SCHOOL OF LAW
CASE WESTERN RESERVE UNIVERSITY

Health Matrix: The Journal of Law-Medicine

Volume 24 | Issue 1

2015

Sustainable Access to Data for Postmarketing Medical Product Safety Surveillance under the Amended HIPAA Privacy Rule

Barbara J. Evans

— Symposium —

SUSTAINABLE ACCESS TO DATA FOR POSTMARKETING MEDICAL PRODUCT SAFETY SURVEILLANCE UNDER THE AMENDED HIPAA PRIVACY RULE

Barbara J. Evans†

CONTENTS

INTRODUCTION

Pharmacoepidemiology explores "the use of and the effects of drugs in large numbers of people."[1] The Food and Drug Administration Amendments Act of 2007 (FDAAA)[2] authorized the U.S. Food and Drug Administration (FDA) to carry out a program of postmarketing drug safety surveillance that relies heavily on pharmacoepidemiological studies to assess safety risks with already-approved drugs.[3] To implement this

† Professor of Law and George Butler Research Professor; Director, Center on Biotechnology & Law, University of Houston Law Center, bjevans@central.uh.edu. This research was supported by grants from the Greenwall Foundation Faculty Scholars Program in Bioethics and the University of Houston Law Foundation.

1. *See* Brian L. Strom, *What is Pharmacoepidemiology?*, *in* PHARMACOEPIDEMIOLOGY 3, 3 (Brian L. Strom ed., 4th ed. 2005).

2. Pub. L. No. 110-85, 121 Stat. 823 (2007) (codified as amended in scattered sections of 21 U.S.C.).

3. 21 U.S.C. § 355(k)(3)(B)(ii) (2012) (setting targets of twenty-five million persons by July 2010 and 100 million by July 2012). *See also id.*

program, the agency is developing the Sentinel system,[4] a very large-scale health information infrastructure, and its pilot phase, Mini-Sentinel (together, Sentinel). Mini-Sentinel already includes health data for ninety-nine million persons.[5] Large-scale data infrastructures for postmarketing drug safety surveillance also exist in Canada,[6] the European Union,[7] and Japan.[8]

---

§ 355(k)(3)(C) (describing the new "postmarket risk identification and analysis system").

4. U.S. FOOD & DRUG ADMIN., THE SENTINEL INITIATIVE (2008), *available at* http://www.fda.gov/downloads/Safety/FDAsSentinelInitiative/UCM124701.pdf (discussing the goals and structure of the Sentinel data network). *See also FDA's Sentinel Initiative*, U.S. FOOD & DRUG ADMIN., http://www.fda.gov/Safety/FDAsSentinelInitiative/default.htm (last modified Jan. 13, 2014) (providing information about the current status of Sentinel System development).

5. Lesley Curtis et al., *Design Considerations, Architecture, and Use of the Mini-Sentinel Distributed Data System*, 21 PHARMACOEPIDEMIOLOGY & DRUG SAFETY 23, 28 (2012). *See also* Press Release, U.S. Food & Drug Admin., FDA Awards Contract to Harvard Pilgrim to Develop Pilot for Safety Monitoring System (Jan. 8, 2010), http://www.fda.gov/NewsEvents/Newsroom/PressAnnouncements/ucm196968.htm; Rachel E. Behrman et al., *Developing the Sentinel System — A National Resource for Evidence Development*, 364 NEW ENG. J. MED. 498, 498 (2011).

6. *See About DSEN*, CANADA INST. OF HEALTH RESEARCH, http://www.cihr-irsc.gc.ca/e/39389.html (last modified October 14, 2012) (describing Canada's DSEN network).

7. *See* Press Release, European Medicines Agency, EMEA-Coordinated PROTECT Project Has Been Accepted for Funding by the Innovative Medicines Initiative Joint Undertaking (Apr. 30, 2009), http://www.ema.europa.eu/ema/index.jsp?curl=pages/news_and_events/news/2009/11/news_detail_000096.jsp&jsenabled=true (describing the PROTECT network); EUR. MEDS. AGENCY, IMPLEMENTATION OF THE ACTION PLAN TO FURTHER PROGRESS THE EUROPEAN RISK MANAGEMENT STRATEGY: ROLLING TWO-YEAR WORK PROGRAMME (2008–2009) (2007), http://www.emea.europa.eu/pdfs/human/phv/28008907en.pdf (describing the ENCePP data network); *What is ENCePP?*, EUR. NETWORK OF CTRS. FOR PHARMACOEPIDEMIOLOGY AND PHARMACOVIGILANCE, http://encepp.eu/structure/index.shtml (last visited Jan. 12, 2014); EU-ADR, http://www.alert-project.org/ (last visited Jan. 14, 2014) (describing the European Union adverse drug reactions data network).

8. Kaoru Misawa, Dir., Office of Safety, Pharm. & Med. Devices Agency, Address at the 9th Kitasato University-Harvard School of Public Health Symposium: Sentinel Initiative in Japan: Utilization of Electronic Health Information in Pharmacovigilance 7–14 (Sept. 12, 2009), *available at* http://www.pharm.kitasato-u.ac.jp/biostatis/khsympo200909/doc/misawa.pdf.

Such systems present privacy and ethical issues that have been extensively discussed elsewhere.[9] This article takes as its starting assumptions that many members of the public support the goal of reducing medical product injuries and that postmarketing surveillance programs can advance that goal. The article explores the challenge of ensuring a sustainable supply of data for these purposes and asks whether recent amendments to the HIPAA Privacy Rule[10] have met that challenge. It concludes that the amendments move closer to but ultimately fall short of resolving this challenge.

I. THE CHALLENGE OF SUSTAINABLE DATA ACCESS

Raw patient health data —the records of a patient's encounters with the healthcare system —are not in themselves a very useful resource for postmarketing surveillance of drugs and other medical products.[11] To be useful, each individual's data must be longitudinally linked to create a chronological record that reflects diagnoses, treatments (including which medical products the patient used), and outcomes.[12] Pharmacoepidemiological studies typically need longitudinal records for large numbers of patients because the product-related injuries of interest often are very rare, making it difficult to detect statistically significant patterns between the use of specific medical products and specific

9. *See, e.g.*, KRISTEN ROSATI ET AL., HIPAA AND COMMON RULE COMPLIANCE IN THE MINI-SENTINEL PILOT 1, 7 (2010), *available at* http://mini-sentinel.org/work_products/About_Us/HIPAA_and_CommonRuleCompliance_in_the_Mini-SentinelPilot.pdf (examining privacy and human-subjects protection laws affecting FDA's postmarket drug safety surveillance activities); KRISTEN ROSATI, AN ANALYSIS OF LEGAL ISSUES RELATED TO STRUCTURING FDA SENTINEL INITIATIVE ACTIVITIES (2009), *available at* http://www.regulations.gov/contentStreamer?objectId=0900006480e4aa00&disposition=attachment&contentType=pdf (same); Deven McGraw et al., *A Policy Framework for Public Health Uses of Electronic Health Data*, 21 PHARMACOEPIDEMIOLOGY & DRUG SAFETY 18, 19 (2012) (describing privacy and human-subject protections implemented by the FDA's Mini-Sentinel pilot project); Barbara J. Evans, *Authority of the Food and Drug Administration to Require Data Access and Control Use Rights in the Sentinel Data Network*, 65 FOOD & DRUG L.J. 67 (2010) [hereinafter Evans, *Authority of the FDA*]; Barbara J. Evans, *Congress' New Infrastructural Model of Medical Privacy*, 84 NOTRE DAME L. REV. 585 (2009) [hereinafter Evans, *Congress' New Infrastructural Model*].

10. 45 C.F.R. pts. 160, 164 (2013) (implementing privacy protections of the Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub. L. No. 104-191, 110 Stat. 1936 (codified as amended in scattered sections of 18, 26, 29, 42 U.S.C.)).

11. Barbara J. Evans, *Much Ado About Data Ownership*, 25 HARV. J.L. & TECH. 69, 90-92 (2011) [hereinafter Evans, *Data Ownership*].

12. *Id.* at 93-94.

injuries. Such studies sometimes require highly inclusive datasets that capture data for most or all of the people who have been exposed to the product. In some cases, even the small biases associated with letting patients "opt in" or "opt out" of having their data used may materially distort the study results.[13] Postmarketing medical product safety surveillance sometimes requires extremely large-scale information assets encompassing longitudinally linked records for tens or hundreds of millions of people.[14]

The various entities that hold raw health data, such as insurers and healthcare providers, do not maintain patients' health information in a standardized format.[15] Each dataset must be translated into a common format before data from different sources can be linked longitudinally (for individual patients) or meaningfully compared (across different patients). This process requires significant inputs of skilled labor and information infrastructure such as software systems.[16] Once the datasets are in a common format, they must be brought together so that they can be used to answer specific questions about medical product safety.

Various system architectures can bring large amounts of data together.[17] Perhaps the most obvious approach is to deposit the data in a large, central database. Centralization of the large amount of data required by medical product safety surveillance, however, has various practical and privacy disadvantages.[18] An alternative seen in many recent postmarketing drug safety surveillance systems is to adopt a distributed network architecture.[19] In a distributed network, individuals' health data stays at its original location, such as a healthcare provider's or insurer's database. These data holders link their datasets together virtually by converting their data into an agreed common format and

13. *Id.* at 95-98.

14. *See, e.g.,* Curtis et al, *supra* note 5, at 28 (describing Mini-Sentinel's ninety-million-person data assets).

15. PRESIDENT'S COUNCIL OF ADVISORS ON SCI. AND TECH., EXEC. OFFICE OF THE PRESIDENT, REPORT TO THE PRESIDENT: REALIZING THE FULL POTENTIAL OF HEALTH INFORMATION TECHNOLOGY TO IMPROVE HEALTHCARE FOR AMERICANS: THE PATH FORWARD 39 (2010).

16. Evans, *Data Ownership*, *supra* note 11, at 99-101.

17. *See* HEALTHCARE INFO. AND MGMT. SYS. SOC'Y, A HIMSS GUIDE TO PARTICIPATING IN A HEALTH INFORMATION EXCHANGE 15–20 (2009), *available at* http://www.himss.org/content/files/HIE/HIE_GuideWhitePaper.pdf (discussing an array of possible architectures, including centralized, decentralized (federated), and hybrid models).

18. Carol C. Diamond et al., *Collecting and Sharing Data For Population Health: A New Paradigm*, 28 HEALTH AFFS. 454, 456 (2009).

19. *See, e.g.*, Behrman et al., *supra* note 5, at 499 (describing the Sentinel system's distributed architecture).

responding to queries using their respective data assets; these piecemeal responses are then aggregated into an integrated response to the question at hand.[20] In a distributed data network, data-holding institutions are not just suppliers of data; they also supply services.[21] The services involve tasks such as: searching through their records to identify data relevant to a specific query; retrieving that information and converting it into the agreed common format; studying it to develop responses to the query; and transmitting the results.[22]

Either option – creating centralized data assets or bringing data together virtually – requires significant investments of labor, information infrastructure, and, of course, money. It is overly simplistic to portray raw patient health data as valuable information assets in themselves. Raw data are *made* valuable, for purposes of postmarketing safety surveillance, only by investing labor and developing information infrastructure to facilitate the operations just described.

A critical question is how to incentivize the necessary investments in information infrastructure so that the needed data resources will be available on a sustainable basis now and in the future. Compulsory approaches to data access are one way to procure data to use in postmarketing surveillance: simply force data holders to make their data available for these activities. This approach echoes Professor Marc Rodwin's proposal to enact legislation requiring data holders to report data in de-identified form for creation of a publicly owned national database to support various research and public health activities.[23] Unfortunately, collecting raw, de-identified health data in a public database would not by itself create a useful information asset for postmarketing surveillance. To make the data useful, data holders also would need to supply services and develop the infrastructure to convert their data into a common format before reporting the data. Compulsory provision of services –forcing civilians to do work for the government –is fraught with legal problems in the United States' system of law.[24] Moreover, if each data holder reports the raw data in de-identified

20. Evans, *Data Ownership*, *supra* note 11, at 99-101.

21. *Id.* at 101.

22. OFFICE OF THE NAT'L COORDINATOR FOR HEALTH IT, DEP'T OF HEALTH & HUMAN SERVS., SUMMARY OF THE NHIN PROTOTYPE ARCHITECTURE 33 tbl. 6 (2007), *available at* http://www.healthit.gov/sites/default/files/summary_report_on_nhin_prototype_architectures.pdf (listing data services that health information networks provide, such as "secure data delivery;" "data look-up, retrieval, and location registries;" and "data anonymization").

23. Marc A. Rodwin, *Patient Data: Property, Privacy & the Public Interest*, 36 AM. J.L. & MED. 586, 589 (2010) (arguing for public ownership of de-identified patient data).

24. Evans, *Data Ownership*, *supra* note 11, at 106-07.

format, the centralized database will not be able to link the data longitudinally because at least some identifying information must be shared in order to establish that data received from various sources relate to the same individual.[25] Compulsory sharing of health data in identified form would raise serious privacy concerns.

An additional critique of compulsory approaches is that they may not ensure sustainable access to data over the long term. Such approaches favor static efficiency over dynamic efficiency: static efficiency focuses on how best to allocate rights to data that already exist today, whereas dynamic efficiency focuses on ensuring adequate supplies of data for the future.[26] Entities that hold rich stores of health data often have invested substantial sums of private capital to develop their datasets and related infrastructures. Forcing them to donate their data may be statically efficient in the sense of meeting today's immediate needs for data, but it also may destroy incentives for them to invest in developing data for future uses.

Expropriating private assets has not been an effective approach in other infrastructure industries where it has been tried. The U.S. is the only nation that kept its large energy and resource infrastructures, such as oil and gas pipelines, under private ownership throughout the twentieth century.[27] Many nations around the world placed such assets under governmental ownership during the middle decades of the twentieth century.[28] As that century ended, however, governments in many nations were backing away from public ownership of these assets in an effort to restore investment incentives and efficiencies lost through the earlier expropriations.[29] Forcing infrastructure investors to donate their information assets and services to the public understandably diminishes the incentives to develop future assets. For this reason, compulsory data access schemes seem unlikely to ensure sustainable supplies of data and information infrastructure to support postmarketing surveillance activities on a long-term basis. And medical product safety is, if anything, a

25. Evans, *Authority of the FDA*, *supra* note 9, at 76-77.

26. Daniel F. Spulber & Christopher S. Yoo, *Mandating Access to Telecom and the Internet: the Hidden Side of Trinko*, 107 COLUM. L. REV. 1822, 1843 (2007).

27. JOSÉ A. GÓMEZ-IBÁÑEZ, REGULATING INFRASTRUCTURE: MONOPOLY, CONTRACTS, AND DISCRETION 4-6 (2003); Jim Chen, *The Nature of the Public Utility: Infrastructure, the Market, and the Law*, 98 NW. U. L. REV. 1617, 1618 (2004).

28. *See* Chen, *supra* note 27, at 1632 (quoting GÓMEZ-IBÁÑEZ, *supra* note 27, at 2).

29. *See* Daniela Klingebiel & Jeff Ruster, *Why Infrastructure Financing Facilities Often Fall Short of Their Objectives* (World Ban, Working Paper No. 2358, 2000), *available at* http://www-wds.worldbank.org/external/default/WDSContentServer/WDSP/IB/2000/07/07/000094946_00062305373440/Rendered/PDF/multi_page.pdf.

long-term problem that requires ongoing study; it is not susceptible to a one-time solution.

Because compulsory data access schemes have so many problems, there is ongoing interest in non-compulsory (voluntary) approaches. These can include both donative and market-oriented approaches. Donative approaches rely on the goodwill of data holders to make their data available *gratis* for use in postmarketing surveillance activities. Market-oriented approaches are still voluntary in the sense that data holders are not forced to supply data and related services, but these approaches harness economic incentives to help overcome the natural human reluctance to share. The Health Information Technology for Economic and Clinical Health (HITECH) Act,[30] enacted in 2009 as part of economic stimulus legislation,[31] called for changes to the HIPAA Privacy Rule. HITECH recognized that donative approaches to data access, by themselves, may be unable to meet the needs of important research and public health activities that require access to health data.

The Office for Civil Rights (OCR) within the U.S. Department of Health and Human Services (HHS) initiated proceedings[32] in 2010 to modernize the HIPAA Privacy Rule and to implement the HITECH Act. The final amendments appeared in the Omnibus HIPAA Privacy Rule revisions published in January 2013.[33] This article explores how the amended HIPAA Privacy Rule approaches the problem of ensuring access to data for research and public health uses, including pharmacoepidemiological studies.

II. THE HITECH ACT'S REGULATED PRICE OF INFRASTRUCTURE SERVICES

The HITECH Act restricts sales of health data[34] by making it unlawful for HIPAA-covered entities and their business associates to exchange an individual's protected health information (PHI) for direct or indirect

30. Pub. L. 111-5, Div. A, Title XIII, § 13101, 123 Stat. 228, 242 (2009) (codified as amended at 42 U.S.C § 300jj-19).

31. American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5, 123 Stat. 115 (2009) (codified as amended in scattered sections of 26 U.S.C.).

32. Modifications to the HIPAA Privacy, Security, and Enforcement Rules under the Health Information Technology for Economic and Clinical Health Act, 75 Fed. Reg. 40,868 (July 14, 2010) (to be codified at 45 C.F.R. Parts 160 &164).

33. Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules, 78 Fed. Reg. 5566 (Jan. 25, 2013) (to be codified at 45 C.F.R. pts. 160 & 164).

34. 42 U.S.C. § 17935(d) (Supp. V 2012).

remuneration unless the individual authorizes the transaction.[35] This restriction does, however, have exceptions.[36] These exceptions allow data holders to receive certain fees in exchange for providing data. As a result, HITECH moves from a purely donative model of data sharing to one that envisions at least some use of economic incentives.

When supplying data to researchers under a HIPAA waiver[37] (in other words, without individual authorization), data holders may charge a price so long as "the price charged reflects the costs of preparation and transmittal of the data."[38] The HIPAA waiver provision, along with related provisions for waiving informed consent under the Common Rule,[39] is one of the major pathways for acquiring health data to use in large-scale studies where it may be impracticable to contact each individual to obtain a privacy authorization.[40] Of importance, HIPAA waivers do not necessarily require that data be de-identified prior to sharing, thus making it possible to supply raw data along with the identifiers that will be needed to assemble the data into longitudinal health records.[41] When granting a waiver, an Institutional Review Board (IRB) or privacy board approves the sharing of data without the affected individuals' permission.[42] HITECH allows this practice to continue so long as data holders do not charge more than the cost-based fee when supplying data under a waiver.[43]

HITECH's cost-based fee is not actually a price for the data. Whether the data holder or the patient "owns" the data is a question of state law and is murky in many states.[44] Data holders obviously cannot sell

35. § 17935(d)(1).

36. § 17935(d)(2).

37. 45 C.F.R. § 164.512(i) (2013).

38. 42 U.S.C. § 17935(d)(2)(B).

39. Basic HHS Policy for Protection of Human Research Subjects, 45 C.F.R. § 46.101–124 (2013). *See also id.* at § 46.116(d) (providing a mechanism for waiver of informed consent upon approval by an IRB).

40. COMM. ON HEALTH RESEARCH & THE PRIVACY OF HEALTH INFO., INST. OF MED., BEYOND THE HIPAA PRIVACY RULE: ENHANCING PRIVACY, IMPROVING HEALTH THROUGH RESEARCH 167-68 (Sharyl J. Nass, Laura A. Levit & Lawrence O. Gostin eds., 2009) [hereinafter IOM, PRIVACY REPORT], *available at* http://www.nap.edu/catalog/12458.html.

41. *See, e.g.*, Evans, *Authority of the FDA*, *supra* note 9, at 76-77.

42. *Id.*

43. 42 U.S.C. § 17935(d)(2)(B) (allowing sales priced at the cost-based fee under the Privacy Rule's waiver provision, 45 C.F.R. § 164.512(i), which allows disclosure to researchers without individual authorization).

44. *See* Paul M. Schwartz, *Property, Privacy, and Personal Data,* 117 HARV. L. REV. 2055, 2076-94 (2004) (discussing conceptual difficulties in applying property rights to information held in databases); David L. Silverman, *Data Security Breaches: The State of Notification Laws*, 19 INTELL. PROP.

the data if they do not legally own it.[45] What data holders own is the health information infrastructure (computer systems, software, and communications equipment) that supports their regular business activities. The cost-based fee is intended to cover infrastructure services: services that data holders perform to prepare and transmit data with the use of their information infrastructures.[46] Colloquially, the phrase "data provisioning" is sometimes used to describe services that make data available to users, and this article uses that phrase as shorthand for data preparation and transmittal. The data are supplied *gratis*, and the HITECH Act's fee[47] covers services a data holder provides during the process of supplying the data. Whether the public whose data are being trafficked will understand this nuance is not clear.

HHS recently implemented HITECH's cost-based fee by amending the HIPAA Privacy Rule.[48] The amended HIPAA regulations define "sale of protected health information" as a "disclosure of protected health information by a covered entity or business associate" where the disclosing entity "directly or indirectly receives remuneration from or on behalf of the recipient of the protected health information in exchange for the protected health information."[49] The HIPAA regulations, like HITECH, then provide various exceptions to this basic definition.[50]

One exception is that disclosures for public health purposes are not considered sales of PHI.[51] This exception includes disclosures made under the existing HIPAA exception that allows unconsented use of data for various public health uses,[52] and it also includes public health uses of limited data sets.[53] Another exception covers disclosures of data for use in research under the HIPAA waiver provision[54] or as a limited data set.

& TECH. L. J. 5, 8 (2007) (noting that "ownership of the contents of a database is a precarious concept in the United States.").

45. Mark A. Hall & Kevin A. Schulman, *Ownership of Medical Information*, 301 JAMA 1282, 1282-84 (2009); Silverman, *supra* note 44, at 8.

46. 42 U.S.C. § 17935(d)(2)(B).

47. *Id.*

48. *See* Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules, 78 Fed. Reg. 5566, 5655 (Jan. 25, 2013) (to be codified at 45 C.F.R. § 164.410).

49. 78 Fed. Reg. at 5697 (inserting a definition of "sale of protected health information" at 45 C.F.R. § 164.502(a)(5)(ii)(B)(1)).

50. 45 C.F.R. § 164.502(a)(5)(ii)(B)(2).

51. § 164.502(a)(5)(ii)(B)(2)(i).

52. § 164.512(b).

53. § 164.514(e).

54. § 164.512(i).

Such disclosures are not considered sales of PHI provided the only remuneration received is "a reasonable cost-based fee to cover the cost to prepare and transmit the protected health information for such purposes."[55] Thus, research disclosures are subject to a price cap in the form of the reasonable cost-based fee, whereas public health disclosures are not subject to a price cap. Sales of PHI are subject to several additional exceptions that are not relevant to this discussion.[56] Also, PHI can be sold without any restriction on pricing if the affected individual authorizes the sale after being informed that his or her data is being disclosed for remuneration.[57]

III. THE DUBIOUS CONCEPT OF A PRICE ELASTICITY OF INFORMATIONAL PRIVACY

HIPAA's new cost-based fee for data preparation and transmission echoes pricing schemes traditionally used in other infrastructure industries. Cost-of-service pricing was widely used in American infrastructure regulation dating back to the Interstate Commerce Act of 1887,[58] which regulated railroads. Congress subsequently imposed it on the interstate shipping,[59] stockyard,[60] telephone,[61] telegraph,[62] trucking,[63] electricity,[64] natural gas,[65] and aviation[66] industries.[67] This form of economic regulation continued to be common until late in the twentieth century, when it

55. § 164.502(a)(5)(ii)(B)(2)(ii).

56. § 164.502(a)(5)(ii)(B)(2)(iii) - (viii).

57. § 164.508 (a)(4)(i).

58. Interstate Commerce Act, ch. 104, 24 Stat. 379 (1887) (codified as amended in scattered sections of 49 U.S.C. app.).

59. Shipping Act of 1916, ch. 451, 39 Stat. 728, 733–35 (1916) (codified as amended at scattered sections of 46 U.S.C. app.).

60. Packers and Stockyards Act of 1921, ch. 64, 42 Stat. 159 (codified as amended at 7 U.S.C. §§ 181–229b).

61. Communications Act of 1934, ch. 652, 48 Stat. 1064 (codified as amended at 47 U.S.C. §§ 151–614).

62. *Id.*

63. Motor Carrier Act of 1935, ch. 498, 49 Stat. 543 (codified as amended in scattered sections of 49 U.S.C.).

64. Federal Water Power Act of 1935, ch. 687, 49 Stat. 838 (codified as amended at scattered sections of 16 U.S.C.).

65. Natural Gas Act of 1938, ch 556, 52 Stat. 821 (codified as amended at 15 U.S.C. §§ 717-717w).

66. Civil Aeronautics Act of 1938, ch. 601, 52 Stat. 973 (codified as amended and before repeal at scattered sections of 49 U.S.C.).

67. Joseph D. Kearney & Thomas W. Merrill, *The Great Transformation of Regulated Industries Law*, 98 COLUM. L. REV. 1323, 1333-34 (1998).

was partially replaced by market-based reforms[68] that sought, when competitive conditions allowed, to let market forces play a greater role in establishing the price of infrastructure services.[69] Because of the somewhat diminished role[70] cost-of-service pricing now plays in many infrastructure industries, this article draws heavily on a respected older treatise[71] describing its development in U.S. federal regulatory practice before subsequent market-oriented reforms.

HITECH's embrace of regulated, cost-based fees for data provisioning is not easily explained as a response to market imperfections. Historically, many infrastructure industries have exhibited natural monopoly characteristics or other structural problems that made it unwise to let prices be set by market forces.[72] These concerns supplied the rationale for imposing cost-based pricing schemes on many infrastructure industries over the years.[73] However, the market for data provisioning is still immature, and it is too soon to speculate whether or when similar problems may emerge. There appears to be no evidence at this point that market-based pricing would lead to monopolistic abuses of researchers and other data users.

A different rationale seems to be motivating HIPAA's cost-based fee structure. Phillips describes an equity-stability theory of price regulation

---

68. *See* Chen, *supra* note 27, at 1618 (reviewing GÓMEZ-IBÁÑEZ, *supra* note 27).

69. Kearney & Merrill, *supra* note 67, at 1333–40.

70. While cost-of-service pricing plays a less prominent role now than it did before the final quarter of the twentieth century, it continues to be widely used, for example, in federal regulation of segments of interstate infrastructure industries where competitive conditions do not support reliance on market-oriented pricing. It also is heavily used in state and municipal regulation of municipal utility distribution systems since local utility services often are not subject to competition from multiple service providers, making market pricing problematic.

71. CHARLES F. PHILLIPS, JR., THE REGULATION OF PUBLIC UTILITIES: THEORY AND PRACTICE (3d ed. 1993).

72. Kearney & Merrill, *supra* note 67, at 1334. *See also* GÓMEZ-IBÁÑEZ, *supra* note 27, at 4-6 (discussing rationales for infrastructure regulation); PHILLIPS, *supra* note 71, at 51-60 (discussing natural monopoly characteristics and structural issues that may call for price regulation); Hank Intven et al., *Module 1-Overview of Telecommunications Regulation*, in TELECOMMUNICATIONS REGULATION HANDBOOK § 1.1.1 box 1-1 (Hank Intven ed., 2000) *available at* http://www.infodev.org/articles/telecommunications-regulation-handbook-1st-edition (stating that one objective of regulation is to "prevent abuses of market power such as excessive pricing and anticompetitive behaviour" in situations where markets do not exist); *id.* at §§ 5.2.2 – 5.2.4 (discussing specific market imperfections common in infrastructure industries such as telecommunications).

73. PHILLIPS, *supra* note 71, at 182-83; GÓMEZ-IBÁÑEZ, *supra* note 27, at 5-6.

in which Congress regulates prices to keep market forces from undermining valued social goals such as fairness and equity.[74] In the telecommunitelecommunications sector, protecting consumers' privacy rights is seen as a legitimate rationale for regulation[75] (albeit not necessarily for *price* regulation). By placing the cost-based fee in a section of the HITECH Act amending the HIPAA Privacy Rule,[76] Congress appears to have been invoking price regulation as an instrument of privacy policy rather than economic policy. This cap on fees is not to protect researchers from price gouging. Instead, the protected class for this regulation is people whose data are in health databases.

Congress apparently was concerned that market-based pricing might over-stimulate research use of data and thereby expose people whose data are in health databases to excess privacy risks. This posits a functional relationship between the fees researchers pay for data and the informational privacy of the people whose data are used —a "price elasticity of privacy" so to speak. If such a relationship exists at all, it is a murky one. Whether privacy and data security protections are strong or weak does not depend on whether a person's health record is being sold for three dollars or three hundred dollars. It depends on many other matters such as the information practices and data security measures implemented by the supplier and user of the data and how well privacy policies are monitored and enforced.[77]

It is not clear whether a higher fee or a lower fee would better serve to reduce people's privacy risks. Allowing data holders to charge a high fee may create supply-side incentives to develop health information systems that facilitate flows of data to researchers, and it may entice data holders to go to the trouble to make their data available for research. Viewed this way, a higher fee seemingly would stimulate development of a "market for data" with its attendant privacy risks. On the other hand, a higher fee would tend to suppress researchers' demand for data, thus reducing people's exposure to research-related privacy risks. The net effect on privacy is hard to predict.

Congress appears to have assumed that the supply of data is, at present, constrained by infrastructure —that is, research use of health data is being limited by a lack of interoperable information systems to supply the data to researchers. Under this assumption, lower fees might tend to protect privacy by reducing data holders' incentives to install infrastruc-

74. PHILLIPS, *supra* note 71, at 187.

75. Intven et al., *supra* note 72, at § 1.1.1 box 1-1.

76. 42 U.S.C. § 17935(d)(2)(B) (Supp. V 2012).

77. *See, e.g.*, MARKLE FOUND., THE CONNECTING FOR HEALTH COMMON FRAMEWORK: OVERVIEW AND PRINCIPLES (2006), *available at* http://www.markle.org/sites/default/files/Overview_Professionals.pdf (discussing principles and practices that affect privacy protection in a networked health information environment).

ture needed to "debottleneck" the flow of data to researchers. This assumption helps explain an apparent anomaly in the HITECH Act: Congress chose not to limit the fees data holders can charge when supplying data for public health uses,[78] even as it capped the fees for data used in research. At first it seems wrongheaded for data holders to charge higher fees for public health uses of data, which traditionally have been considered to have a greater social value than research.[79] Yet this policy makes sense under an assumption that the data supply, at present, is infrastructure-constrained. Under such conditions, a higher fee would help support investment in needed systems[80] to resolve the constraint, thus promoting wider availability of data for use by public health agencies. By letting them pay more than researchers can pay for data provisioning, Congress was helping ensure adequate flows of data to important public health uses. Later, when America has finished installing its health IT infrastructure, it may make sense to limit the fees for public health uses. The HITECH Act allows the Secretary of HHS to impose such a cap at a later time[81] based on an evaluation of how it may affect availability of data.[82] HHS evaluated whether this cost-based fee structure also should apply to data supplied to public health users,[83] but ultimately chose not to cap the remuneration a data holder can receive for data destined for public health uses.[84]

Concerning research, the question is whether infrastructure constraints really do protect privacy by limiting research uses of data. If so, capping fees would be an effective strategy for protecting privacy insofar as it limits infrastructure installation and chokes flows of data to researchers.[85] Yet many data holders –such as large health insurers that already have sophisticated information systems in place –stand ready to

78. Modifications to the HIPAA Privacy, Security, and Enforcement Rules under the Health Information Technology for Economic and Clinical Health Act, 75 Fed. Reg. 40,868, 40,921 (July 14, 2010) (to be codified at 45 C.F.R. § 164.508(a)(4)(ii)(A)).

79. *See, e.g.*, LAWRENCE O. GOSTIN, PUBLIC HEALTH LAW 47 (2d ed. 2008) (discussing the high value traditionally accorded to public health activities).

80. PHILLIPS, *supra* note 71, at 172 (noting the necessity of adequate earnings to support development and expansion of the industry).

81. 42 U.S.C. § 17935(d)(3)(B) (Supp. V 2012).

82. *Id.*

83. 75 Fed. Reg. at 40,891.

84. Modifications to the HIPAA Privacy, Security, and Enforcement Rules under the Health Information Technology for Economic and Clinical Health Act, 78 Fed. Reg. 5566, 5605-06 (Jan. 25, 2013) (to be codified at 45 C.F.R. pts. 160 & 164).

85. Whether it is a *good* policy to protect privacy at the expense of research is a separate issue not relevant to the immediate discussion.

supply data to researchers using existing infrastructure for which capital outlays already have been made.[86] For these data holders, higher fees will not necessarily stimulate investments in infrastructure. Limiting fees, as Congress has done, may have the opposite effect of stimulating demand for their data and increasing overall research use (and privacy risks). This is not to deny that many data holders are still in the process of installing health IT systems; for these, a fee cap may indeed constrain investments, hinder data delivery to researchers, and decrease privacy risks.

Privacy advocates need to nuance their positions in recognition that the relationship between the fee level and privacy risks is largely unknown and is likely to evolve over time. As an instrument of privacy policy, a fee cap is highly experimental and, frankly, a bit strange.

IV. CONSTITUTIONALLY REQUIRED ELEMENTS OF COST-BASED FEES FOR INFRASTRUCTURE SERVICES

During the rulemaking to amend the HIPAA Privacy Rule, HHS sought public comment on how to define the cost-based fee: which cost items should and should not be included?[87] The agency received exten-

86. *See* Alexis Ogdie et al., *Medical Record Databases*, *in* PHARMACOEPIDEMIOLOGY 217-346 (Brian L. Strom, et al. eds., 4th ed. 2005) (describing various databases already in use in pharmacoepidemiology research); *see also* NAT'L RESEARCH COUNCIL, HEALTH PERFORMANCE MEASUREMENT IN THE PUBLIC SECTOR: PANEL ON PERFORMANCE MEASURES & DATA FOR PUBLIC HEALTH PERFORMANCE PARTNERSHIP GRANTS, NAT'L RESEARCH COUNCIL 95 (Edward B. Perrin et al. eds., 1999), *available at* http://www.nap.edu/openbook.php?isbn=0309064368 (discussing administrative databases and their use in observational research); Peter Ian Pillans, *Clinical Perspectives in Drug Safety and Adverse Drug Reactions*, 1 EXPERT REV. CLINICAL PHARMACOLOGY 695, 697 (2008). (noting the expanded availability and improved quality of these databases); Jed Weissberg, *Use of Large System Databases*, *in* INST. OF MED., THE LEARNING HEALTHCARE SYSTEM: WORKSHOP SUMMARY 46 (LeighAnne Olsen et al. eds., 2007), *available at* http://books.nap.edu/openbook.php?record_id=11903 (describing observational research with a large HMO clinical database); Fred D. Brenneman et al., *Outcomes Research in Surgery*, 23 WORLD J. SURGERY 1220, 1220 (1999) (noting that modern cohort and registry studies use large administrative databases, such as claims databases maintained by health insurers, and large clinical databases).

87. Modifications to the HIPAA Privacy, Security, and Enforcement Rules Under the Health Information Technology for Economic and Clinical Health Act, 75 Fed. Reg. 40,868, 40, 891 (July 14, 2010) (to be codified at 45 C.F.R. Parts 160 &164) (seeking public comment on what should be included in the cost-based fee).

sive comments on this issue.[88] In the preamble to the final rule,[89] HHS stated:

> In response to comments about the types of costs that are permitted in the reasonable cost-based fee to prepare and transmit data, we clarify that this may include both direct and indirect costs, including labor, materials, and supplies for generating, storing, retrieving and transmitting the protected heath information: labor and supplies to ensure the protected health information is disclosed in a permissible manner; as well as related capital and overhead costs. However, fees charged to incur a profit from the disclosure of protected heath information are not allowed.[90]

This section explains why the above interpretation is legally problematic. To summarize, the words "reasonable" and "cost-based" have well-developed meanings in U.S. infrastructure regulation. These meanings have been shaped by over a century of Supreme Court cases examining cost-based pricing structures in various infrastructure industries. The HITECH Act's reasonable cost-based fee, as HHS interprets it, does not satisfy constitutional requirements established in all the other contexts where cost-of-service pricing has been employed. HIPAA's cost-based fee has been set so low that it presents constitutional questions and it may chill incentives to invest in needed informational infrastructures to support postmarketing medical product surveillance and other socially valuable research and public health activities.

Conceptually, a fee for data preparation and transmittal should meet several criteria. For example, it should be high enough to encourage private data holders to invest in information systems to support flows of data to socially beneficial studies. At the same time, it should be low enough to make important observational studies affordable, and the fee

88. *See, e.g.*, Comment from Ctr. for Democracy & Tech. et al., Docket No. 2010-16718, REGULATIONS.GOV (Sept. 13, 2010), *available at* http://www.regulations.gov/contentStreamer?objectId=0900006480dc0881&disposition=attachment&contentType=msw12; Comment from Barbara J. Evans, Docket No. 2010-16718, REGULATIONS.GOV (Sept. 10, 2010), *available at* http://www.regulations.gov/contentStreamer?objectId=0900006480dc073f&disposition=attachment&contentType=msw8; Comment from Kristen Rosati, Nat'l Cancer Inst. et al., Docket No. 2010-16718, REGULATIONS.GOV (Sept. 13, 2010), *available at* http://www.regulations.gov/contentStreamer?objectId=0900006480dc087f&disposition=attachment&contentType=msw12.

89. Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules, 78 Fed. Reg. 5566, 5607 (Jan. 25, 2013) (to be codified at 45 C.F.R. pts. 160 & 164).

90. *Id.*

should be set with regard to the potential privacy impacts (as ambiguous as they are).

HHS has constraints on its discretion to peg the fee to a conceptually "ideal" level, even if all stakeholders could agree what is ideal. In particular, there are constitutional constraints. HHS is obliged to heed constitutional requirements enunciated in other infrastructure regulatory contexts. Health information technology (IT) infrastructure *is* infrastructure and, as such, it falls into this line of precedents.[91] Professor Gómez-Ibáñez defines infrastructure as "networks that distribute products or services over geographical space."[92] Large health data systems and interoperable networks meet this definition; indeed, so does a physician's office fax machine when hooked up to a phone line.

In theory there are various options for setting a cost-based fee, differing according to which costs are covered by the fee. At the lower limit, the fee would cover just the incremental (variable) operating costs of responding to researchers' requests for data. Such costs might include, for example, wages paid to personnel for time spent retrieving, copying, and processing data that meet the researcher's specifications and costs of the data transmittal. Many members of the public, bioethicists, and privacy advocates might wish for HHS to limit the fee to this level since this would eliminate any profit on the unauthorized sale of data, deter investment in interoperable health IT systems, and chill development of a market for nonconsensual research use of data. Even if it were desirable, as a policy matter, to deter private investment in America's health IT infrastructure, there would be real constitutional problems with setting the fee at a level that only lets data holders recover their variable operating costs.

The problem with such a fee is that it is "confiscatory," a venerable concept dating back to 1913 in infrastructure rate litigation.[93] A variable cost-only fee would be analogous to letting a railroad charge its passengers only for diesel fuel and wages paid to the engineer and conductors while the passenger actually was riding the train, but ignoring the capital costs of the train itself and the tracks on which it runs. In an 1890 railroad rate case, the Supreme Court noted that a "reasonable"

91. PHILLIPS, *supra* note 71 (providing a detailed discussion of judicial decisions affecting cost-of-service rates for infrastructure services in several industries).

92. GÓMEZ-IBÁÑEZ, *supra* note 27, at 4.

93. *See* David R. Stras, *Pierce Butler: A Supreme Technician*, 62 VAND. L. REV. 695, 706 (2009) (attributing the term "confiscatory" to Pierce Butler—who later became a Supreme Court justice—in 1913 when he was still a corporate lawyer representing a group of railroads in the well-known Minnesota Rate Cases, 230 U.S. 352 (1913)).

charge involves an "element of reasonableness both as regards the company and as regards the public":[94]

> If the company is deprived of the power of charging reasonable rates for the use of its property . . . it is deprived of the lawful use of its property and thus, in substance and effect, of the property itself, without due process of law and in violation of the Constitution of the United States; and in so far as it is thus deprived, while other persons are permitted to receive reasonable profits upon their invested capital, the company is deprived of the equal protection of the laws.[95]

These basic concerns have guided cost-of-service ratemaking in many different infrastructure industries over many years. Summarizing this history, Phillips notes that the Supreme Court "has made it clear that confiscation of property must be avoided."[96] Moreover, the Court has required a fair rate of return with "fairness" conceived along three general dimensions: "financial integrity, capital attraction, and comparable earnings."[97] That is, cost-based rates must be sufficient to give the regulated company a meaningful prospect of maintaining its financial position and credit rating, attracting new investment as needed to continue providing its infrastructure services, and reaping returns in line with those of other companies whose businesses entail a similar level of overall risk.[98]

A reasonable, cost-based fee for data provisioning can and indeed must include an allowance for recovery of the capital invested to create the underlying health information infrastructure plus a reasonable rate of return on that invested capital. A data holder is in a position to respond to a request for data only because it previously invested to create the information systems from which the data are being drawn. If the data holder were limited to a price that shares the benefits of that capital investment with customers (in this case, the researchers) for free, that could amount to a taking of the data holder's capital. Also, singling out health database operators for earnings restrictions that do not apply to investors in other types of databases (such as retail sales databases) could deny equal protection.

---

94. Chi. Milwaukee & St. Paul Ry. Co v. Minn. ex rel. R.R. & Warehouse Comm'n, 134 U.S. 418, 458 (1890). *See also* Fed. Power Comm'n v. Hope Natural Gas Co., 320 U.S. 591, 603 (1944) (noting that setting just and reasonable rates "involves a balancing of the investor and consumer interests").

95. *Chi. Milwaukee & St. Paul Ry. Co.*, 134 U.S. at 458.

96. PHILLIPS, *supra* note 71, at 381.

97. *Id.*

98. *Id.*

In addition to capital costs, database operators also have fixed operating costs that are not directly traceable to any specific data request but which nevertheless must be incurred to keep their systems ready to respond. An example would be wages for the IT personnel who routinely keep the system operating and secure, even if they are not personally involved in responding to data requests. In many infrastructure industries, operating costs are the largest item that must be recovered in rates,[99] and these costs may include significant fixed-cost components that are not traceable to particular services the system provides.[100] A reasonable cost-based fee for infrastructure services must include an allowance for recovery of fixed costs, but there is an obvious challenge in deciding how much of the shared costs each user should pay:

> [W]here as here several classes of services have a common use of the same property, difficulties of separation are obvious. Allocation of costs is not a matter for the slide-rule. It involves judgment on a myriad of facts. It has no claim to an exact science.[101]

"But, despite the difficulties that confessedly attend the proper solution of such questions,"[102] infrastructure service providers are entitled to recover their fixed costs.[103]

It is one thing to acknowledge that operating costs (variable and fixed), capital costs, and a rate of return on capital must be included in the cost-based fee; it is quite another thing to calculate these figures. Administering a cost-based fee will require HHS to address several key issues: (1) valuation of capital investments to be included in the cost-based fee; (2) uniform accounting standards for all included cost items; (3) the cost allocation formula for apportioning capital and fixed operating costs among various users that receive services from the system; and (4) the fair rate of return on capital used to provide the services. In addition, a cost-based pricing scheme requires appropriate institutional arrangements, including a transparent procedural framework to protect the interests of all affected stakeholders.

1. Capital Valuation. "No other conflict in the history of regulation has received so much attention or been the subject of so much litigation."[104] A computer, for example, might be valued at its original cost, at its replacement cost, or at its current depreciated value, to name just

99. *Id.* at 255.

100. *See, e.g.*, *id.* at 179 ("For many public utilities, nonallocable (common or joint) costs represent a significant percentage of total costs.").

101. Colo. Interstate Gas Co. v. Fed. Power Comm'n, 324 U.S. 581, 589 (1945).

102. Smyth v. Ames, 169 U.S. 466, 527 (1898).

103. PHILLIPS, *supra* note 71, at 176-77.

104. *Id.* at 315 (discussing capital valuation).

some of the alternatives[105] that have been analyzed, disputed, and litigated since 1898.[106] The Supreme Court has shown willingness to let regulators exercise considerable discretion in choosing the best approach for a particular industry,[107] and regulators use a variety of methodologies.[108] Different methodologies may create different incentives for industry development and can influence operational practices (such as the frequency of system upgrades) that may affect reliability, security, or—in this case—privacy. These impacts will require careful analysis before HHS adopts a methodology. The decision will need to recognize that health data holders are diverse, with infrastructure ranging from simple file cabinets to vast interoperable data networks. The valuation method(s) may need to reflect their varied circumstances.

2. Uniform System of Accounts. When cost-of-service ratemaking was in its infancy early in the twentieth century, there were numerous accounting abuses and "enormous profits often accrued to the unscrupulous."[109] As early as 1912 and 1913, the Supreme Court recognized that regulators overseeing cost-based fees need to be able to require companies to disclose information about their costs and follow standard accounting practices for any costs included in the fees.[110] Uniform systems of accounts developed gradually after that, sometimes imposed by regulators and sometimes developed by the regulated industries themselves.[111] After modern federal infrastructure regulators were established under the New Deal, they approved uniform systems of accounts for their industries, sometimes drawing on industry-developed standards already in use. Despite adjustments over the years, these basic systems remain in use today.[112] The principles embodied in these systems

105. *Id.* at 331-55 (discussing alternative valuation methodologies).

106. *Smyth*, 169 U.S. at 546-47 (1898) (discussing factors to consider in assessing the fair value of property, such as "original cost of construction, the amount expended in permanent improvements, the amount and market value of [the infrastructure owner's] bonds and stocks, the present as compared with the original cost of construction . . .").

107. *See, e.g.*, Fed. Power Comm'n v. Hope Natural Gas, 320 U.S. 591, 617-18 (1944) ("Congress has entrusted the administration of the [Natural Gas] Act to the Commission not to the courts. Apart from the requirements of judicial review it is not for us to advise the Commission how to discharge its functions."). The notion here is that courts generally should leave questions of rate methodology to the responsible regulatory agency and intervene only in instances of clear injustice.

108. PHILLIPS, *supra* note 71, at 338-40 (providing examples of methodologies used by various federal and state infrastructure regulators).

109. *Id.* at 215.

110. Kan. City S. Ry. v. United States, 231 U.S. 423, 442-43 (1913); Interstate Commerce Comm'n v. Goodrich Transit Co., 224 U.S. 194, 211 (1912).

111. PHILLIPS, *supra* note 71, at 219.

112. *See id.* at 220.

can inform HHS's efforts to develop a uniform system of accounts for the cost-based data provisioning fee.

Health database operators and service providers would be well advised to work together to propose an industry consensus standard based on their intimate knowledge of their own cost structures. Lessons from the early twentieth century strongly suggest, however, that a knowledgeable regulator needs to oversee the final decision, since industry-developed standards may endorse accounting practices that disfavor other stakeholder groups.[113] Ongoing oversight is essential after standards are in place to ensure they are being followed.

3. Cost Allocation. Cost allocation also presents tough analytical issues.[114] In the context of health information infrastructure, these choices also may be rife with ethical complexities and problems of public trust. Taking an insurance data system as an example, the infrastructure may be providing services to several user groups: (1) health insurance beneficiaries —the people whose data are in the system —for whom it is used to process insurance claims; (2) public health agencies that occasionally request data to further their public health missions; and (3) researchers that receive provisioning of data. How much of the capital and fixed operating costs of the system should each group be expected to cover? That is the question that cost allocation addresses.

At present, the capital and fixed costs of health insurance data systems presumably are being paid entirely by insurance beneficiaries whose insurance rates include pass-through of their insurers' administrative costs. To expect these people to continue bearing all of these costs would be unjust in an environment where the system is providing services to other paying user groups. Under HIPAA's waiver provisions, insured persons already must endure the dignitary injury of having their data used without their permission; must they suffer the additional indignity of having to *subsidize* unconsented uses of their data? This would be a recipe for public outrage.

This example suggests why cost allocation issues traditionally have been a contentious matter in cost-of-service pricing. If researchers do not pay at least some of the capital and fixed operating costs of the systems that supply them with data, this may invite state insurance regulatory agencies to second guess how HHS's cost-based fee should be calculated in their states. Admittedly their power to do so is somewhat limited. The federal Employee Retirement Income Security Act of 1974 (ERISA)[115] preempts state regulation of a large part of the overall health insurance market, the self-insured employer-sponsored health plans.[116]

113. *See id.* at 219.

114. *See infra* notes 117-22 and accompanying text.

115. 29 U.S.C. § 1001 *et seq.* (2012).

116. *See* ERISA, § 514(a), 29 U.S.C. § 1144(a) (2012) (providing for broad general ERISA preemption of state law); *see also* ERISA, § 514(b), 29

Even when ERISA preemption is not an issue, not all states regulate health insurance premiums, and among those that do, regulation often is focused on specific segments of the market such as individual and small group plans.[117] Finally, the vast majority of costs included in health insurance premiums reflect payments made for beneficiaries' health care; insurers' administrative costs are but a small portion of their overall costs,[118] and health information systems are but a portion of administrative costs. Still, insurance regulators in some states have authority to inquire into insurers' cost structures and may take an interest in HHS's formula for allocating information system costs as between insurance beneficiaries and other users of the system.[119] Other federal infrastructure regulators have many years' experience devising allocation formulas that, while never universally loved, at least struck stable compromises.[120] Their approaches offer possible concepts for HHS to consider as it implements HIPAA's cost-based fee.

One of a regulator's key duties, with respect to cost allocation, is to prevent capital and other fixed costs from being disproportionately loaded onto users in the weakest bargaining position —typically, the unorganized mass of ordinary users who have few options to change suppliers.[121] Insured Americans are largely captive with little choice over

---

U.S.C. §§ 1144(b)(2)(A)-(B) (2012) (providing a "savings" clause that exempts certain categories of state laws, including laws regulating insurance, from ERISA preemption, but providing a "deemer" clause that has the effect of causing ERISA preemption to apply in cases involving self-insured ERISA health plans).

117. *See, e.g.*, FAMILIES U.S.A., ISSUE BRIEF: UNDERSTANDING HOW HEALTH INSURANCE PREMIUMS ARE REGULATED 2, 5 (2006), *available at* http://www.familiesusa.org/issues/private-insurance/rate-regulation-1-table-of-contents.html (discussing state insurance regulation and providing figures for the number of states that regulate premiums for individual and small group policies).

118. *Id.* at 1 (noting that a goal of regulators and lawmakers is to ensure that the majority of premium dollars are actually used to pay healthcare claims rather than for administration or profits).

119. U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-11-701, PRIVATE HEALTH INSURANCE: STATE OVERSIGHT OF PREMIUM RATES 10, 12 tbl. 1 (2011) (indicating that 48 of the 50 states reported that they reviewed rate filings in at least some segments of the health insurance market in 2010 and that 32 of these states reported that their review process includes scrutiny of health insurers' administrative costs).

120. *See, e.g.*, PHILLIPS, *supra* note 71, at 455, 459-61 (discussing cost allocation in the electric power industry); *id.* at 490-91, 503-04 (discussing allocation methods in the natural gas production and transmission industries); *id.* at 225-27 (discussing allocation methods in the telephone industry); *id.* at 652-54 (discussing allocation in federal electricity infrastructure projects); *id.* at 842 (discussing allocation methods in the water industry).

121. *Id.* at 179.

the insurance plan their employer or government arranges for them.[122] This fact does not justify making them bear the full brunt of health IT capital and operating costs. Researchers and other users, including public health agencies, must bear their own fair share of these costs when they receive infrastructure services. That share may be very small to the extent a user only makes occasional requests for data. Allocation formulas rely on metrics to assess each user group's share of overall system usage —for example, the number of requests made for information services, the number of records accessed, etc. —and costs are allocated in proportion to each group's past or projected usage.[123] There is no single, best set of metrics to use,[124] and a regulator must use its discretion to develop metrics that are generally reasonable and fair to all user groups.

Costs of providing IRB and privacy board review present an interesting cost allocation problem. Infrastructure shareholders are not expected to absorb the routine costs of ensuring lawful, socially responsible operations; they are allowed to pass these costs to their customers in rates.[125] Thus an energy utility would expect its rates to cover legal and consulting fees incurred to make sure that energy is delivered in a lawful, environmentally sound manner. In the same way, a cost-based fee for data provisioning must include costs incurred for ethical and privacy review of data requests since this is a cost of routine regulatory compliance when the data holder is subject to the Common Rule or HIPAA Privacy Rule. The unresolved question is whether these should be treated as a variable operating cost (billed to the specific researcher whose request is being reviewed) or a fixed operating cost (allocated among all users of the system).

Because IRB review costs are directly traceable to particular data requests, it may seem sensible to treat them as a variable cost of data preparation and transmittal. Yet there is a problem with this approach: what happens if the IRB does not approve the transmittal? When an IRB review is negative, no data provisioning takes place, so there is no "customer" to which variable costs can be billed as part of data provisioning fees. Variable-cost billing of IRB review costs could create financial pressure for IRBs to approve all data requests. To avoid this terrible incentive, the costs of negative IRB reviews might instead be treated as a fixed cost of doing business. They are indeed fixed to the

122. *See* Evans, *Authority of the FDA*, *supra* note 9, at 102-03.

123. *See* FAMILIES U.S.A., *supra* note 117, at 5-6 (providing examples).

124. PHILLIPS, *supra* note 71, at 226 (observing that "any cost allocation method involves elements of arbitrariness").

125. *Id.* at 261 (explaining that routine regulatory compliance costs, such as the cost of preparing reports required by regulators, are allowed in rates, but that the cost of fines for *failing* to comply with applicable laws and regulations generally is not allowed in rates).

extent they are not necessarily proportional to the volume of data provisioning services that a system ultimately provides. The system operator would then be able to allocate these costs into the fees it charges to researchers and other users whose requests ethically were able to be served. Two possible approaches would be:

(1) to treat the costs of all IRB reviews (positive and negative) as fixed operating costs to be allocated among some or all groups of system users, or
(2) to bill the costs of positive IRB reviews on a variable cost basis to the specific researcher whose project was under review, while treating the costs of negative reviews as fixed costs to be allocated among system users.

To which user groups these costs can be allocated is a question that would need to be decided in either case. For example, should fixed IRB review costs be allocated only within the user group of researchers, whose activities create the need for IRB reviews? Alternatively, should a portion of the fixed IRB review costs be allocated to the insurance beneficiaries, whose rights are being protected by IRB reviews (particularly the negative ones)? Any portion of these fixed costs allocated to researchers would be included in data provisioning fees. Any portion allocated to insurance beneficiaries would be a business cost reflected in their insurance rates.

4. Rate of Return. In common usage, selling a thing "at cost" means that the seller reaps no profit on the transaction. One of the hardest ratemaking concepts to grasp is that cost-based fees, in American infrastructure law, include a profit margin —that is, a fair rate of return on capital used in providing the infrastructure services.[126] The infrastructure would not exist unless people had invested capital to build it, and that capital came from somewhere, such as from a loan on which interest must be paid or from shareholders who expect to receive dividends. A rate of return is needed to reimburse these costs of procuring capital. Denying infrastructure investors the opportunity to earn a return on their capital would be constitutionally unacceptable. When cost-based fees are set by a regulator, the regulated pricing formula must allow for a reasonable rate of return.

The Supreme Court first attempted to define a fair rate of return in 1909,[127] and the matter was extensively studied, debated, and litigated throughout the twentieth century.[128] It suffices for present purposes to note several main principles that have emerged. A reasonable rate of

126. *See supra* notes 94-98 and accompanying text.

127. Willcox v. Consol. Natural Gas Co., 212 U.S. 19, 48-49 (1909).

128. *See* PHILLIPS, *supra* note 71, at 375-432 (providing a brief history).

return is not a unique figure but rather a range of values or a "zone of reasonableness"[129] that may vary over time[130] with "circumstances and locality"[131] and in response to the level of business risk.[132] Whether a rate is confiscatory depends on company-specific factors such as the company's capital structure (debt versus equity) and its cost of attracting capital as well as on industry-wide and broader economic conditions, such as the cost of borrowing.[133] The requirement that rates be nonconfiscatory acts as a floor below which rates constitutionally cannot go.[134] However, a reasonable rate of return may be higher than a nonconfiscatory one. "The mere fact that a rate is nonconfiscatory does not indicate that it must be deemed to be just and reasonable."[135]

The amended HIPAA Privacy Rule limits remuneration to a reasonable, cost-based fee when data are disclosed for research under a waiver or as a limited data set.[136] This implies a rather detailed, company-specific inquiry into reasonable rates of return for diverse health data infrastructure providers operating in multiple sectors (insurance, academia, healthcare) and many localities. In other infrastructure sectors that use cost-based rates, determining the allowed rate of return typically involves proceedings in which companies propose a rate of return and offer expert testimony and data to support it; other affected stakeholders are provided an opportunity to present opposing views; the regulator arrives at a reasoned decision that is subject to judicial review.[137]

To be clear, there is no guarantee that infrastructure service providers will earn their reasonable rates of return in actual practice. The

129. *Id.* at 181 (quoting EMERY TROXEL, ECONOMICS OF PUBLIC UTILITIES 224 (1947)).

130. *See, e.g.*, United Rys. & Elec. Co. of Balt. v. West, 280 U.S. 234, 249 (1930) ("[A fair rate of return] cannot be settled by invoking decisions of this court made years ago based upon conditions radically different from those which prevail to-day. The problem is one to be tested primarily by present-day conditions.").

131. *Willcox,* 212 U.S. at 48.

132. *Id.* at 48-49.

133. *See, e.g.*, Bluefield Waterworks & Imp. Co. v. Pub. Serv. Comm'n, 262 U.S. 679, 692-93 (1923) (identifying factors to consider in determining whether a rate is confiscatory). *See also* PHILLIPS, *supra* note 71, at 376-82 (providing a brief history and discussion of standards the court has enunciated).

134. Fed. Power Comm'n v. Texaco, 417 U.S. 380, 391-92 (1974) ("All that is protected against, in a constitutional sense, is that the rates fixed by [a regulator] be higher than a confiscatory level.").

135. Banton v. Belt Line Ry. Corp., 268 U.S. 413, 423 (1925).

136. 45 C.F.R. § 164.502(a)(5)(ii)(B)(2)(ii) (2013).

137. PHILLIPS, *supra* note 71, at 188-201 (providing a brief overview of procedures used by regulatory commissions when setting rates).

Supreme Court repeatedly has made this clear.[138] The Constitution merely requires that cost-based fees be calculated in a way that offers companies a realistic *potential* to earn a reasonable profit. This implies, for example, that the formula for calculating the fee must not incorporate wildly optimistic assumptions that, in practice, could never be met. However, infrastructure operators like any other business are subject to commercial risks. They may fail to realize their projected earnings if, for example, the demand for data provisioning services falls short of reasonable, but erroneous, forecasts.

V. PROBLEMS WITH HIPAA'S COST-BASED FEE STRUCTURE

HIPAA's cost-based fee for data preparation and transmittal includes all of the elements that are constitutionally required with one exception: it does not allow health informational infrastructure investors to earn a reasonable rate of return (profit margin) on their investments.[139] As HHS explained in the preamble to the recent HIPAA amendments, "We believe allowing a profit margin would not be consistent with the language of Section 13405 of the HITECH Act."

HHS did not clarify its basis for this belief. The HITECH Act makes no statement about whether the cost-based fee should or should not include a profit margin. It merely requires that data holders limit themselves to a cost-based fee when supplying data for research under a HIPAA waiver.[140] Moreover, what the statute says would be irrelevant if the Constitution states otherwise. As discussed above, the requirement for cost-based fees to allow investors a prospect of a reasonable profit margin arises under the U.S. Constitution, which would trump a conflicting statute. If HHS interprets the HITECH Act as disallowing a profit margin on health database infrastructure investments, this interpretation seemingly is entitled to no judicial deference. As the Tenth Circuit has stated, "[A]n unconstitutional interpretation is not

138. *See, e.g.*, Fed. Power Comm'n v. Hope Natural Gas Co., 320 U.S. 591, 603 (1944) (quoting Fed. Power Comm'n v. Natural Gas Pipeline Co., 315 U.S. 575, 590 (1942)) ("[R]egulation does not insure that the business shall produce net revenues."); Market St. Ry. Co. v. R.R. Comm'n, 324 U.S. 548, 567 (1945) (citing *Hope Natural Gas Co.*, 320 U.S. at 601) (noting that "regulation does not assure that the regulated business make a profit").

139. Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules, 78 Fed. Reg. 5566, 5607 (Jan. 25, 2013) (to be codified at 45 C.F.R. pts. 160 & 164).

140. 42 U.S.C. § 17935(d)(2)(B) (2012) (allowing sales priced at the cost-based fee under the Privacy Rule's waiver provision, 45 C.F.R. § 164.512(i), which allows disclosure to researchers without individual authorization).

entitled to *Chevron* deference."[141] When an agency's interpretation of a statute raises serious constitutional questions about the statute-as-interpreted, courts will construe the statute in a way that avoids these difficulties.[142] Under the doctrine of constitutional avoidance, courts can be expected to construe the HITECH Act in a way that makes the statute consistent with the Constitution. HHS's view that the HITECH Act does not allow a profit margin seems inconsistent with over 100 years of precedents in other infrastructure industries. The doctrine of constitutional avoidance trumps *Chevron* deference.[143]

It seems unlikely that HHS was deliberately flouting the Constitution. Rather, HHS may simply have preferred to leave it for courts to decide whether HIPAA's cost-based fee must include a profit margin. HHS and OCR have a history of administrative modesty in the face of constitutional questions that arise under the HIPAA Privacy Rule.[144] Rather than attempt to interpret the Constitution themselves, these agencies display a pattern of avoiding constitutional questions and leaving them for courts to resolve.[145] Thus, the agency may simply have felt that the courts have superior institutional competence to decide what, precisely, must be included in HIPAA's cost-based fee. This fee does appear to fall under other infrastructure-industry precedents, which would allow data holders to earn a profit margin on their investments in health data infrastructure. However, the notion of earning profits in connection with sharing people's sensitive health data is fraught with bioethical as well as constitutional concerns. HHS may have felt that courts, rather than the agency, are better positioned to decide this question.

While this question remains unresolved, HIPAA's cost-based fee structure arguably is set too far– below the level necessary to encourage infrastructure investment and data access to support important public health and research uses like postmarketing medical product safety surveillance. The only way to fix this problem seemingly will be to challenge the constitutionality of HIPAA's cost-based fee. This challenge

141. U.S. West, Inc. v. F.C.C., 182 F.3d 1224, 1231 (10th Cir. 1999) (referring to deference to agencies' interpretation of statutes under *Chevron, U.S.A., Inc. v. Natural Res. Def. Council*, 467 U.S. 837, 843-44 (1984)).

142. Edward J. DeBartolo Corp. v. Fla. Gulf Coast Bldg. & Const. Trades Council, 485 U.S. 568, 574-75 (1988) (citing NLRB v. Catholic Bishop of Chi., 440 U.S. 490, 499-501, 504 (1979)).

143. *Id.* at 574.

144. *See, e.g.*, Barbara J. Evans, *Institutional Competence to Balance Privacy and Competing Values: The Forgotten Third Prong of HIPAA Preemption Analysis*, 46 U.C. DAVIS L. REV. 1175, 1216 (2013) (describing how HHS and OCR chose to leave certain questions about the scope of HIPAA preemption for courts to resolve).

145. *Id.*

could be brought either by data holders who are being denied a reasonable rate of return on their investments in health database infrastructure or by data users who are being denied access to needed services because nobody is willing to supply them under HIPAA's too-low fee structure. In light of the precedents discussed above, the prospects for a successful constitutional challenge appear rather good, and such a challenge may provide the long-term solution to data access problems.

In the meantime, HHS has offered an interim solution. In the preamble to the HIPAA Privacy Rule revisions, the agency provided guidance that favors the use of distributed data networks. The agency stated that it does not:

> consider sale of protected health information . . . to encompass payments a covered entity may receive in the form of grants, contracts, or other arrangements to perform programs or activities, such as a research study, because any provision of protected health information to the payer is a byproduct of the service being provided.[146]

This language seems to allow data holders to provide research-related services in the context of a distributed data network without becoming subject to HIPAA's cost-based fee structure. Data holders would be able to enter contracts to provide services that support distributed data network operations and to price those services at negotiated, cost-based rates. Thus, data provided to researchers under HIPAA waivers would be subject to the cost-based fee cap, but market rates apply when data holders respond to researchers' queries within a distributed network architecture.

This solution does not completely solve the data access problem. Virtual access to data through a distributed data network ultimately is not equivalent to actual access under a HIPAA waiver. To achieve fully integrated network operations, it occasionally is necessary to share some patient-identifying information outside the privacy firewalls of the respective data holders that participate in the network.[147] Sharing patient-identifying information outside data holders' privacy firewalls requires either individual authorization or a HIPAA waiver, and this remains true even when the data holder is participating in a distributed data network. At the point when HIPAA waivers are required, the cost-based fee structure once again becomes relevant. To the extent the cost-based fee is set at a confiscatory level, this may chill incentives for data holders to participate.

146. Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules, 78 Fed. Reg. 5566, 5606 (Jan. 25, 2013) (to be codified at 45 C.F.R. pts. 160 & 164).

147. *See* Evans, *Authority of the FDA*, *supra* note 9, at 76-77.

VI. ADMINISTERING HIPAA'S COST-BASED FEE

Apart from the overall level of HIPAA's cost-based fee, there is the question of how this fee will be administered. OCR has been thrust into the role of a traditional infrastructure regulator charged with administering cost-of-service pricing. This role lies outside OCR's traditional regulatory competence, which is to oversee the privacy and security of health information and to ensure that people have equal access, without unlawful discrimination, to services from HHS-funded programs such as Medicare.[148]

OCR is not staffed at a level to carry out this new role. In 2010 when HIPAA's cost-based fee was proposed, OCR had 270 full time equivalent (FTE) employees,[149] over 180 of which were at its ten regional offices,[150] and there were only 28 employees in OCR's Health Information Privacy Division.[151] This reflected a significant expansion over OCR's 2009 staffing level of 227 FTE employees.[152] The HITECH Act provided for some expansion of OCR's staffing, such as appointing one privacy advisor for each regional office and expanding public education programs.[153] Even so, OCR anticipated only a ten-person staffing increase between 2010 to 2011 (moving from 270 to 280 with the Health Information Privacy Division remaining steady at 28 FTE employees).[154]

At these staffing levels, OCR's auditing, enforcement, and oversight of HIPAA Privacy Rule compliance were necessarily light even before passage of the HITECH Act.[155] These staffing levels appear wholly inadequate to administer a cost-based pricing scheme, at least if this is to be done in-house by OCR itself. For comparison, the Federal Energy Regulatory Commission (FERC), which even after market-oriented reforms continues to administer cost-of-service rates in the interstate transmission segments of the electricity, oil, and natural gas industries, has around 1,300 personnel.[156] The Federal Communications Commission

148. U.S. DEP'T OF HEALTH & HUMAN SERVS., FISCAL YEAR 2011 JUSTIFICATION OF ESTIMATES FOR APPROPRIATIONS COMMITTEES 5, *available at* http://www.hhs.gov/ocr/office/about/cj2011.pdf.

149. *Id.* at 29.

150. *Id.* at 2.

151. *Id.* at 29.

152. *Id.*

153. *Id.* at 17-18.

154. *Id.* at 29.

155. Ron Stein, *Medical Privacy Law Nets No Fines*, WASH. POST, June 5, 2006, at A1 (reporting that OCR did not impose a single civil fine and prosecuted only two criminal cases in its first three years of operation).

156. FED. ENERGY REGULATORY COMM'N, U.S. DEP'T OF ENERGY, FY 2006 CONGRESSIONAL PERFORMANCE BUDGET REQUEST 1, *available at*

(FCC), which continues to regulate aspects of telecommunications rates, has about 1,800 personnel.[157] OCR faces the dual challenge of deciding the details of the new pricing scheme and developing (or arranging) institutional capacity to carry it out.

If OCR is not in a position to administer the cost-based fee structure, can this responsibility be delegated to IRBs? The answer is emphatically "no." OCR's proposed regulation correctly framed this very important issue. The regulation does not engage IRBs or privacy boards in determining whether fees are reasonable and cost-based: this determination is not listed among the criteria for IRB approval of a waiver.[158] Because it is not a waiver criterion, this is not a determination that IRBs must make when approving disclosure of data for research under a waiver. The requirement of reasonable, cost-based fees appears elsewhere in the regulation.[159] It is a precondition of selling people's data pursuant to a waiver, but the proposed rule did not envision that IRBs would be responsible for making sure this precondition is met.[160] In the preamble to the final rule, HHS confirmed that IRBs are not responsible for ensuring that the fees received, when data are disclosed for research under a HIPAA waiver, are reasonable and cost-based.[161]

HHS instead stated that covered entities and business associates are responsible for ensuring that any fees they receive meet this condition.[162] Unfortunately, there is no way for them to do so unless the agency supplies clear guidance on permissible capital valuation methods, accounting conventions, cost allocation formulas, and the many other

---

http://www.ferc.gov/about/strat-docs/FY06-budg.pdf (requesting a full year 2006 budget of $220 million and 1295 employees).

157. FED. COMMC'NS COMM'N, 2007 ANNUAL FCC EMPLOYEE SURVEY RESPONSES 2, *available at* http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-280549A1.pdf (reporting 1814 employees as of November 2007).

158. *See* 45 C.F.R. § 164.512(i)(2)(ii) (2013) (listing criteria that an IRB or privacy board must determine have been met, before approving a waiver of individual privacy authorization).

159. § 164.502(a)(5)(ii)(B)(2)(ii).

160. Modifications to the HIPAA Privacy, Security, and Enforcement Rules Under the Health Information Technology for Economic and Clinical Health Act, 75 Fed. Reg. 40,868, 40,922 (July 14, 2010) (to be codified at 45 C.F.R. Parts 160 &164) (amending the waiver provisions at § 164.512(i) of the HIPAA Privacy Rule but not adding a requirement for IRB's to determine that fees are reasonable and cost based when approving a waiver).

161. Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules, 78 Fed. Reg. 5566, 5608-09 (Jan. 25, 2013) (to be codified at 45 C.F.R. pts. 160 & 164).

162. *Id.* at 5609.

aspects of a cost-based fee calculation. HHS has not yet done so and merely stated an intention "to work with the research community to provide guidance and help the research community reach a common understanding of appropriate cost-based limitations on remuneration."[163]

One thing is clear: HHS was entirely correct in concluding that IRBs should not be involved in administering the cost-based fee structure. IRBs and privacy boards have no competence to assess whether fees charged on specific data transactions are reasonable or cost-based. Moreover, it would be deeply problematic from the standpoints of due process and good regulatory practice for them to do so.

Apart from the fact that IRBs typically are staffed by biomedical researchers, physicians, and bioethicists who have no experience with cost-of-service pricing methodologies, IRBs have conflicts of interest that preclude their involvement in decisions of this type. Independence is fundamental to the legitimacy of infrastructure regulatory decisions.[164] Smith defines independence in terms of three elements: (1) "[a]n arm's-length relationship with regulated firms, consumers, and other private interests;" (2) "[a]n arm's-length relationship with political authorities;" and (3) "[t]he attributes of organizational autonomy"—such as adequately trained staff and stable funding to support oversight activities—"to foster the requisite expertise to underpin those arm's-length relationships."[165] IRBs are not independent decision makers in this sense.

The HIPAA privacy rule lets waivers be approved by an IRB or privacy board located either at the institution supplying the data or at the institution requesting the data. When promulgating waiver provisions of the initial HIPAA Privacy Rule in December 2000, HHS expressly rejected suggestions that review by an outside, disinterested review body should be required.[166] IRBs and privacy boards make heavy use of voluntary staffing by insiders (employees) of the institutions whose transactions are being regulated. Having no independent source of

163. *Id.* at 5607.

164. Intven et al., *supra* note 72, at §1.2.2.2.

165. Warrick Smith, *Utility Regulators—The Independence Debate*, VIEWPOINT, Oct. 1997, at 1, *available at* https://openknowledge.worldbank.org/bitstream/handle/10986/11570/multi0page.pdf?sequence=1 (describing infrastructure regulatory arrangements in which a regulatory decision maker is granted substantial discretion to set prices and services standards for the regulated firm).

166. Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. 82,462, 82,695 (Dec. 28, 2000) (to be codified at 45 C.F.R. pts. 160, 164) (rejecting, in the preamble to the final HIPAA Privacy Rule promulgated in 2000, public comments that suggested that outside review should be required; reaffirming the proposed rule's policy of imposing no requirements for the location or sponsorship of the IRB or privacy board that approves a waiver; and reaffirming that the review can occur either at the data-supplying or data-requesting institution).

funding, these bodies usually depend on the regulated institutions to support their activities.[167] To let such bodies determine that fees for data sales are "reasonable" and "cost-based" would be like letting insiders at an electric power company set its rates.

Alternatively, a so-called "independent IRB"[168] can be hired to perform functions such as approving waivers and determining whether fees are cost-based. A better adjective for these review bodies would be "unaffiliated" or "stand-alone;" they are not independent in the regulatory sense of the word.[169] These bodies are commercial businesses that work for a fee; the fees typically are paid by either the institution supplying or requesting the data. This financial relationship with an interested party would disqualify them from deciding rate issues under the most minimal norms of good regulatory practice followed not only in developed but in developing economies around the world.[170]

Regardless whether they are unaffiliated or operating within the regulated institutions, IRBs and privacy boards are not subject even to the most rudimentary norms of due process such as the Administrative Procedure Act's requirements of reasoned, evidence-based decision-making due process rights for affected parties, reviewable records, and

167. *See* OFFICE OF INSPECTOR GENERAL, U.S. DEP'T OF HEALTH & HUMAN SERVS., INSTITUTIONAL REVIEW BOARDS: A TIME FOR REFORM ii, 7-8 (1998), *available at* http://www.oig.hhs.gov/oei/reports/oei-01-97-00193.pdf (discussing problems with independence of IRBs in the context of their traditional role of providing ethical review of research); *see also* Evans, *Congress' New Infrastructural Model*, *supra* note 9, at 623-65; Evans, *Authority of the FDA, supra* note 9, at 103-05 (discussing problems with the lack of independence of these bodies and the lax procedural norms they follow).

168. *See* OFFICE OF INSPECTOR GENERAL, U.S. DEP'T OF HEALTH & HUMAN SERVS., INSTITUTIONAL REVIEW BOARDS: THE EMERGENCE OF INDEPENDENT BOARDS I (1998) [hereinafter OIG, INDEPENDENT IRBS], *available at* http://oig.hhs.gov/oei/reports/oei-01-97-00192.pdf (defining "independent IRBs" as "entities working outside institutions where research is performed").

169. *See* Smith, *supra* note 165.

170. An arm's length relationship between regulatory decision-makers and regulated companies is so basic that its absence gives rise to the presumption that a legitimate regulatory framework is not in place. *See, e.g.*, Robert Bacon, *A Scorecard for Energy Reform in Developing Countries*, VIEWPOINT, April 1999, at 2 box 1, *available at* http://rru.worldbank.org.documents/publicpolicyjournal/175bacon.pdf (surveying 115 developing countries to ascertain whether they had or had not instituted effective regulatory frameworks based on six criteria—such as whether the nations had passed regulatory laws and whether they had completed various restructuring and privatization steps within the regulated industries—and applying a single criterion to judge whether appropriate regulatory decision making bodies were in place: was there a regulator that was separate from the regulated companies and from political authorities).

rights of appeal.[171] Involving these review bodies in cost-based fee determinations is inappropriate.[172] "What is most important in this regard is separation of the regulator from the [infrastructure] operator(s) in the market. Such separation inspires market confidence . . . ."[173]

If OCR, within its current resource constraints, cannot do this job and if IRBs and privacy boards should not do it, this leads inescapably to the conclusion that other institutional arrangements will have to be made. The most straightforward would be to form a special, independent commission charged with overseeing development and administration of the cost-based fee for data preparation and transmission. It is fairly common, when implementing new regulatory frameworks, to have to develop special-purpose oversight bodies from scratch.[174] This carries with it the task of establishing a means of funding the costs of running these bodies.[175] Neither of these problems is novel and both have been resolved successfully many times in recent decades as infrastructure privatizations around the world created a need for new oversight bodies to regulate the newly privatized sectors.

There are various ways a special commission could be organized. One approach would be to establish it within a federal agency such as OCR or HHS – in other words, to provide traditional governmental oversight[176] of the cost-based fee structure. In modern practice, it is accepted that this approach does not always provide optimal oversight because of problems like information asymmetries and agency staffing and resource constraints.[177] The trend in recent years has been toward greater reliance[178] on arrangements in which the agency delegates some or all of the oversight activities to nongovernmental actors.[179]

---

171. *See* 5 U.S.C. §§ 551–559, 701–706 (2012); Carl H. Coleman, *Rationalizing Risk Assessment in Human Subject Research*, 46 ARIZ. L. REV. 1, 13–17 (2004); Evans, *Congress' New Infrastructural Model*, *supra* note 9, at 623-24; Evans, *Authority of the FDA*, *supra* note 9, at 103-05.

172. *See* OIG, INDEPENDENT IRBS, *supra* note 168.

173. Intven et al., *supra* note 72, at §1.2.2.1.

174. Smith, *supra* note 165, at 1.

175. *Id.* at 3 (discussing issues that must be addressed when creating new regulatory bodies). *See also* Intven et al., *supra* note 72, at §1.2.2.2 ("It is essential to provide adequate funding for the regulatory process. Funding is required to hire good caliber professional staff and consultants that can implement regulatory objectives. Without adequate funding, regulation will not usually be effective.").

176. Jody Freeman, *Extending Public Law Norms Through Privatization*, 116 HARV. L. REV. 1285, 1325-26 (2003) [hereinafter Freeman, *Extending Public Law Norms*].

177. David M. Lawrence, *Private Exercise of Governmental Power*, 61 IND. L.J. 647, 670-71 (1986).

178. Jody Freeman, *The Private Role in Public Governance,* 75 N.Y.U. L. REV. 543, 551-56 (2000) [hereinafter, Freeman, *Private Role*] (discussing the

Public-private collaborations (also called public-private partnerships)[180] of this sort can be structured various ways, for example, by contracting with private entities to perform specific oversight tasks or creating a framework for independent private oversight. These possibilities offer a range of intermediate options between the two extremes of self-regulation (by IRBs and Privacy Boards affiliated with or hired by parties to the data transaction) and non-delegation (in which OCR oversees the cost-based fee itself). Under the modern federal private nondelegation doctrine, a wide array of functions can be delegated to private actors.[181] The constitutions of a few states continue to restrict private delegations.[182] Even so, at all levels of government there are

---

pervasive role private actors now play both in delivering governmentally financed public services and in performing functions traditionally regarded as public functions).

179. For discussion of public-private collaborations, *see, e.g.*, DONALD F. KETTL, THE TRANSFORMATION OF GOVERNANCE: PUBLIC ADMINISTRATION FOR TWENTY-FIRST CENTURY AMERICA 118 (2002); Paul R. Verkuil, *Public Law Limitations on Privatization of Government Functions,* 84 N.C. L. REV. 397 (2006); Kenneth Bamberger, *Regulation as Delegation: Private Firms, Decisionmaking, and Accountability in the Administrative State*, 56 DUKE L.J. 377 (2006); Edward Rubin, *The Myth of Accountability and the Anti-Administrative Impulse,* 103 MICH. L. REV. 2073, 2073-76 (2005); Jody Freeman, *Extending Public Law Norms, supra* note 176; Gillian E. Metzger, *Privatization as Delegation*, 103 COLUM. L. REV. 1367 (2003); Martha Minow, *Public and Private Partnerships: Accounting for the New Religion*, 116 HARV. L. REV. 1229 (2003); Jody Freeman, *Private Parties, Public Functions and the New Administrative Law,* 52 ADMIN. L. REV. 813 (2000); Jody Freeman, *The Contracting State,* 28 FLA. ST. U. L. REV. 155 (2000); Jody Freeman, *Collaborative Governance in the Administrative State,* 45 UCLA L. REV. 1 (1997).

180. *See, e.g.*, CATHERINE M. DONNELLY, DELEGATION OF GOVERNMENTAL POWER TO PRIVATE PARTIES: A COMPARATIVE PERSPECTIVE (2007) (reviewing literature about U.S. federal and state approaches to public-private collaborations); KETTL, *supra* note 179, at 118 (discussing the recent transformation in which "American governments at all levels became increasingly interconnected with private corporations and nongovernmental organizations (NGOs) that share the task of delivering public services"); Lester M. Salamon, *The New Governance and the Tools of Public Action*, in THE TOOLS OF GOVERNMENT: A GUIDE TO THE NEW GOVERNANCE 1 (Lester M. Salamon, ed., 2002) (describing alternatives to top-down, command-and-control regulation by a governmental agency).

181. *See* DONNELLY, *supra* note 180, at 57-60, 117-26 (summarizing modern federal non-delegation doctrine and noting the extent to which private delegations of governmental power are allowed in modern practice); Freeman, *Private Role*, *supra* note 178, at 580-81 (noting that the desuetude of the federal non-delegation doctrine is well settled); Lawrence, *supra* note 177, at 648-49, 672 (noting the modern trend for U.S. federal courts to allow private delegations); Salamon, *supra* note 180, at 3; Verkuil, *supra* note 179, at 418, 432.

182. DONNELLY, *supra* note 180, at 127-35.

examples of seemingly public functions, including functions associated with regulatory oversight, delegated to private actors.[183] The old "hierarchial and bureaucratic notion of public action," which posited a sharp, clear line between delegable and nondelegable functions, is "badly out of synch with reality."[184]

If OCR does choose to delegate some or all of the functions associated with oversight of HIPAA's cost-based fee, it will be able harness skills of numerous private-sector entities that have applied cost-based pricing principles in other industries such as energy, transportation, and telecommunications. To the extent these entities have not previously worked in healthcare, academic medicine, or insurance, they would be free of conflicts for purposes of administering OCR's data preparation and transmittal fee. There are many options for involving private bodies in oversight activities. These could involve the use of (genuinely) independent standard-setting organizations, auditors, or decision making bodies to help administer the cost-based fee structure.[185] Ombudspersons, independent interest organizations, or legal representatives could be appointed to represent the interests of affected stakeholder groups such as the research community and people whose data are in health information systems.[186] An independent, private-sector body could be engaged to help develop procedural standards to ensure appropriate transparency and accountability.

The matter of procedural standards is critically important when setting up a new oversight body.[187] Some functions are sensitive or problematic to delegate to private bodies; there are analytical frameworks for assessing which functions these are.[188] For such functions, it is

183. Verkuil, *supra* note 179, at 432.

184. Freeman, *Extending Public Law Norms*, *supra* note 176, at 1288.

185. *See* Lawrence, *supra* note 177, at 686-87 (discussing delegation to a private but neutral party).

186. *See id.*

187. Smith, *supra* note 165, at 2-3.

188. *See* Christopher K. Leman, *Direct Government,* in THE TOOLS OF GOVERNMENT: A GUIDE TO THE NEW GOVERNANCE 48, 61-62 (Lester M. Salamon ed., 2002) (discussing factors for identifying inherently governmental functions that should not be delegated to private actors). *See also* Tex. Boll Weevil Eradication Found. Inc. v. Lewellen, 952 S.W.2d 454, 470, 472 (Tex. 1997) (stating an eight-factor test for assessing whether a private delegation is problematic, in the context of a case decided under State non-delegation doctrine); U.S. GEN. ACCOUNTING OFFICE, GAO/GGD-92-11, GOVERNMENT CONTRACTORS: ARE SERVICE CONTRACTORS PERFORMING INHERENTLY GOVERNMENTAL FUNCTIONS? (1991); OFFICE OF MGMT. & BUDGET, EXEC. OFFICE OF THE PRESIDENT, Circular No. A-76, A-2 (May 29, 2003), *available at* http://www.whitehouse.gov/omb/circulars/a076/a76_rev2003.pdf (enunciating factors similar to those in Leman's discussion); Freeman, *Extending Public Law Norms*, *supra* note 176, at 1291, 1342-51 (identifying

important to establish a framework of controls to ensure the oversight body properly protects the interests of all affected stakeholders. These typically include a set of policies, such as a conflicts policy to make sure that the oversight body is truly independent and procedures mimicking the due process protections that would apply had oversight been provided by a governmental body.[189] Such protections typically include procedural norms to ensure fair and open decision making processes, respect for individual rights, unbiased decision making, and nondiscriminatory treatment of similarly situated persons.[190]

There are various ways to fund the oversight body.[191] In recent decades the problem of funding regulatory oversight has received a great deal of attention both in developed and developing nations.[192] A key challenge has been to reduce or avoid reliance on governmental appropriations without undermining the perception of independence.[193] One popular approach has been to require infrastructure owners to receive a license before they may provide infrastructure services and to levy licensing fees initially and/or periodically thereafter. This distributes the cost of providing regulatory oversight among all service providers, usually in proportion to their share of gross revenues from the infrastructure service in question.[194] Thus, data holders could be required to obtain a license in order to participate in the "market" for provisioning data to researchers and could be charged licensing fees in proportion to the annual volume of such services they provide. A related approach, also widely applied, is user fees in which the suppliers pay for specific

---

factors for assessing whether a given private delegation is problematic in ways that call for special controls to protect the interests of all stakeholders).

189. *See generally* Freeman, *Extending Public Law Norms*, *supra* note 176 (discussing public law norms that should apply to private decision makers who perform functions of a sensitive or public nature).

190. *Id.* at 1288; Freeman, *Private Role*, *supra* note 178, at 544, 549; Minow, *supra* note 179, at 1266-67.

191. Intven et al., *supra* note 72, at § 1.2.2.2.

192. Katja Sander Johannsen et al., Dimensions of Regulatory Independence—A Comparative Study of the Nordic Electricity Regulators 6 (unpublished manuscript), *available at* http://www.elforsk–marketdesign.net/archives/2003/conference/papers/13_pedersen_larsen.pdf (comparing regulatory funding in Nordic countries); Kathleen Riviere-Smith, Funding the Regulator: The Bahamian Framework 4–7 (Oct. 8, 2003) (unpublished manuscript), *available at* http://www.oocur.org/Proceedings/Presentations/RiviereSmith1.pdf (detailing regulatory funding in the Bahamas).

193. *E.g.*, Intven et al., *supra* note 72, at § 1.2.2.2.

194. *Id.*

regulatory oversight services[195] such as having their allowed, cost-based rates approved on a periodic basis. An example of this latter approach is the FDA's reliance on user fees to fund its drug and device approval processes.[196] The disadvantage of both these approaches is that they can create real or perceived problems with the oversight body's independence because the regulatory body in effect is being paid by the industry it regulates.

From the standpoint of protecting independence, there is a better approach that is used to fund the work of some U.S. infrastructure regulatory agencies. This approach levies small fees that are spread broadly among members of the protected class (in this case, people whose data are in health information systems) or consumers (in this case, researchers). The FERC is funded, in part, by a small surcharge equal to a few cents added to the price of every thousand cubic feet of natural gas that moves through an interstate pipeline.[197] Pipelines collect the charge from their customers and remit it to the FERC.[198] In this situation, the oversight body is not beholden to the industry it regulates because it is being paid by those whose interests it is trying to protect.

When OCR sought public comments on how to implement the cost-based data provisioning fee,[199] the question was posed in the context of a HIPAA privacy rulemaking. Parties who read and file comments in HIPAA privacy rulemakings are not the same people who regularly work with cost-of-service rate regulation in other infrastructure industries where it is used. There is a real risk that relevant expertise is not being brought to bear on this important problem. Fortunately, the needed expertise is widely available in other industrial sectors and will not have

195. *See generally* Bruce N. Kuhlik, *Industry Funding of Improvements in FDA's New Drug Approval Process: The Prescription Drug Use Fee Act of 1992*, 47 FOOD & DRUG L.J. 483 (1992) (discussing the FDA's reliance on user fees).

196. *See* David A. Kessler & David V. Vladeck, *A Critical Examination of FDA's Efforts to Preempt Failure-to-Warn Claims*, 96 GEO. L.J. 461, 485–86 (2008).

197. *See* 18 C.F.R. §§ 382.101, 382.202 (2013) (establishing procedures for "calculating and asserting annual charges to reimburse the United States for . . . costs incurred by [the FERC]," specifically the costs of the administration of natural gas regulation, "assessed against each natural gas pipeline company" in accordance with the proportion of regulated gas it transported).

198. *See* 18 C.F.R. § 154.402 ("[A] natural gas pipeline company may adjust its rates, annually, to recover from its customers annual charges assessed by the Commission under part 382 of this chapter.").

199. Modifications to the HIPAA Privacy, Security, and Enforcement Rules Under the Health Information Technology for Economic and Clinical Health Act, 75 Fed. Reg. 40,868, 40, 891 (July 14, 2010) (to be codified at 45 C.F.R. Parts 160 &164) (seeking public comment on what should be included in the cost-based fee).

to be developed from scratch. OCR might consider adopting an interim fee structure while taking steps to harness this expertise to design a more permanent solution including both a fee design and institutional arrangements for administering the fee.

Conclusion

HIPAA's new cost-based fee for data preparation and transmittal recognizes that purely donative models of data access cannot ensure the levels of data access and infrastructure development that are needed to support important research and public health objectives such as postmarketing medical product safety surveillance. HIPAA's cost-based fee structure moves in the direction of harnessing economic incentives to encourage data access. As with any new approach, it may require a period of years to work out all the kinks. One important challenge concerns the overall level of the fee, which presently is so low that it would be considered confiscatory under judicial precedents established in other infrastructure industries. HHS has signaled that it does not wish to decide the permissible rate of return on health database infrastructure investments and, in effect, has referred this matter to the courts. The other looming challenge concerns day-to-day administration of HIPAA's cost-based fee structure. Here, there are various options available to the agency, which has signaled its willingness to work with stakeholders to work out suitable arrangements.