't*, N.Y. TIMES, Nov. 30, 2005, at A-24 (describing a growing emotional and communicative disconnect between patients and providers in the current U.S. health care system).

26. *See generally* HHS REPORT, *supra* note 4.

27. *See* HHS Report, *supra* note 4, at 1-6. This confluence of technology and health care

privacy and security standards,[28] HHS aims to eliminate current barriers of transferring electronic health care data.[29] Reiterating President Bush's directive,[30] the proposal asks the health care industry to adopt interoperable EHRs[31] and improve patient access to personal health information.[32] Most importantly, the report also anticipates a national health care information network ("NHIN").[33]

Under President Bush's proposal, HHS foresees an easily accessible, web-based EHR vault.[34] To improve population health and clinical research, the network would increase and diversify health data collection and dissemination.[35] HHS also intends to publicly monitor[36] and limit the network solely for non-proprietary use.[37] Although it claims the plan does not "constitute a change in policy, rule, or law, and does not call for statutory changes in its own right,"[38] the Department acknowledges that the NHIN must co-exist with federal medical privacy protections.[39]

---

has also been referred to as "Telemedicine." *See* Cheri J. Young, *Telemedicine: Patient Privacy Rights of Electronic Medical Records*, 66 U.M.K.C. L. REV. 921, 923 (1998) (citing JOINT WORKING GROUP ON TELEMEDICINE EXECUTIVE SUMMARY: TELEMEDICINE REPORT TO CONGRESS (1997), http://ntia.doc.gov/reports/telemed).

28. *See* HHS Report, *supra* note 4, at 5 (specifically referring to HIPAA).

29. *See id.* at 23-27.

30. *See* Exec. Order No. 13,335, 69 Fed. Reg. 24,059 (Apr. 30, 2004) (creating a "National Health Information Technology Coordinator"). The National Health Information Technology Coordinator must "address privacy and security issues related to interoperable [health information technology]." HHS REPORT, *supra* note 4, at 28.

31. Interoperable EHRs would include portable data in order to ensure "secure movement of health information" and "follow patients as they move through care settings." HHS REPORT, *supra* note 4, at 16.

32. *See id.* at 21-22.

33. *See id.* at 18-19.

34. *See id.*

35. *See id.* at 24.

36. *See id.* at 20. Since President Bush's proposal and recent congressional legislation do not specifically address oversight authority, this article assumes that HHS will devise and manage the network. *See* HHS RFI, *supra* note 6, at 12 ("While some respondents who addressed governance considerations indicated that little or no NHIN governance was required, most indicated that a well-built governance model was needed to develop, set policies and standards for, operate, and promote the adoption of NHIN"); *see also* Catherine Louisa Glenn, *Protecting Health Information Privacy: The Case For Self-Regulation of Electronically Held Medical Records*, 53 VAND. L. REV. 1605, 1633-34 (2000) (discussing the dangers surrounding self-regulating EHR access and use).

37. *See* HHS REPORT, *supra* note 4, at 18.

38. *See id.* at 2.

39. *See id.* at 5. HHS stated that "[n]early every [request for information] response addressed patient privacy and reiterated that the American people must feel confident that their health information is secure, protected, portable, and under their control." HHS RFI, *supra* note 6, at 21.

Given the heightened privacy concerns surrounding EHRs and computer networks,[40] understanding operational technology remains essential. How HHS proceeds will largely determine the influence and application of federal medical privacy law, and ultimately, the legal and political viability of President Bush's NHIN proposal.[41]

III. THE COMPUTER NETWORK CONCEPT

Web-based computer networks allow users to share and exchange data.[42] Peer-to-peer networks grant multiple users simultaneous access to information. Although programs like *Napster*, *Grokster*, *Kazaa*, and *Morpheus* continue to highlight the technology's growing popularity, distinct differences exist.[43] In its original form, *Napster* utilized a "closed network," where a common server linked users.[44] More

---

40. "The exponential increase in the use of computers and automated information systems for health-record information... [has contributed to] substantial pressure on traditional confidentiality protections." Patricia I. Carter, *Health Information Privacy: Can Congress Protect Confidential Medical Information In The "Information Age"?* 25 WM. MITCHELL L. REV. 223, 230 (1999) (quoting UNIF. HEALTH-CARE INFORMATION ACT, prefatory note 9, pt. I, U.L.A. 475 (1988)). *See also*, Press Release, Found. for Taxpayer & Consumer Rights, Hillary Clinton and Gingrich Support Legislation That Could Increase Medical Privacy Risks (May 11, 2005) (go to http://www.consumerwatchdog.org/pr/; then follow the 2005 archive hyperlink; then follow direct link to article listed by date) (citing its ability to use the Internet in order to cheaply purchase the Social Security numbers of various Bush administration officials).

41. *See* GAO REPORT, *supra* note 5, at encl. II. ("While there are some issues that may need to be worked out with respect to compliance with the [HIPAA's] Privacy and Security Rules in adopting [a national health care network], these protections help address one of the President's goals set forth in his Executive Order and could help overcome significant barriers to adoption . . .").

42. *See* Reno v. American Civil Liberties Union, 521 U.S. 844, 844 (1996) (defining the Internet as "an international network of interconnected computers"). Given President Bush's goal of allowing patients and necessary parties to conveniently access medical information, and because HHS should engage in operation and management, a NHIN will likely be considered a "public network." As a result, it may be subject to First Amendment viewpoint-discrimination restrictions. *See* Michael I. Meyerson, *Virtual Constitutions: The Creation of Rules for Governing Private Networks*, 8 HARV. J. LAW & TECH. 129, 131 (1994). Nonetheless, federal courts have routinely upheld federal medical privacy protections against similar First Amendment challenges. *See also* Citizens for Health v. Leavitt, 428 F.3d 167, 184-85 (3rd Cir. 2005); Ass'n of Am. Physicians and Surgeons, Inc. v. United States Dep't of Health and Human Serv., 224 F. Supp. 2d 1115, 1125 (S.D. Tex. 2002) *aff'd* 67 F. App'x 253 (5th Cir. 2003).

43. *See generally* H. Michael Drumm, *Life After Napster: Will Its Successors Share Its Fate?*, 5 TEX. REV. ENT. & SPORTS L. 157, 157-58 (2003) (discussing the operational technologies that empower *Napster*, *Kazaa*, and *Morpheus*).

44. *See* Hillary M. Kowalski, *Peer-to-Peer File Sharing & Technological Sabotage Tactics: No Legislation Required,* 8 MARQ. INTELL. PROP. L. REV. 297, 299 (2004) (citing Joseph A. Sifferd, *The Peer-to-Peer Revolution: A Post-Napster Analysis of the Rapidly Developing File-Sharing Technology,* 4 VAND. J. ENT. L. & PRAC. 93, 104 (2002)). *See also* Christopher Fazekas, *Vigilantes v. Pirates: The Rumble Over Peer-to-Peer Technology Hits the House Floor*, 2002 DUKE L. & TECH.

recent peer-to-peer programs operate under decentralized "pure networks."[45] Through specialized software, a pure network empowers users to independently operate and share data.[46]

While peer-to-peer networks allow for high-volume data exchange, privacy and security concerns remain. Tech savvy users can easily retrieve and manipulate sensitive information. Individuals can also plant viruses, spyware, or other malicious logic onto another's computer. Because peer-to-peer networks do not utilize a centralized server, accurately monitoring information use and disclosure also proves difficult.[47]

Client-server networks appear far more secure.[48] With client-server technology, users do not directly communicate; they only share and obtain data through a unifying, centrally-managed server.[49] Individuals utilize the network through an assigned username and password that the server must recognize and verify.[50] To protect against unauthorized activity, administrators can singularly employ numerous protective measures and dictate access levels.[51] Nonetheless, as technology and user expertise continue to develop, unassailable client-server network safety remains far from certain.[52]

REV. 20 (2002) (utilizing the term "hybrid" peer-to-peer network to describe *Napster*).

45. *See also* Fazekas, *supra* note 44 (describing *Morpheus* as epitomizing a new generation of "pure" peer-to-peer networks).

46. *See* Metro-Goldwyn-Mayer Studios Inc. v. Grokster, 125 S. Ct. 2764, 2771 (2005) (illustrating how programs such as *Morpheus* and *Grokster* utilize peer-to-peer network technology in order to allow users to independently exchange information).

47. *See generally* Fazekas, *supra* note 44; Kowalski, *supra* note 44. *See also Grokster*, 125 S. Ct. at 2771-72.

48. *See* David Hueneman, *Privacy on Federal Civilian Computer Networks: A Fourth Amendment Analysis of the Federal Intrusion Detection Network*, 18 J. MARSHALL J. COMPUTER & INFO L. 1049, 1054-57 (2000) (describing the Internet as one large client-server network).

49. *See* R. Carter Kirkwood, *When Should Computer Owners Be Liable for Copyright Infringement by Users?*, 64 U. CHI. L. REV. 709, 713 (1997).

50. *See* Hueneman, *supra* note 48, at 1054-55 (explaining that under a client-server network, administrators can also authorize access levels that specifically correlate with an individual participant's password or username).

51. *See id. See also infra* note 87.

52. *See generally* Scott Charney & Kent Alexander, *Computer Crime*, 45 EMORY L. J. 931 (1996) (highlighting the challenges that evolving computer technology poses to law enforcement, including unauthorized access to medical information).

Similar to the framework currently envisioned by other federal agencies,[53] the Bush administration's proposed NHIN should employ client-server technology.[54] Client-server technology allows HHS to authorize and regulate network activity. It empowers network managers to effectively monitor patient information use and disclosure. Given the medical privacy protections that HHS must honor, NHIN client-server technology also stands apart as the Bush administration's most viable option.

IV. HIPAA AND CREATING A SUCCESSFUL NHIN FRAMEWORK

Over the last decade, "safeguarding medical privacy" emerged as a key mantra in the U.S. health care debate.[55] Despite gradual progress, until the mid-1990s, universal safeguards remained weak. The federal government left states to their own devices, causing protection levels to vary nationwide.[56]

---

53. In response to President Bush's executive order, the U.S. Department of Defense (DoD) outlined its approach to electronically using and disclosing patient health information. The DoD report specifically references providers enjoying access to a centralized client-server network. *See* DEPARTMENT OF DEFENSE, REPORT ON APPROACHES TO WORK WITH THE PRIVATE SECTOR TO MAKE HEALTH INFORMATION SYSTEMS AVAILABLE AND AFFORDABLE TO RURAL AND MEDICALLY UNDERSERVED COMMUNITIES (July 2004), http://www.hhs.gov/healthit/attachment_3/attachment_3.html [hereinafter DoD REPORT].

54. *See* HHS RFI, *supra* note 6, at 43-44 (describing two competing client-server proposals for NHIN implementation: 1) a single federally administered client-server network; 2) multiple local client-server networks managed by Regional Health Information Organizations (RHIOs)). While this article contends that HHS should devise and operate the NHIN, HHS should establish a localized management structure. Minimizing centralized bureaucratic inefficiency, RHIOs will greatly aid HHS in receiving user feedback, swiftly addressing and resolving administrative issues, and detecting where and how the NHIN can improve.

55. *See generally* Lawrence O. Gostin et. al., *Balancing Communal Goods and Personal Privacy Under a National Health Informational Privacy Rule*, 46 ST. LOUIS U. L.J. 5 (2002) (detailing the lack of universal medical privacy protection prior to the mid-1990s); Hussong, *supra* note 25 (detailing a variety of legislative proposals aimed at strengthening perceived gaps in federal privacy law); Ryan Lowther, *U.S. Privacy Regulations Dictated by EU Law: How the Healthcare Profession May Be Regulated*, 41 COLUM. J. TRANSNAT'L L. 435 (2003) (addressing how the European Union has recently approached the concept of medical privacy protection and its implications for the United States); Jamie Lund, *ERISA Enforcement of the HIPAA Privacy Rules*, 72 U. CHI. L. REV. 1413 (2005) (arguing the plaintiffs may be able to pursue private causes of action under the Employee Retirement Income Security Act (ERISA) for various HIPAA violations); Peter A. Winn, *Confidentiality in Cyberspace: The HIPAA Privacy Rules and the Common Law*, 33 RUTGERS L. J. 617 (2002) (advocating common law avenues to supplement medical privacy in the evolving digital and electronic age).

56. *See* Gostin et. al., *supra* note 55, at 14 (although lauding Washington and California for enacting thorough medical information privacy acts, generally criticizing the pre-HIPAA state and federal protections); Eric Wymore, *It's 1998, Do You Know Where Your Medical Records Are? Medical Record Privacy After the Implementation of the Health Insurance Portability and Accountability Act of 1996*, 19 HAMLINE J. PUB. L. & POL'Y 553, 561-62 (1998) (discussing the

In 1996, President Clinton signed the "Health Insurance Portability and Accountability Act" ("HIPAA").[57] Among its various provisions,[58] HIPAA included a self-imposed deadline for Congress or the acting HHS Secretary[59] to finalize national medical privacy and security protections.[60]

Privacy cannot exist without security. By statutorily segregating these two interrelated interests, Congress viewed each with equal importance. Regarding privacy safeguards, Congress sought to "define and limit the circumstances in which an individual's protected health information may be used or disclosed by covered entities."[61] With key implications for the Bush administration's NHIN proposal, HIPAA's security provision primarily aimed to safeguard how parties physically access and transmit digital and electronic health data.[62] In 2002, the Bush administration affirmed HIPAA's final privacy regulations.[63] Required compliance with HIPAA's privacy rules began in April 2003,[64] but the federal government delayed adherence to the law's security mandates[65] until April 2005.[66]

---

conflict in various state medical privacy laws and lack of state enthusiasm for the "Uniform Healthcare Information Act," designed by the National Conference of Commissioners on Uniform State Laws to provide a model to universally safeguard health information).

57. Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (1997) (codified as amended in various sections of 42 U.S.C.).

58. HIPAA contains five health care-related sections. Title II, entitled "Administrative Simplification," governs medical privacy and security. *See* HIPAA, 110 Stat. at 1936-39.

59. Due to legislative inaction, acting HHS Secretary Donna Shalala issued the law's medical privacy mandates in December 2000. *See* 45 C.F.R. §§ 160, 164 (2006) [hereinafter "Privacy Rule"]. However, "[e]ven President Bill Clinton and former HHS Secretary Donna Shalala, who presided over the enactment of the HIPAA rules, did not consider HHS rulemaking to be a 'satisfactory long-term substitute for comprehensive legislation that could, and preferably would, be enacted by Congress in the future.'" Grace Ko, *Partial Preemption Under The Health Insurance Portability And Accountability Act*, 79 S. CAL. L. REV. 497, 526 (2006) (citing Charity Scott, *Is Too Much Privacy Bad for Your Health? An Introduction to the Law, Ethics, and HIPAA Rule on Medical Privacy*, 17 GA. ST. U. L. REV. 481, 510 (2000)).

60. *See* HIPAA § 264, 110 Stat. at 2033.

61. *See* Elizabeth Hutton & Devin Barry, *Medical: Privacy Year in Review: Developments in HIPAA*, 1 ILSJP 347, 352 (2005) (citing OFFICE FOR CIVIL RIGHTS, U.S. DEP'T OF HEALTH & HUMAN SERVICES, SUMMARY OF THE HIPAA PRIVACY RULE 4 (2003) http://www.hhs.gov/ocr/privacysummary.pdf).

62. *See* OFFICE FOR CIVIL RIGHTS, U.S. DEP'T OF HEALTH & HUMAN SERVICES, SUMMARY OF THE HIPPA PRIVACY RULE 1 (2003), http://www.hhs.gov/ocr/privacysummary.pdf.

63. Standards for Privacy of Individually Identifiable Health Information, 67 Fed. Reg. 53,181, 53,182 (Aug. 14, 2002) (codified as 45 C.F.R. §§ 160-164).

64. *See* 45 C.F.R. § 164.534(a) (2006). *See also* 45 C.F.R. § 164.534(b)(2) (2006) (setting an April 14, 2004 compliance deadline for "small health plans").

65. 45 C.F.R. §§ 164.306-312 (2006).

66. 45 C.F.R. § 164.318(a)(1) (2006); *see also* 45 C.F.R. § 164.318(a)(2) (2006) (providing small health plans with an extra year to adhere to security mandates).

Although Bush administration officials might envision a de-centralized approach to electronic health information exchange,[67] HHS retains responsibility for ensuring that its NHIN adheres to federal law.[68] In order to inspire the faith and confidence of patients, lawmakers, and others, the Bush administration should proceed with caution in directing HHS to devise, implement, and regulate the NHIN. Accordingly, HIPAA's medical privacy and security rules must play a central role.[69]

A. *HIPAA's Privacy Rule*

1. Protected Health Information

HIPAA prohibits the improper use and disclosure of protected health information (PHI).[70] Whether in electronic or paper format,[71] PHI pertains to individually

---

67. "Health information exchange networks could [also] be privately operated and governed by many State, regional or community level health information exchange authorities. These authorities would have responsibility for protecting information and ensuring that data is used to advance the public interest, and used in compliance with applicable State and federal laws." *Health Information Technology: Hearing Before the Subcomm. on Health of the H. Comm. on Ways and Means*, 108th Cong. (2004) (statement of Dr. David Brailer, M.D. Ph.D, National Health Information Technology Coordinator, U.S. Department of Health and Human Services) *available at* http://waysandmeans.house.gov/hearings.asp?formmode=view&id=1652.

68. *See* HHS REPORT *supra* note 4, at 5.

69. HIPAA's significance has been magnified due to the federal courts' reluctance to recognize a constitutional privacy right regarding patient medical information. *See* Whalen v. Roe, 429 U.S. 589, 591 (1977) (upholding government interests in maintaining a computerized database of individuals obtaining particular prescription drugs and deferring to state and common law tort protections); United States v. Westinghouse Corp., 638 F.2d 570, 580 (3d Cir. 1980) (allowing the National Institute of Occupational Safety and Health to accumulate private medical records of employees exposed to toxins); Doe v. Southeastern Pennsylvania Transp. Auth., 72 F.3d 1133, 1139 (3d Cir. 1995) (supporting government interests in monitoring prescription drug use for fraud and abuse detection). *But see* James D. Molenaar, *The HIPAA Privacy Rule: It Helps Direct Marketers Who Help Themselves To Your Personal Information*, 2002 MICH. ST. L. REV. 855, 860-62 (2002) (arguing that medical privacy should be construed as a constitutional "fundamental right").

70. 45 C.F.R. § 164.502 (2006). Although HIPAA does not specifically authorize private causes of action, the HHS Secretary retains the authority to impose civil penalties. *See* 42 U.S.C. § 1320d-5 (1996). *But see* Rob Stein, *Medical Privacy Law Nets No Fines*, WASH. POST, June 5, 2006, at A.01 (citing a lack of civil enforcement by HHS officials since HIPAA's inception). On March 16, 2006, HHS published rules regarding the imposition of civil penalties for HIPAA violations including the law's security mandates. The new rules detailed investigation, hearing, and appeal procedures and clarified liability and penalty standards. *See* 45 C.F.R. §§ 160.400-426; 160.500-552 (2006). Particular HIPPA violations can also lead to criminal liability. *See* 42 U.S.C. § 1320d-6 (1996). In November 2004, a former employee of the Seattle Cancer Care Alliance wrongfully disclosed PHI for monetary gain and became the first individual to be criminally convicted under HIPAA. *See* American Medical Association, Current Legal Issues: HIPAA Criminal Enforcement Starts, http://www.ama-assn.org/ama/pub/category/15692.html (last visited Sept. 4, 2006).

71. 45 C.F.R. § 160.103 (2006) ("health information"). *See also* S. Carolina Med. Ass'n v.

identifiable health information.[72] Although typically used to refer to medical history, PHI also includes any data that may reasonably identify a patient.[73]

Regardless of how HHS may pursue uniform patient classification,[74] EHRs will allow for more efficient PHI use and disclosure.[75] Because HHS should design the NHIN with client-server technology, network architects must consider how prospective participants may fall under HIPAA's reach.[76]

2. Covered Entities

HIPAA directly governs covered entities:[77] health care providers,[78] health plans,[79] and health care clearing houses.[80] Generally, health care providers furnish, or

---

Thompson, 327 F.3d 346, 353 (4th Cir. 2003) ("[t]he plain language of HIPAA indicates that HHS could reasonably determine that the regulation of individually identifiable health information should include [electronic and] non-electronic forms of that information.").

72. 45 C.F.R. § 160.103 ("individually identifiable health information"). Key information excluded from PHI involves student records applicable to the "Family Educational Rights and Privacy Act" and employer-maintained work records. *See id.* ("protected health information").

73. *See* Jack A. Rovner et al., *Managing the Privacy Challenge: Compliance With The Amended HIPAA Privacy Rule*, HEALTH LAW., Sept. 2002, at 18, 21.

74. HIPAA contains language that authorizes HHS to create numeric health identifiers for individuals, employers, health plans, and providers. *See* 42 U.S.C. § 1320d-2(b) (1996). The Bush administration largely continues to neglect the specific provision regarding individuals; however, to effectively register participants and implement any effective NHIN, the federal government will continue revisit the concept. *See* 45 C.F.R. §§ 162.402-414 (2006) (mandating the use of a national provider identifier (NPI) for health care providers); 45 C.F.R. §§ 162.600-610 (2006) (mandating the use of a standard unique employer identifier (EIN) for employers); *see also* Sobel, *supra* note 24, at 61 ("[N]ow that HHS medical records regulations have been approved, the idea of a unique health identifier is likely to resurface."). *See also* Press Release, U.S. Dep't of Health and Human Services, HHS Awards Contracts to Develop Nationwide Health Information Network (Nov. 10, 2005) *available at* http://www.hhs.gov/news/press/2005pres/20051110.html (announcing that Accenture, Computer Science Corporation, International Business Machines, and Northrop Grumman recently received federal contracts to develop NHIN prototypes that will include patient identification).

75. *See generally* HHS REPORT, *supra* note 4, at 23-27; *see also* PRESIDENT BUSH'S HEALTH INFORMATION TECHNOLOGY PLAN, *supra* note 2.

76. "[HIPAA's privacy and security] standards, which are carefully balanced to ensure individuals' access to quality care, will guide the development of a national health information infrastructure and form the basis of the safeguards to protect the privacy and confidentiality of personal health information." *Health Information Technology: Hearing Before the Subcomm. on Health of the H. Comm. on Ways and Means*, 108th Cong. (2004) (statement of Dr. David Brailer, M.D. Ph.D, National Health Information Technology Coordinator, U.S. Department of Health and Human Services) *available at* http://waysandmeans.house.gov/hearings.asp?formmode=view&id=1652.

77. 45 C.F.R. §§ 160.102, 164.103 (2006). HIPAA also provides for "organized health care arrangements" (OHCAs). An OHCA is an association of covered entities that share PHI to manage and benefit a common enterprise. *See* 45 C.F.R. § 164.506(c)(5) (2006). In determining who will enjoy access, HHS must assure users that its network does not constitute a de-facto OCHA. If not,

receive payment for, medical services.[81] Health plans pay for or authorize medical care.[82] Health care clearinghouses include public and private entities that convert and format health information.[83]

To achieve President Bush's goals, covered entities will utilize the NHIN. The initial hurdles involve selecting participants, assigning access, and regulating network activity. While increasing administrative efficiency and improving health care delivery are noble, preventing unaccountable information exchange must remain a paramount concern.[84] To maximize medical privacy protection and ensure regulatory consistency, HHS should utilize HIPAA's definitions and mandates to organize and authorize NHIN activity.[85]

For PHI use, HHS should limit network access according to the covered functions[86] applicable to providers, plans, and clearinghouses.[87] HHS should also

---

participants may balk at potential joint-several liability issues and refuse to participate. *See* HHS RFI, *supra* note 6, at 22 ("Respondents noted a variety of options with respect to the privacy and security provisions of HIPAA, including . . . expanding the definition of covered entities to include a NHIN or RHIOs . . . .").

78. 45 C.F.R. § 160.103 (2006) ("health care provider").

79. 45 C.F.R. § 160.103 ("health plan"(1); "health plan"(2)(i)-(ii)) (excluding certain government-funded programs and coverage for certain "excepted benefits," including disability income, worker's compensation, and automobile medical liability payments).

80. 45 C.F.R. § 160.103 ("health care clearinghouse").

81. 45 C.F.R. § 160.103 ("health care provider"). Unlike health plans and health care clearinghouses, health care providers are not covered entities if they only maintain, but do not transmit, PHI. *See* Robert W. Woody, *Health Information Privacy: The Rules Get Tougher*, 37 TORT & INS. L. J. 1051, 1055 (2001). Nonetheless, to avoid ambiguity, HHS should still utilize HIPAA's mandates and definitions to uniformly regulate network use and access for all providers.

82. 45 C.F.R.§ 160.103 ("health plan") (involving HMOs, numerous government benefit programs, and most health insurance companies).

83. 45 C.F.R. § 160.103 ("health care clearinghouse") (specifically including billing services, repricing companies, community health information systems, and value-added networks and switches).

84. *See* Hussong, *supra* note 25, at 455-57. *But see* David R. Morantz, *HIPAA's Headaches: A Call for a First Amendment Exception to the Newly Enacted Health Care Privacy Rules*, 53 U. KAN. L. REV. 479, 489-98 (2005) (stating that HIPAA unduly stifles First Amendment principles and calling for a public vs. private interest distinction in creating additional exceptions to the law's patient authorization requirement); Meredith Kapushion, *Hungry, Hungry HIPAA: When Privacy Regulations Go Too Far*, 31 FORDHAM URB. L.J. 1483, 1502-05 (2004) (advocating that an unregulated market-based approach would provide greater privacy protections and ultimately, arguing for HIPAA's repeal).

85. HIPAA's April 2003 compliance deadline required the health care industry to define itself in terms of providers, plans, and clearinghouses. *See* 45 C.F.R. § 164.534 (2006). Utilizing HIPAA to identify and authenticate network participants provides HHS with a convenient organizational framework already in use.

86. "Covered functions" dictate whether organizations qualify as a provider, plan, or clearinghouse. 45 C.F.R. § 164.103 ("covered functions").

create sections for every EHR. Based on assigned access privileges, each portion should only display the minimum information necessary[88] for a covered entity to complete its covered function.[89]

For PHI disclosures,[90] covered entities should direct HHS to authorize network access to specifically identified recipients. As determined by the covered entity and authenticated by HHS, PHI recipients should only be able to view the applicable EHR sections required to complete a covered function or other specifically authorized activity. HHS should also require that covered entities, in order to authorize access for specific PHI recipients, enjoy a patient-relationship.[91] Inspiring trust in the Bush administration's dedication to protecting individual privacy,[92] these requirements eliminate non-essential parties from accessing an individual's medical history.[93]

---

87. Prior to granting access rights, HHS will also need to authenticate all NHIN-eligible health providers, plans, clearinghouses, business associates, patients, and others. Authentication should compass confirming an organization's identity, purpose, and current compliance with HIPAA and applicable state medical privacy laws. *See supra* note 74.

88. *See infra* notes 127-132 (discussing HIPAA's "minimum necessary" requirement).

89. Requiring all NHIN participants to install computer "smart cards" may be an effective secondary method for securely utilizing EHRs and accessing PHI over the network. Containing various memory zones, with different access and security levels, smart cards can regulate the scope and duration of all network activity. *See* Jurevic, *supra* note 21, at 826; Wendy Wuchek, *Conspiracy Theory: Big Brother Enters the Brave New World of Health Care Reform*, 3 DEPAUL J. HEALTH CARE L. 293, 301-03 (2000). NHIN smart card technology would only enable providers to view EHR sections related to furnishing, and receiving payment for, medical services. Health plans could only access sections with information necessary to pay for or authorize medical care. Health care clearing houses could solely view data needed to convert and format health information. If HHS deems wide network access essential, these same limitations should apply for business associates and others according to the services that they provide.

90. *See infra* notes 115, 168, and accompanying text. Under HIPAA's security mandates, covered entities must "[I]mplement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed." 45 C.F.R. § 164.312(d) (2006).

91. When defining what qualifies as a patient-relationship, HHS should use the "health care operations" model for all network access. *See* 45 C.F.R. § 164.506(c)(4) (2006) (including current and prior patient relationships and requiring that the PHI disclosed must pertain to the relationship). This common-sense approach would placate privacy advocates and also allow HHS to gauge if, and where, access should later expand. *See* HHS RFI, *supra* note 6, at 7 (highlighting comments that NHIN use should "evolve incrementally").

92. *But see* AMERICAN MEDICAL ASSOCIATION, COUNCIL ON ETHICAL AND JUDICIAL AFFAIRS, CODE OF MEDICAL ETHICS, OPINION E5.07 CONFIDENTIALITY COMPUTERS (1998), http://www.ama-assn.org/ama/pub/category/8360.html (while not required by HIPAA, recommending that patients should retain the right to authorize any electronic release of their health information).

93. Although some may fear that a national health care information network could enable organizations to more efficiently access and exploit a competitor's payment activities and business relationships, the NHIN will exist for non-proprietary use. *See* HHS REPORT, *supra* note 4, at 18. *See also* 42 U.S.C. § 1320d-6 (authorizing criminal fines and incarceration for obtaining or disclosing PHI under false pretenses or with the intent to use PHI for commercial gain). *But see* June Mary Zekan Makdisi, *Commercial Use of Protected Health Information Under HIPAA's Privacy Rule:*

3. Business Associates

Other organizations fall under HIPAA as "business associates."[94] Business associates perform activities for, or provide services to, covered entities.[95] Through contract they must also promise covered entities that they will adequately safeguard PHI.[96]

Privacy concerns involving business associates will largely hinge on the network's intended scope. At first glance, HHS could withhold business associate participation. Even outside the NHIN, covered entities could independently exchange PHI with their business associates. However, if the Bush administration strives to uniformly improve efficiency throughout the health care system, including business associates is imperative. Because most business associates deliver incidental administrative services,[97] allowing limited NHIN access would conserve time, effort, and resources. In turn, savings could be re-directed toward delivering improved care and containing costs.

Nonetheless, HIPAA fails to directly regulate business associates.[98] The law merely requires covered entities to monitor business associate behavior, uncover potential wrongdoing, and maintain patient privacy.[99] Unfettered NHIN access could compromise a covered entity's ability to supervise how its business associates utilize patient PHI. Should the Bush administration determine that maximizing efficiency must drive initial NHIN implementation and use, HHS must work to preserve the delicate affiliation between covered entities and their business associates.

Reasonable Disclosure or Disguised Marketing?, 82 NEB. L. REV. 741, 764-73, 780-82 (2004) (describing HIPAA's failure to adequately protect patients from commercial marketing abuses).

94. 45 C.F.R. § 160.103 (2006) ("business associates").

95. *Id.* Business associates may include lawyers, accountants, utilization and quality review companies, or certain data processing and management firms. *See also* Rovner et al., *supra* note 73, at 22 (discussing the scope of HIPAA's business associate definition).

96. 45 C.F.R. § 164.502(e) (2006) (business associates must provide covered entities with "satisfactory assurances" regarding PHI use and disclosure). Should the relationship expire, the business associate must destroy or return the covered entity's PHI. 45 C.F.R. § 164.504(e)(2)(ii)(I) (2006). Under the NHIN, business associates would eventually no longer physically possess electronic PHI provided by a covered entity; instead they would enjoy access to the information over the network. Accordingly, HHS should require covered entities to immediately obtain written confirmation that the relationship has expired and request that the Department withdraw their business associate's NHIN access rights.

97. *See* Rovner et al., *supra* note 73, at 22 (discussing HIPAA's business associate provision).

98. *See* OCR GUIDANCE EXPLAINING SIGNIFICANT ASPECTS OF THE PRIVACY RULE (2003), http://www.hhs.gov/ocr/hipaa/guidelines/businessassociates.pdf (specifically failing to mention HHS authority over business associates).

99. 45 C.F.R. § 164.504(e)(1) (2006).

HIPAA's business associate contract provision may remedy concerns.[100] HHS ought to require each covered entity to include additional terms that regulate the duration and scope of its business associate's NHIN activity. Indicating the nature of their relationship, HHS should also compel covered entities to annually provide the Department with a detailed synopsis of their current business associates.[101] Upon certification, HHS should then only authorize limited NHIN access according to the particular service that each business associate provides.[102]

4. Authorization and Treatment, Payment, and Health Care Operations

Although not absolute,[103] covered entities may only use or disclose PHI pursuant to a valid, revocable authorization from the patient.[104] The authorization must identify the individual[105] and detail the specific PHI to be used or disclosed.[106] It shall also describe the specific purpose for intended PHI uses or disclosures[107] and highlight when any authorized activity expires.[108]

Prior to the NHIN's debut, covered entities will need to alter their patient authorizations. Updated notices ought to include how and why covered entities intend to utilize the network. They should also inform patients how to access the network in order to view their own EHR.

Regardless, many health care functions escape HIPAA's authorization requirement. Covered entities do not require patient authorization to use or disclose

---

100. *Id.*

101. *See infra* note 168 and accompanying text.

102. *See* HHS RFI, *supra* note 6, at 22 (although described within the context of RHIO participation, highlighting the importance of certification and accreditation to "ensure adherence not only to HIPAA regulations, but also to more uniform business policies and procedures, interoperability standards, and other harmonized standards").

103. The most common exceptions to HIPAA's authorization rule include: uses and disclosures for treatment, payment, and health care operations, HHS investigations, health oversight, public health and safety, and research. 45 C.F.R. § 164.502(a) (2006). Nonetheless, key aspects of NHIN activity should escape HIPAA's authorization requirement. *See* HHS REPORT, *supra* note 4, at 24.

104. 45 C.F.R. §§ 164.502(a)(1)(iv) (2006); 164.508(c)(2)(i) (2006).

105. 45 C.F.R. § 164.508(c)(1)(ii) (2006).

106. 45 C.F.R. § 164.508(c)(1)(i) (2006). Although HIPAA requires covered entities to obtain patient authorization for certain marketing purposes, they can market some of their own goods and services to their own patients without authorization. 45 C.F.R. § 164.508(a)(3) (2006). *But see* HHS REPORT, *supra* note 4, at 18 (limiting network use for non-proprietary purposes). *See also* Hatch, *supra* note 25, at 1493 (criticizing HIPAA's self-marketing exception as an irresponsible capitulation to commercial lobbying interests).

107. 45 C.F.R. § 164.508(c)(1)(iv) (2006). If the patient initiates the authorization, the covered entity only needs to include the reasons for the authorization at the patient's request. *Id.*

108. 45 C.F.R. § 164.508(c)(1)(v) (2006).

PHI for treatment, payment, and health care operations ("TPO").[109] As a result, HHS must resolve whether the NHIN is necessary and appropriate for all TPO purposes.[110]

Under HIPAA, treatment involves the "provision, coordination, or management of health care and related services by one or more health care providers . . . ."[111] Utilizing patient PHI over the NHIN to improve health care delivery remains a key premise behind President Bush's proposal.[112] Even with limitations, the network will allow providers to more effectively use PHI when administering care. Because EHRs will maintain past and current diagnoses, prescriptions, and procedures, providers will enjoy immediate access to a patient's entire medical history. Moreover, solely relying on patient memory or displaced paper records will no longer impair providers, especially in emergency situations.

For treatment-related PHI disclosures,[113] although not required by HIPAA, HHS should require that each party enjoy a patient-relationship.[114] For each intended recipient, NHIN architects should also require that covered entities individually authorize HHS to grant time-specific EHR access.[115] Striking the appropriate balance between maximizing efficiency and ensuring patient privacy, this process facilitates proper treatment-related data exchange.

Although HIPAA's payment exception primarily refers to provider reimbursements,[116] it also applies to health plans receiving premiums or processing coverage and benefits.[117] For payment-related PHI use and disclosure, EHR access privileges will again play a large role regarding how the network will ultimately operate. While HHS should delineate PHI use based on covered function, and

---

109. 45 C.F.R. § 164.506(c)(1) (2006).

110. Although President Bush's proposal currently envisions voluntary patient participation and authorization for EHRs and electronic PHI use and disclosure, this article assumes that the NHIN will ultimately operate as the universal tool for utilizing and exchanging health data. While adhering to HIPAA's definitions and mandates, architects should devise the network with maximum participation in mind.

111. 45 C.F.R. § 164.501 (2006) ("treatment") (including patient consultation and referrals and health management and coordination with third parties).

112. *See* HHS REPORT, *supra* note 4, at 23-27; *See also* PRESIDENT BUSH'S HEALTH INFORMATION TECHNOLOGY PLAN, *supra* note 2.

113. For their own treatment purposes, providers may also disclose PHI to each other without patient authorization. 45 C.F.R. § 164.506(c)(1)-(2) (2006). *See also* 45 C.F.R. §§ 164.502(b), 164.514(d)(1)-(2) (2006) (describing HIPAA's "minimum necessary" requirement).

114. *See supra* notes 25, 91, and accompanying text.

115. Similar to a business associate contract, HHS should direct covered entities to enter into memorandums of understanding with their PHI recipients that detail the duration and scope of their authorized network access. Both additional safeguards would help ensure that PHI recipients do not utilize or access patient PHI for unnecessary time periods or unauthorized means.

116. 45 C.F.R. § 164.501(2006) ("payment").

117. *Id.* (including Medicare and Medicaid claims).

limited pursuant to patient-relationships,[118] HIPAA allows covered entities to disclose payment-related PHI to any third-party, including non-covered entities.[119]

Understandably, opening the network to any non-covered entity raises glaring privacy concerns. While business associate activity can be held accountable through contract,[120] NHIN managers must take additional steps to safeguard patients. HHS should require applicable covered entities to identify specific payment-related PHI recipients.[121] After receiving individual authorization from the covered entity, HHS should delineate access only to those EHR sections necessary to complete the targeted transaction.[122]

For health care operations, HIPAA separates regulated activity into quality and competence assurance,[123] insurance services,[124] fraud detection and compliance,[125] and various business functions.[126] Covered entities may use or disclose PHI to any third party for its own health care operations.[127] If the PHI disclosure involves another covered entity, both parties must enjoy a patient-relationship.[128]

Similar to HIPAA's payment provision, health care operations involving third parties also creates privacy dilemmas. For PHI disclosures between covered entities, utilizing a covered function, patient-based approach not only ensures HIPAA compliance, it duly protects individual privacy. If HHS deems broad NHIN activity essential, it should require covered entities to identify non-covered entity health care operations recipients, and after receiving authorization, delineate limited EHR access.[129]

---

118. *See supra* note 91 and accompanying text.

119. 45 C.F.R. § 164.506(c)(3) (2006).

120. 45 C.F.R. § 164.504(e) (2006).

121. *See also supra* notes 91, 115 and accompanying text.

122. *See* 45 C.F.R. §§ 164.502(b)(1); 164.514(d) (2006) (describing HIPAA's "minimum necessary" requirement).

123. 45 C.F.R. § 164.501 (2006) ("health care operations") (referring to certain non-research activity, evaluations of health care professional qualifications, and training programs).

124. *Id.* (involving underwriting, premium rating, and activity regarding health insurance contracts).

125. *Id.* (including the arrangement of medical reviews, auditing, and legal services).

126. *Id.* (pertaining to certain business planning, management, and development). These also include fundraising or de-identifying PHI for certain research and public health functions. *See generally* 45 C.F.R. § 164.514 (2006). For a discussion on how this provision hampers HIPAA's overall goal of enhanced privacy protection see Makdisi, *supra* note 93, at 766-80.

127. 45 C.F.R. § 164.506(c)(1) (2006).

128. *See supra* note 91 and accompanying text.

129. Those involved with quality and competence assurance, fraud detection, and insurance and business activities should only enjoy access to the minimum EHR sections necessary to complete their corresponding duties. *See* 45 C.F.R. §§ 164.502(b); 164.514(d) (2006).

6. The "Minimum Necessary" Standard

When utilizing PHI, HIPAA requires covered entities to adhere to its "minimum necessary" standard.[130] For PHI use, covered entities must identify workforce members that require access to an individual's PHI[131] and proscribe appropriate limitations.[132] For PHI disclosures, HIPAA addresses routine and non-routine activity.[133] For routine disclosures, covered entities shall only transmit the amount reasonably necessary to achieve the specifically intended purpose.[134] Regarding non-routine releases, covered entities must develop internal procedures that limit the amount of PHI disclosed.[135]

Because client-server networks provide centralized access to information, oversight must rest with HHS operators. Creating a uniform framework not only provides clarity and consistency,[136] but it also allows HHS to properly regulate how participants and others utilize and access patient PHI over the network. Therefore, HIPAA's minimum necessary standard should govern all NHIN use.

Prior to implementation, HHS should solicit feedback and require covered entities to differentiate between "routine" and "non-routine" disclosure activity. Covered entities ought to indicate why any "non-routine" disclosure cannot be achieved through alternative means.[137] Upon receiving this information, HHS should

---

130. 45 C.F.R. §§ 164.502(b); 164.514(d). However, treatment disclosures to the individual or those made pursuant to a valid patient authorization, HHS investigation, or legal requirement escape HIPAA's minimum necessary clause. *See* 45 C.F.R. § 164.502(b)(2)(ii)-(v) (2006). *But see* Pierre, *supra* note 15, at 567 (advocating for no exceptions to HIPAA's "minimum necessary" standard for EHRs or other electronic PHI use and disclosure).

131. 45 C.F.R. § 164.514(d)(2)(i)(A)(2006).

132. 45 C.F.R. § 164.514(d)(2)(i)(B) (2006). Covered entities only need to take "reasonable steps" to limit employee access to patient PHI. 45 C.F.R. § 164.514(d)(2)(ii) (2006). Regarding NHIN activity, mandated employee training and appropriate technological safeguards should adequately address this provision. *See also infra* notes 216, 225-229 and accompanying text.

133. HIPAA also includes a routine and non-routine distinction for PHI requests. 45 C.F.R. § 164.514(d)(4) (2006). For non-routine disclosures, covered entities may reasonably rely on the judgment of those requesting the PHI regarding the minimum PHI necessary to accomplish the request's intended purpose. 45 C.F.R. § 164.514(d)(3)(ii)-(iii) (2006). *See also* OCR GUIDANCE EXPLAINING SIGNIFICANT ASPECTS OF THE PRIVACY RULE (2003), http://www.hhs.gov/ocr/hipaa/guidelines/minimumnecessary.pdf. Because PHI disclosure over the NHIN will be based on assigned access rights, creating uniform minimum necessary standards for all NHIN activity eliminates ambiguity and should alleviate patient privacy concerns. *See infra* note 168 and accompanying text.

134. 45 C.F.R. § 164.514(d)(3)(i) (2006).

135. 45 C.F.R. § 164.514(d)(3)(ii)(A) (2006).

136. Because HIPAA does not precisely articulate what "minimum necessary" use and disclosure entails, HHS enjoys an added opportunity to refine its application and meaning for NHIN activity.

137. For non-routine activity, NHIN participants should also annually provide HHS with the

develop specific minimum necessary EHR access standards for covered functions and activities by business associate and other third parties.[138] Although requiring users to abide by strict guidelines may initially stifle efficiency, HHS should nonetheless proceed with caution. Given the potential for abuse and the delicate nature of an individual's PHI, NHIN-specific 'minimum necessary' standards properly uphold patient privacy and ensure the network operates according to President Bush's intended goals.[139]

For PHI use, the federal government must work closely with covered entities in properly training workforce members.[140] HHS should also require that business associates and other third parties adequately instruct their employees regarding NHIN access and use.[141] Under HIPAA, HHS could delineate internal employee NHIN access authority to network participants.[142] However, centralized control empowers HHS to maximize patient privacy and ensure that participants and their employees properly utilize the network.

NHIN participants should identify specific employees based on how they manage patient PHI.[143] Depending on whether employed by a covered entity, business associate, or other third party, HHS should authorize work force members to only enjoy access to the minimum EHR sections necessary to complete their work-related tasks.[144] While perhaps cumbersome, the Bush administration must ensure patients, lawmakers, and others who utilize the NHIN remain properly trained and closely monitored.

---

internal procedures they utilized in order to minimize the amount of electronic PHI disclosed outside the network. 45 C.F.R. § 164.514(d)(3)(ii)(A). Based on this input, HHS could later expand NHIN access to incorporate certain non-routine activity.

138. *See supra* note 115 and accompanying text; *infra* note 167 and accompanying text.

139. *See generally* PRESIDENT BUSH'S HEALTH INFORMATION TECHNOLOGY PLAN, *supra* note 2.

140. 45 C.F.R. § 164.308(a)(3)(i) (2006).

141. *See id.*

142. *Id.* Similar to the DoD model, HHS could also allow NHIN participants to create their own smaller network to self-regulate internal PHI use. *See* DOD REPORT, *supra* note 53. Network traffic may lessen and new employees could avoid waiting until HHS authorized access. *But see* Glenn, *supra* note 36, at 1633 (citations omitted) ("... multiplying reports of surreptitious collection of consumer data by Internet marketers and questionable distribution of such personal data by other companies make privacy an issue of increasing public concern").

143. *See supra* notes 131-132.

144. *See supra* note 89 (detailing how "smart card" technology will assist in minimizing the amount of PHI that authorized employees will be able to access and use).

7. Patient Rights

HIPAA also grants patients key rights over their medical information. Health plans and covered entities with direct treatment relationships[145] must notify patients regarding their privacy practices.[146] Explaining the covered entity's duties and obligations,[147] the notice also informs patients regarding their PHI rights and explains enforcement procedures.[148]

Covered entities will need to alter their notification practices and include information regarding PHI use and disclosure through the NHIN. To meet the April 2003 compliance deadline,[149] most covered entities mailed or posted in-office notices. To alleviate additional administrative burdens, the federal government needs to provide further assistance. Congress should authorize financial support for NHIN notice-related costs. Through its website, the Department should also require that all patients, prior to receiving individualized access to their own EHR, register with a username and password[150] and acknowledge a universal, NHIN-oriented privacy notice.[151]

By utilizing dual NHIN notification procedures, HHS will accomplish two key goals. First, locally administered NHIN-based notices ensure continued compliance with HIPAA. Additionally, they immediately inform patients, especially those without computer access, about how their PHI could be used and exchanged over the network. Second, through website notice acknowledgement and registration, HHS can further increase trust and awareness regarding NHIN privacy practices and begin to securely account for individuals seeking personal access to their own EHR.[152]

---

145. 45 C.F.R. § 164.501 (2006) ("direct treatment relationship"). HIPAA's notice requirement does not apply to indirect treatment relationships. Indirect treatment relationships occur when a provider delivers care to a patient based on another provider's orders or when a provider gives "services or products, or reports the diagnosis or results associated with the health care, directly to another health care provider, who provides the services or products or reports to the individual." *Id.*

146. 45 C.F.R. § 164.520(a) (2006).

147. 45 C.F.R. §§ 164.520(b)(1)(ii) & (v) (2006). The notice must also inform patients that filing a complaint will not result in retaliatory action. *See id.*

148. 45 C.F.R. § 164.520(b)(1)(iv) (2006).

149. 45 C.F.R. § 164.534 (2006).

150. Because not all patients possess home computers, HHS should direct health care providers, or applicable equivalent, to instruct patients to register with HHS through provider-based computer workstations.

151. On its website, HHS should also provide links that direct covered entities and individual users to their applicable RHIO for guidance regarding additional notice requirements under applicable state medical privacy law. *See infra* note 198 and accompanying text.

152. *See also supra* note 69 and accompanying text.

a. Individual Right to PHI Access

Although not absolute, HIPAA also grants patients the right to access their PHI.[153] Patients can review and obtain copies of their PHI; however, their PHI must be a part of a covered entity's "designated record set."[154] If a covered entity declines an individual access to their own PHI, HIPAA also differentiates between "reviewable" and "non-reviewable" denials.[155] "Reviewable" denials involve decisions intended to protect patients from harm.[156] A "non-reviewable" access denial pertains to PHI which is located within psychotherapy notes, compiled in anticipation for certain legal action, regulated by federal clinical research rules, held by correctional facilities, protected under the "Privacy Act of 1974," or obtained under a promise of confidentiality.[157]

Because EHRs incorporate HIPAA's designated record set model, patients should be entitled to view all information in their EHR. Accordingly, HHS must create and maintain secure patient access to the NHIN, including user-names and passwords.[158] Unlike coordinating with larger organizations, ensuring individual privacy and security for home computer use seems unrealistic. To further strengthen the patient-provider relationship,[159] HHS should authorize personal access to EHRs through secure computer workstations operated by an individuals' primary care provider or applicable equivalent.[160]

Although patients may still utilize their HIPAA rights to demand access to PHI outside the NHIN, HHS, through a client-server network, will manage EHR access. As a result, the federal government must also assume greater responsibility for HIPAA's "reviewable" and "non-reviewable" distinction. Prior to the NHIN's debut,

---

153. *See generally* 45 C.F.R. § 164.524 (2006). This right is also the driving force behind EHRs and the Bush administration's proposed national health care network. *See generally* HHS REPORT, *supra* note 4, at 21-22; PRESIDENT BUSH'S HEALTH INFORMATION TECHNOLOGY PLAN, *supra* note 2.

154. 45 C.F.R. § 164.524(a)(1) (2006). A designated record set is the group of medical records kept by a covered entity to make health care decisions. 45 C.F.R. § 164.501 (2006) ("designated record set").

155. 45 C.F.R. §§ 164.524(a)(2) (3) (2006).

156. 45 C.F.R. §§ 164.524(a)(3).

157. 45 C.F.R. §§ 164.524(a)(2).

158. This dilemma again increased the likelihood that HHS must develop a national patient identification system. *See supra* note 74.

159. *See supra* note 25.

160. For individuals without primary care providers, RHIOs will need to coordinate with applicable local governments and non-profit organizations to ensure that all Americans, regardless of health coverage, will possess an EHR and enjoy NHIN access. *See* KAISER COMMISSION ON MEDICAID & THE UNINSURED, THE UNINSURED: A PRIMER: KEY FACTS ABOUT AMERICANS WITHOUT HEALTH INSURANCE 1 (2006), http://www.kff.org/uninsured/upload/7451.pdf (stating that over 45 million Americans lacked health insurance in 2004).

HHS should require covered entities to inform the Department regarding any patient PHI that they initially deem inaccessible under HIPAA.[161] Upon review, HHS should then develop protocols that eliminate certain information from a patient's view.[162]

If a patient still seeks access to PHI not located in their EHR or believes that their EHR remains incomplete, HHS should direct patients to request access from the applicable covered entity outside the NHIN. If unsuccessful, patients should resolve any dispute through their local Regional Health Information Organization (RHIO).[163] As a last resort, patients should enjoy the right to appeal any decision by a covered entity or RHIO to HHS for final disposition.

b. Individual Right to PHI Amendments

Under HIPAA, individuals may also ask any covered entity to amend PHI existing within the individual's designated record set.[164] Within sixty days, covered entities must provide a written reply.[165] Under certain conditions, covered entities may deny PHI amendment requests.[166] However, once accepted, covered entities must incorporate updated information and notify their business associates.[167] If specifically identified by the patient, covered entities must also inform any other persons that receive the individual's PHI.[168]

While allowing patients to directly submit amendment requests through HHS or RHIOs may appear convenient, the Bush administration should work to strengthen

---

161. When devising the NHIN, HHS must also incorporate this information when creating viewable EHR sections applicable to covered entities, business associates, patients, and authorized third-parties.

162. *See supra* note 89 and accompanying text.

163. *See supra* note 54 and accompanying text.

164. 45 C.F.R. § 164.526 (2006).

165. 45 C.F.R. § 164.526(b)(2) (2006).

166. Covered entities can reject amendment requests if the PHI does not exist within the individual's designated record set, the covered entity did not create the PHI, or the PHI proves inaccessible under 45 C.F.R. § 164.524, or remains complete and accurate. 45 C.F.R. §§ 164.526(a)(2)(i)-(iv) (2006).

167. 45 C.F.R. §§ 164.526(c)(1)-(3) (2006). Covered entities must also provide the individual's amended PHI to anyone that could "foreseeably rely" on the current information to the individual's own harm. 45 C.F.R. § 164.526(c)(3)(ii) (2006). In order for HHS to authorize network access for their PHI recipients, covered entities will need to provide the Department with a list of covered entities, business associates, and other third parties. Because only those organizations will "foreseeably rely" on a patient's amended PHI, the NHIN should greatly assist covered entities in efficiently complying with this provision.

168. 45 C.F.R. § 164.526(c)(3)(i) (2006). If honoring a patient's specific request, if covered entities must disclose amended PHI to groups or individuals outside the NHIN, they should adhere to the HIPAA's "minimum necessary" provision and follow procedures currently in place. *See* 45 C.F.R. §§ 164.502(b); 164..514(e) (2006).

the patient-provider relationship.[169] When attempting to amend PHI located within their EHR, individuals ought to deliver requests through their primary care provider.[170] If accepted, HHS should then require providers to inform all necessary parties, ensure the new information accurately enters the NHIN, and prompt patients to immediately acknowledge and verify the correction.

Aiding patients and covered entities alike, the NHIN will greatly facilitate HIPAA's amendment process. Because EHRs mirror the law's designated record set, most valid amendment requests should be honored. Patients should encounter minimal resistance, and the time between amendment requests and final action ought to greatly decrease. Most importantly, health care providers and others will be able to perform their duties while continually utilizing the most accurate information.[171]

c. Individual Right to PHI Accounting and Restrictions

HIPAA also creates a limited accounting right regarding PHI disclosures.[172] The main exceptions include: activity prior to the April 2003 compliance date,[173] PHI disclosures for TPO,[174] and PHI released pursuant to individual authorization,[175] law enforcement,[176] or national security.[177] Individuals may only demand an accounting for PHI disclosures covering a six-year period.[178]

Patients can request that covered entities only release their information for TPO purposes.[179] HIPAA also allows individuals to dictate how and where they receive their own PHI.[180] Covered entities must document, and comply with, reasonable

---

169. *See generally supra* note 25.

170. HIPAA specifically requires that patient amendment requests must pass through covered entities. 45 C.F.R. § 164.526(a)(1), (b)(1) (2006). *See also supra* note 160 and accompanying text.

171. *See generally* PRESIDENT BUSH'S HEALTH INFORMATION TECHNOLOGY PLAN, *supra* note 2.

172. 45 C.F.R. § 164.528(a)(1)(ix) (2006).

173. 45 C.F.R. § 164.528(a)(1)(ix).

174. 45 C.F.R. § 164.528(a)(1)(i) (2006). *See also* 45 C.F.R. § 164.506 (2006) (detailing PHI disclosures for TPO).

175. 45 C.F.R. § 164.528(a)(1)(iv) (2006). *See also* 45 C.F.R. § 164.508 (2006) (describing PHI releases pursuant to an individual's authorization).

176. 45 C.F.R. § 164.528(a)(1)(vii) (2006) (this also includes inmate PHI disclosures to correctional facilities).

177. 45 C.F.R. § 164.528(a)(1)(vi) (2006). *See also* 45 C.F.R. § 164.512(k)(2) (2006) (allowing PHI disclosures to designated federal officials for investigations under the "National Security Act," 50 U.S.C. § 401, et seq.).

178. 45 C.F.R. § 164.528(a)(3) (2006).

179. 45 C.F.R. § 164.522(a)(1)(i).

180. 45 C.F.R. § 164.522(b)(1) (2006). The Bush administration must be aware that patients, citing this provision, may refuse to register with HHS in order to view their own EHR. If so, covered entities would retain direct responsibility for honoring valid non-electronic access, amendment,

requests,[181] including instances where an individual's health and safety may be in danger.[182]

The NHIN should greatly empower patient accounting and restriction rights. Client-server technology will enable HHS to efficiently trace all network activity. In complying with HIPAA's "Security Rule,"[183] all covered entities must also monitor and safeguard their network activity.[184] As such, patients deserve broader network accounting rights. While maintaining HIPAA's law enforcement and national security exceptions, HHS should expand NHIN accounting rights to include all TPO disclosures.

The Bush administration ought to provide patients with the option to request NHIN accounting through either specific covered entities or their applicable RHIO.[185] Given the advantages that client-server technology provides, either option will ensure that valid accounting requests are quickly answered.[186] Unlike HIPAA's accounting right, HHS should require patients to initially contact their primary care provider, or applicable equivalent,[187] regarding PHI restrictions. Upon accepting a patient's request, providers should notify all necessary parties[188] and direct HHS to limit access to applicable TPO-related EHR sections. Should patients worry that a covered entity ignored their accepted restriction request, periodic accounting requests through their local RHIO ensure that any alleged misbehavior does not escape governmental review.

8. HIPAA Preemption and State Medical Privacy Law

HIPAA will only preempt state laws[189] with inferior privacy protections.[190] HIPAA preemption also applies when covered entities cannot possibly comply with both statutes or a state law frustrates HIPAA's goals.[191]

---

accounting, and restriction requests. As such, HHS may need to amend this provision in order to facilitate broad NHIN participation. *See supra* note 74 and accompanying text.

181. 45 C.F.R. § 164.522(b)(1)(I) (2006).

182. 45 C.F.R. § 164.522(b)(1)(ii) (2006).

183. 45 C.F.R. §§ 164.308; 164.310 (2006).

184. 45 C.F.R. § 164.312 (2006).

185. Similar to PHI access disputes, patients should also enjoy the right to ultimately appeal accounting and restriction disputes directly to HHS.

186. HHS should direct patients to first resolve accounting requests through applicable covered entities. This approach minimizes HHS's immediate involvement in potential accounting disputes and encourages patients to cultivate positive relationships with those most actively involved in administering care and processing their medical information.

187. *See supra* note 161 and accompanying text.

188. *See supra* note 168 and accompanying text.

189. HIPAA refers to state law as any "constitution, statute, regulation, rule, common law, or other State action having the force and effect of law." 45 C.F.R. § 160.202 (2006) ("state law").

190. *See generally* 45 C.F.R. § 164.203 (2006) (explaining how HIPAA's preemption

HIPAA will not supersede "more stringent" state law.[192] Typically "more stringent" state statutes contain tougher restrictions that limit PHI use or disclosure,[193] allow individuals broader rights to PHI access or amendment,[194] provide more focused notice,[195] or require greater detailed accounting practices.[196] Where HIPAA does not wholly preempt state law, it may supplement local practice and impart additional obligations.[197]

Although HIPAA operates as a national baseline for patient privacy protection, how the NHIN will interact with state medical privacy law remains unclear.[198] Through client-server technology, patient EHRs will electronically reside at a centrally managed location. Moreover, network participants will invariably operate in different states and access patient information from various locations.

In meeting the April 2003 compliance deadline,[199] health care organizations should already understand where HIPAA does not preempt applicable state law. Nonetheless, because simultaneously placating every state's medical privacy laws would be impractical,[200] network drafters should defer to HIPAA. Devising a HIPAA-compliant network provides two key advantages: 1) a cognizable framework

---

component interacts with existing state law). The Fourth Circuit affirmed this provision's constitutional health in S. Carolina Med. Ass'n v. Thompson, 327 F.3d 346, 354 (4th Cir. 2003).

191. 45 C.F.R. § 160.202, 203 (2006) ("contrary").

192. 45 C.F.R. § 160.202, 203(b) (2006) ("more stringent').

193. *See* 45 C.F.R. § 150.202(1) (2006).

194. *See* 45 C.F.R. § 160.202(2)(2006).

195. *See* 45 C.F.R. § 160.202(3)-(4) (2006); *see also* United States v. Diabetes Treatment Centers of Am., 2004 LEXIS 21830, 12-13 (D.D.C. May, 17 2004) (discussing patient notice requirements for third party disclosure and finding that Florida law is more stringent than HIPAA).

196. 45 C.F.R. § 160.202 (2006). "More stringent" also applies "with respect to any other matter, [that] provides greater privacy protection for the individual who is the subject of the individually identifiable health information." *Id.*

197. *See generally* 45 C.F.R. §§ 160.203(a) (2006); 160.204 (explaining, in part, that the HHS Secretary may also independently determine that HIPAA does not preempt particular state laws if they are necessary to prevent fraud and abuse, properly regulate insurance companies, continue state reporting for health care costs, or serve a compelling interest regarding health, safety, and welfare).

198. *See* HHS RFI, *supra* note 6, at 21-22 (detailing the role RHIOs could play in resolving discrepancies in federal and state medical privacy law regarding NHIN operation and management). For recent scholarship addressing HIPAA's interaction with state medical privacy law *see* Misty C. Boyer, *Texas Administrative Agencies Tackle Compliance With The Health Insurance Portability And Accountability Act's Privacy Rule*, 5 TEX. TECH. J. TEX. ADMIN. L. 87 (2004); Ko, *supra* note 59; Joy L. Pritts, *Altered States: State Health Privacy Laws and The Impact Of The Federal Health Privacy Rule*, 2 YALE J. HEALTH POL'Y L. & ETHICS 325 (2002); Tamela J. White & Charlotte A. Hoffman, *The Privacy Standards Under The Health Insurance Portability And Accountability Act: A Practical Guide To Promote Order And Avoid Potential Chaos*, 106 W. VA. L. REV. 709 (2004).

199. *See* 45 C.F.R. § 164.534 (2006).

200. *See* Wymore, *supra* note 56, at 560-64 (discussing the conflict in various state medical privacy laws).

for covered entities to evaluate how "more stringent" state medical privacy protections may apply to their NHIN activity;[201] and 2) a legally sound operating system, should state medical privacy law not apply to the NHIN.[202]

Nonetheless, in order to ensure that organizations do not initially balk at utilizing its NHIN, the federal government must provide additional guidance. Prior to granting access, HHS should require covered entities, business associates, and others to indicate a "home of record" and direct all participants to acknowledge written guidance regarding NHIN's potential impact on local medical privacy laws. As time elapses, the Department ought to explore devising state-specific NHIN software and implementing internal network protocols that preemptively limit NHIN access and use according to individual state laws.

Although federal courts are certain to wrestle with how the NHIN, HIPAA, and state medical privacy laws intersect, the federal government must empower and assist local organizations in preparing for this foreseeable legal uncertainty. If neglected, confidence in HHS's ability to competently manage the national use and exchange of electronic patient health information will likely plummet.

B. *HIPAA's Security Rule*

Effective April 2005,[203] HIPAA's security protections require covered entities to protect the integrity and availability of all electronic PHI that they create, receive,

---

201. *See* P. Greg Gulick, *E-Health and the Future of Medicine: The Economic, Legal, Regulatory, Cultural, and Organizational Obstacles Facing Telemedicine and Cybermedicine Programs*, 12 ALB. L.J. SCI. & TECH. 351, 405-06 (2002) (proposing a "Center for E-Health Services" to help simplify regulatory ambiguity between federal, state, and local government regarding electronic health information).

202. *See id.* at 386-87 (2003) (describing Quintiles Transnational Corporation v. WebMD, No. 5:01-CV-180-BO(3) (E.D.N.C. Mar. 21, 2001), *available at* http://world.std.com/~goldberg/quintilesorder.pdf, where a federal district court initially held that the U.S. Constitution's commerce clause prohibited state medical privacy laws from regulating the interstate transmission of PHI). Complete federal preemption regarding state attempts to regulate Internet transactions continues to curry favor with jurists and lawmakers. *See* Rebecca Bishop, *The Final Patient Privacy Regulations Under the Health Insurance Portability and Accountability Act - Promoting Patient Privacy or Public Confusion?*, 37 GA. L. REV. 723, 749-53 (2003) (discussing the Quintiles lawsuit and the U.S. Supreme Court's growing sympathy toward complete preemption in Geier v. American Hondo Motor Co., 529 U.S. 861 (2000)); *see also* Ko, *supra* note 59 at 526 (citing Workgroup for Elec. Data Interchange, Preemption White Paper 8-9, 11-12 (2003)).

203. 45 C.F.R. § 164.318 (2006).

maintain, or transmit.[204] Covered entities must also "protect against any reasonably anticipated threats or hazards to data security or integrity."[205]

To ensure compliance, HIPAA grants broad flexibility to covered entities. In addition to considering costs and the likelihood of security threats, covered entities must also examine their own size and technological capabilities.[206] For implementation specifics, HIPAA also differentiates between "required" and "addressable" security mandates.[207] Covered entities must employ "required" provisions,[208] but may examine environmental and feasibility factors when deciding to enact "addressable" safeguards.[209]

Given the vast amount of patient PHI that participants will use and access through the NHIN, HHS must work diligently to address all foreseeable security issues.[210] Conversely, the Department must demand heightened security precautions from all network participants. Although HIPAA only compels covered entities to abide by its "required" implementation standards,[211] HHS should utilize HIPAA's "Security Rule" as the template for NHIN security management. As such, the Bush administration must demand that all NHIN participants abide by the law's mandatory provisions.

1. Administrative Safeguards

HIPAA requires covered entities to "implement policies and procedures to prevent, detect, contain, and correct security violations."[212] Specifically, they must

---

204. 45 C.F.R. § 164.306(a)(1) (2006). Due to the constantly evolving state of computer technology, this article does not attempt to address technological specifics. Instead, this section offers common-sense ideas that HHS can immediately implement to allay security fears prior to NHIN implementation.

205. 45 C.F.R. § 164.306(a)(2) (2006).

206. 45 C.F.R. § 164.306(b)(1)-(2) (2006).

207. 45 C.F.R. § 164.306(d)(1) (2006).

208. 45 C.F.R. § 164.306(d)(2) (2006).

209. 45 C.F.R. § 164.306(d)(3) (2006). If an "addressable" mandate is reasonable and appropriate, the covered entity must implement the provision or document its decision to utilize an equivalent alternative. 45 C.F.R. § 164.306(d)(3)(i)-(ii) (2006). Regardless, this portion of the article will only explore HIPAA's "required" security mandates.

210. Before the NHIN becomes reality, the Bush administration must ensure that HHS has resolved it own electronic security flaws. According to the United States House of Representatives' Committee on Government Reform, HHS deserved an "F" grade regarding computer security in 2003 and 2004. *See* FEDERAL COMPUTER SECURITY REPORT CARD, HOUSE. COMM. ON GOV'T REFORM, 108th Cong. (2004) *available at* http://reform.house.gov/UploadedFiles/2004%20Computer%20Security%20Report%20card%202%20years.pdf.

211. 45 C.F.R. § 164.302 (2006). Covered entities must also document their security policies and procedures in writing. 45 C.F.R. § 164.316(b)(1) (2006).

212. 45 C.F.R. § 164.308(a)(1)(i) (2006).

conduct a risk analysis of electronic PHI confidentiality, integrity, and availability.[213] Covered entities shall also implement appropriate safeguards to reduce threats and vulnerabilities.[214]

Covered entities must develop and utilize procedures to "review records of information system activity."[215] They shall assess and train their work force and only as needed, assign individual electronic PHI access privileges.[216] HIPAA also requires covered entities to identify, document, and remedy suspected security breaches.[217] They must implement contingency plans to back up and store copies of electronic PHI.[218] In addition, covered entities shall conduct regular technical and non-technical evaluations to ensure their electronic PHI remains properly secure.[219]

Because HHS will utilize client-server technology in order to manage and operate its NHIN,[220] it must ensure that all users meet these strict guidelines. Although the Department cannot possibly monitor every worksite, it can take preventative measures to maximize NHIN security.

First, HHS should require that all network participants submit an annual NHIN security report. Authored by each organization's Security Official,[221] the report would assure the Department that each participant both implemented and adhered to HIPAA's administrative safeguards.[222] The reports should also indicate how

---

213. 45 C.F.R. § 164.308(a)(1)(ii)(A) (2006). If a covered entity contains a healthcare clearinghouse component, it must separate those activities. 45 C.F.R. § 164.308(a)(4)(ii)(A). The covered entity must separately craft distinct policies and procedures to protect the clearinghouse's PHI from unauthorized access and use. *Id.* Accordingly, HHS should require these hybrid-covered entities to devise NHIN-specific security policies and procedures for each covered function.

214. 45 C.F.R. § 164.308(a)(1)(ii)(B) (2006).

215. 45 C.F.R. § 164.308(a)(1)(ii)(D) (2006).

216. 45 C.F.R. § 164.308(a)(3)(i) (2006).

217. 45 C.F.R. § 164.308(a)(6)(ii) (2006).

218. 45 C.F.R. § 164.308(a)(7)(ii)(A) (2006).

219. 45 C.F.R. § 164.308(a)(8) (2006). Covered entities must also obtain and document satisfactory assurances from their business associates that they will employ adequate security safeguards when creating, using, or disclosing electronic PHI. 45 C.F.R. §§ 164.308(a)(8)(b)(4); 164.314(a)(1)-(2) (2006). *See also supra* notes 95-96 (detailing how business associate contract language incorporates this provision).

220. *See* 45 C.F.R. § 164.306 (2006). Because HHS will retain sole control over the NHIN, it must also engage its own review and implement policies that ensure maximum security. *See* 45 C.R.F. § 164.308. These steps would include: data backups, audit trails, disaster prevention, and authentication software. *See* C.F.R. § 164.308(a)(1)-(7) (2006).

221. HIPAA requires each covered entity to appoint a "Security Official" to ensure security compliance. 45 C.F.R. § 164.308(a)(2) (2006). They shall also administer sanctions against employees that violate HIPAA security provisions. 45 C.F.R. § 164.308(a)(1)(ii)(C) (2006). HHS should also require each Security Official to receive NHIN-specific training and serve as a liaison to the Department regarding all NHIN security issues.

222. *See also* Jurevic, *supra* note 21, at 821-24 (urging strong security measures for computers and health care information, including the use of background checks and confidentiality

participants have upheld NHIN security and appropriately addressed security threats and violations.

Second, HHS should coordinate with the private sector to create, provide, and continually update specific software that enables access to the NHIN. Upon authenticating covered entities, businesses associates and others for NHIN access,[223] HHS should individually permit Security Officials to download NHIN software for their organization through the Department's website. In addition to minimizing unauthorized use, universally mandated NHIN software will help guarantee that users access the network in the same manner. Streamlining how participants access the NHIN provides HHS with the best opportunity to uniformly combat emerging security threats.[224]

Finally, HHS should require annual security training for all authorized NHIN users. Coordinated through a participant's Security Official, yearly training would minimize data entry errors and ensure PHI integrity.[225] NHIN participants should also document each session in their annual report. In turn, the Department will be able to collect and analyze various procedures as well as implement future uniform training guidelines for all NHIN users.

2. Physical and Technical Safeguards

HIPAA also requires covered entities to establish individual physical security procedures to limit electronic access to patient PHI.[226] Covered entities must ensure that computer workstations function properly and contain safeguards that prohibit unintended PHI access.[227] In addition to utilizing software that monitors computer activity,[228] covered entities must protect PHI from improper modification and destruction.[229]

For their workforce members, covered entities are required to create individual authorization mechanisms for those required to access patient PHI.[230] Most pertinent

---

agreements for all authorized individuals).

223. *See supra* note 167 and accompanying text.

224. *See e.g.*, Benjamin D. Kern, *Whacking, Joyriding & War-Driving: Roaming Use of Wi-Fi & the Law*, 21 SANTA CLARA COMPUTER & HIGH TECH. L.J. 101, 111-14 (2004) (describing the inherent security threats to wireless fidelity networks due to lack of access uniformity).

225. Jurevic, *supra* note 21, at 827 ("An estimated 75% of data security problems in health care institutions result from the failure to properly train employees on what constitutes a breach and how to avoid it").

226. 45 C.F.R. § 164.310(a)(1) (2006).

227. 45 C.F.R. §§ 164.310(b)-(c) (2006).

228. 45 C.F.R. § 164.312(b) (2006).

229. 45 C.F.R. § 164.312(c)(1) (2006). Covered entities must also implement operational procedures for properly discarding, or reusing, electronic software containing patient PHI. 45 C.F.R. § 164.310(d)(2)(i)-(ii) (2006).

230. 45 C.F.R. § 164.312(a)(1) (2006).

to the NHIN, covered entities must implement procedures to "guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network."[231] Further, covered entities are required to establish procedures for electronic PHI access during emergencies.[232]

Similar to HIPAA's administrative requirements, HHS should specifically demand all network participants indicate their full compliance with the law's physical and technical safeguards.[233] HHS should require all NHIN users to maintain and examine audit trials of their own network activity, conduct periodic simulated emergency drills, and include appropriate analysis in their Security Official's annual report.

For workforce computers, HHS should require that all NHIN activity occur through specified stationary machines.[234] The Department should also mandate that all NHIN-capable computers utilize technology that immediately recognizes authorized individual users and automatically disconnects from the network after a specified period of inactivity.[235]

To further aid NHIN participants in physically securing electronic patient PHI from unauthorized use and improper alteration, HHS should provide specific technological assistance. In addition to NHIN software, the Department should employ firewalls and transmission control protocol wrappers.[236] It should also require all network users to utilize standardized NHIN-specific smart card devices.[237] In addition, HHS should recommend and authorize security programs that NHIN users may utilize to further safeguard PHI.[238]

---

231. 45 C.F.R. § 164.312(e)(1) (2006).

232. 45 C.F.R. § 164.312(a)(2)(ii) (2006).

233. NHIN participants should include this information in their individual memorandums of understanding and their Security Official's annual report to HHS.

234. *See* Jurevic, *supra* note 21, at 821, 823, 827 (arguing that laptop computers are too prone to theft and infrequently used computers should be placed behind locked doors and individual workstations disabled from reading CDs and floppy disks).

235. *See also supra* note 89 and accompanying text.

236. *See also* Jurevic, *supra* note 21, at 823-24 (proposing the use of firewalls, transmission control protocol wrappers, single-session passwords, and encryption technology). Firewalls involve the point of network entry for authorized users. *Id.* at 823 n.90 (citing FOR THE RECORD, Ch. 4, p. 13, (1997) http://www.nap.edu/catalog/5595.html). They help limit network access and functions according to a list of authorized users and locations. *Id.* Transmission control protocol wrappers intercept network communications. Jurevic, *supra* note 21, at 823 n.91. They assist in performing security screening by limiting the date, time, duration, and location that network information can be viewed or altered. *See id.*

237. *See supra* note 84 and accompanying text.

238. *See* HHS RFI, *supra* note 6, at 35 (detailing specific programs such as: XML Encryption, Public Key Cryptography Standards, Security Assertion Markup Language, and E31.20 Data and System Security for Health Information).

As computer technology continues to evolve, HHS will inevitably need to develop additional safety measures. Nonetheless, by faithfully adhering to HIPAA's security mandates during initial NHIN creation and implementation, HHS and network participants will be able to rely on a sound organizational foundation to collectively address future threats and concerns. By demonstrating a proactive, universal approach to NHIN security, the Bush administration will also continue to gain the trust of lawmakers, patients, and other health care participants.

V. CONCLUSION

The Bush administration's plan for a national health care information network offers an abundance of promise. Once fully realized, the NHIN will empower authorized users to access medical information from anywhere in the country. It will also revolutionize how patients, providers, and others interact under our present health care system. While almost certain to improve efficiency and reduce costs, the network also presents the federal government with grave challenges.

Given the highly sensitive nature of medical information, the health care industry and network architects face complex, transitional hurdles. Moreover, the Bush administration must work to convince patients, lawmakers, and others that increased performance is compatible with meaningful medical privacy protection. Instead of eschewing HIPAA, the Bush administration should direct HHS to utilize the law—and its privacy and security regulations—to devise, implement, and manage the NHIN.

HIPAA provides network drafters with a familiar national framework to organize and regulate NHIN access and use. By using HIPAA, the federal government conveys to patients that it does not intend to use the NHIN to weaken privacy or autonomy. This approach relieves providers, hospitals, insurers, and others from new and unnecessary regulatory burdens. It also provides opportunities to uncover and remedy operational defects in the law, further empowers patient rights, and ensures that federal medical privacy law keeps pace with the evolving digital landscape.

As Americans grow increasingly comfortable with the instant convenience that computer technology provides, the U.S. health care system must follow suit. Yet, without the faith and confidence of those who will fund and utilize it, any attempts at establishing a national health care network are destined to fail.