CONGRESS' NEW INFRASTRUCTURAL MODEL OF MEDICAL PRIVACY

*Barbara J. Evans**

* Associate Professor of Law; Co-director, Health Law & Policy Institute; Director, Center on Biotechnology & Law, University of Houston Law Center.

INTRODUCTION

Efforts have been underway for several years in the private sector and in the United States Department of Health and Human Services (HHS) to conceptualize how a Nationwide Health Information Network (NHIN) would work.[1] Until recently, Congress had not authorized large-scale implementation of any concrete pieces of such infrastructure. That changed with passage of the Food and Drug Administration Amendments Act (FDAAA) in September 2007.[2] FDAAA's section 905[3] authorizes the Food and Drug Administration (FDA) to oversee development of a nationwide data network, the Sentinel System,[4] aimed at including data for 25 million patients by July 2010 and 100 million by July 2012.[5] Speculative concerns about health database privacy suddenly are enlivened with a riveting immediacy. This is here, now. One in three Americans is slated to be inducted into this data network within four years.[6]

Section 905 responds to shortcomings in FDA's traditional approach to drug safety, which relied heavily on preapproval clinical trials. Clinical trials, which typically test a drug on several hundred to

1 U.S. Dep't of Health & Human Servs., Nationwide Health Information Network (NHIN): Background, http://www.hhs.gov/healthit/healthnetwork/background/ (last visited Oct. 5, 2008).

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

3 § 905, 121 Stat. at 944–49 (codified at 21 U.S.C.A. § 355 (k)(3)–(4) (West Supp. 2008)).

4 U.S. Food & Drug Admin., U.S. Dep't of Health & Human Servs., FDA's Sentinel Initiative, http://www.fda.gov/oc/initiatives/advance/sentinel/ (last visited Oct. 10, 2008); *see also* U.S. FOOD & DRUG ADMIN., U.S. DEP'T OF HEALTH & HUMAN SERVS., THE SENTINEL INITIATIVE 1 (2008), http://www.fda.gov/oc/initiatives/advance/reports/report0508.pdf (discussing the goals and structure of the Sentinel Initiative).

5 FDAAA § 905(a), 21 U.S.C.A. § 355(k)(3)(B)(ii).

6 For persons with health coverage, odds of being in the system are even greater than one in one in three, since the system's initial 100 million inputs are expected to be drawn from Medicare and insurance claims data. *See* discussion *infra* Part I.

a few thousand people[7] for fewer than twenty-four months, may fail to detect rare risks, risks that emerge only in long-term use, and risks of off-label uses not tested in the original clinical trials.[8] The 2004 scandal involving rofecoxib, which was widely marketed under the brand name Vioxx, was one in a series of instances where serious risks escaped detection in clinical trials.[9] Designed in the mid-twentieth century, FDA's drug safety regulatory framework was failing to harness modern information technology to glean additional drug safety information in the postmarket period after drugs are in wide clinical use.[10] In 2005, the HHS Secretary directed FDA to explore the potential for using information technology to improve drug safety monitoring.[11] In 2006, FDA decided to harness the power of bioinformatics as one of its top six priorities under the agency's Critical Path Initiative.[12]

---

7 *See* Sharona Hoffman, *Continued Concern: Human Subject Protection, The Institutional Review Board, and Continuing Review*, 68 TENN. L. REV. 725, 728 (2001) (finding that an average of 4,237 human subjects are needed before a single new drug reaches the marketplace).

8 *See* U.S. FOOD & DRUG ADMIN., *supra* note 4, at 5; *see also* Barbara J. Evans, *What Will It Take to Reap the Clinical Benefits of Pharmacogenomics?*, 61 FOOD & DRUG L.J. 753, 783–85 (2006) (describing the risks and benefits of off-label uses); Margaret Z. Johns, *Informed Consent: Requiring Doctors to Disclose Off-Label Prescriptions and Conflicts of Interest*, 58 HASTINGS L.J. 967, 969 (2007) (discussing the health risks of off-label prescription use); David C. Radley et al., *Off-label Prescribing Among Office-Based Physicians*, 166 ARCHIVES OF INTERNAL MED. 1021 (2006) (reporting statistics on the prevalence of off-label use); Alastair J.J. Wood et al., *Making Medicines Safer—The Need for an Independent Drug Safety Board*, 339 NEW ENG. J. MED. 1851, 1851 (1998) (discussing several drugs that exhibited rare or late-emerging risks after FDA approval).

9 *See* Barbara J. Evans & David A. Flockhart, *The Unfinished Business of U.S. Drug Safety Regulation*, 61 FOOD & DRUG L.J. 45, 45–48 (2006) (summarizing late-emerging drug safety risks).

10 *See id.* at 47–54 (discussing problems with FDA's postmarket monitoring and reporting systems that emphasize collection of data which would have been relevant during premarket approval, but which are not necessarily relevant to safe clinical use); *see also* U.S. Food & Drug Admin., U.S. Dep't of Health & Human Servs., Sentinel Network Public Meeting 4 (Mar. 7, 2007) [hereinafter FDA, March 7 Proceedings] (statement of Dr. Andrew von Eschenbach), http://www.fda.gov/ohrms/dockets/dockets/07n0016/07n-0016-tr00001.pdf (discussing how developments in technology now afford FDA the opportunity to collect necessary information during the postmarket period).

11 *See* U.S. FOOD & DRUG ADMIN., *supra* note 4, at 11 (explaining that the HHS Secretary directed FDA to expand its current system for monitoring medical product performance by capitalizing on the emerging sciences of information technology and drug safety).

12 *See generally* U.S. Food & Drug Admin., U.S. Dep't of Health & Human Servs., FDA's Critical Path Initiative, http://www.fda.gov/oc/initiatives/criticalpath/ (last visited Oct. 10, 2008) (providing information about the goals and activities of the Critical Path Initiative).

That same year, reports by the Institute of Medicine[13] and Government Accountability Office[14] called on Congress to grant FDA additional authority and resources to modernize its drug safety information systems. Section 905 implements recommendations in those reports.[15]

Sentinel System data will include patients' Medicare, military, and private insurance claims data, health records, pharmaceutical purchase data, and "other data as the Secretary [of HHS] deems necessary."[16] In theory, this last clause would let FDA requisition people's entire medical records or their stored tissue or tumor specimens[17] for testing to see whether patients were genetically predisposed to drug-related injuries that they suffered, although FDA has not indicated it intends to take such steps. The 25-million-person milestone initially will be met with Medicare claims data,[18] and a new regulation already has been issued to enable FDA's access to Medicare data.[19] The agency already has signed a memorandum of understanding with the Veterans' Health Administration for sharing of information.[20] The 100-million-person milestone can be met by obtaining claims data from about ten large private health insurers.[21] Including data for 200 million people, while not one of section 905's stated milestones, is regarded as technically feasible[22] and desirable.[23]

---

13 COMM. ON THE ASSESSMENT OF THE U.S. DRUG SAFETY SYS., INST. OF MED., THE FUTURE OF DRUG SAFETY 167–73 (Alina Baciu et al. eds., 2006).

14 U.S. GOV'T ACCOUNTABILITY OFFICE, DRUG SAFETY: IMPROVEMENT NEEDED IN FDA'S POSTMARKET DECISION-MAKING AND OVERSIGHT PROCESSES 1, 4–6 (2006), *available at* http://www.gao.gov/new.items/d06402.pdf.

15 U.S. Food & Drug Admin., U.S. Dep't of Health & Human Servs., The Sentinel Initiative: Fact Sheet, http://www.fda.gov/oc/initiatives/advance/sentinel/factsheet.html (last visited Nov. 14, 2008).

16 FDAAA § 905(a), 21 U.S.C.A. § 355(k)(3)(C)(i)(III)(aa)–(cc) (West Supp. 2008).

17 By "stored" specimens, I refer to previously collected specimens left over from prior surgical and diagnostic procedures to which the patient consented during the course of medical care. Compulsory collection of new specimens would not be lawful under the clause in question.

18 Press Release, U.S. Dep't of Health & Human Servs., New Efforts to Help Improve Medical Products for Patient Safety and Quality of Medical Care (May 22, 2008), *available at* http://www.hhs.gov/news/press/2008pres/05/20080522a.html.

19 Medicare Program; Medicare Part D Claims Data, 73 Fed. Reg. 30,664, 30,664 (May 28, 2008) (to be codified at 42 C.F.R. pt. 423).

20 U.S. FOOD & DRUG ADMIN., *supra* note 4, at 18.

21 *See* FDA, March 7 Proceedings, *supra* note 10, at 73 (statement of Dr. Richard Platt).

22 *Id.*

Congress intends for these data to be used in postmarket surveillance and advanced analysis of drug safety. Studying insurance claims can reveal, for example, that an individual began purchasing Cox-2 painkillers—the class of drugs that includes Vioxx—in 2003 and suffered a heart attack in 2004. On average, only two in ten such coincidences turn out, after further study, to be a drug safety issue.[24] Thus there will need to be occasional access to patients' whole medical records to pin down causes of specific suggestive coincidences, although there are no current plans for routine canvassing of people's entire medical histories.[25] As yet, FDA has not indicated any plans to obtain data from previously stored specimens, although the value of genetic studies of specimens in drug safety research is recognized.[26]

Congress authorized FDA to engage private-sector companies to help develop and operate the system infrastructure.[27] The agency also is authorized to allow access to Sentinel System data for specified uses, including certain types of studies and research,[28] by academic, private sector, and public entities.[29] Thus, FDA has the power to approve access to sensitive health data by two types of outside entity: infrastructure operators and outside data users. An unanswered question is how patients' privacy will be protected.

If transparency is conducive to public trust, then FDA arguably missed its first opportunity to cultivate public trust in the Sentinel System. The day section 905 became law, HHS issued a press release that tersely described FDA's sweeping new data-gathering powers as "activities related to medical product safety"[30]—a thing to which few Americans could object given our status as the world's most assiduous pill-

23 *Id.* at 72–73 (statement of Dr. Miles Braun) (querying whether a 100-million-person database might fail to be representative of important subgroups of the American population).

24 *Id.* at 57 (statement of Dr. Marc Overhage).

25 *See id.* at 57–59; *see also id.* at 66–68, 71 (statement of Dr. Richard Platt) (discussing the need, in occasional instances, to review full medical records to assess causes of specific adverse incidents).

26 *See id.* at 114–18 (statements of Drs. Michael Caldwell and Jeffrey Shuren).

27 FDAAA § 905(a), 21 U.S.C.A. § 355(k)(3)(C)(iii) (West Supp. 2008).

28 *Id.*, 21 U.S.C.A. § 355 (k)(4)(A)(i)–(iii); *see also* U.S. FOOD & DRUG ADMIN., *supra* note 4, at 16 (showing a research component as part of the system's organizational structure).

29 FDAAA § 905(a), 21 U.S.C.A. § 355(k)(4)(A), (D).

30 Press Release, U.S. Dep't. of Health & Human Servs., New Law Ensures Access to Medical Treatments and Information (Sept. 27, 2007), *available at* http://www.hhs.gov/news/press/2007pres/09/pr20070927e.html.

eaters.[31] The announcement did not elaborate that these activities involve gathering personal health data on 100 million Americans for sharing, at FDA's discretion, with outside academic and commercial entities. As read by committed privacy advocates, this press release was as transparent as stating that FDA intends to bake apple pie, not mentioning that the congressionally approved recipe calls for blood of their first-born child. The Sentinel System is intended to serve important public health objectives. Achieving these objectives entails doing things that may make many members of the public uncomfortable. Squarely recognizing what Congress has approved and openly airing the issues it presents are essential in cultivating public trust and in bringing this system—and its hoped-for benefits—to fruition.

Part I describes the Sentinel System and explores why section 905 of FDAAA amounts to an infrastructure regulatory mandate. Part II notes the inherent conflict between privacy protection and other, competing objectives Congress set out in section 905. Part III examines the breadth of FDA's power to share Sentinel System data with outside parties, assuming FDA were to go to the full limit of what section 905 allows. Decisions allowing access to Sentinel System data are coercive in their effect on persons whose data are included in the network. Part IV notes how little history FDA has had in making decisions with coercive effect on the public; the agency's existing framework of institutional protections is not suited to its new regulatory mission. Part V draws on experience of other infrastructure regulators to explore ways to promote legitimacy and public acceptability of decisions to release Sentinel System data.

31 *See, e.g.*, Press Release, U.S. Dep't of Health & Human Servs., *supra* note 18, at 2 (noting that Americans not on Medicare average thirteen prescriptions per year, while those on Medicare average about twenty-eight per year). Those Medicare beneficiaries who consider themselves in poor health consume about forty-five prescriptions per year. *Id.* (citing U.S. Dep't of Health & Human Servs., Medicare Current Beneficiary Survey (2004), http://www.cms.hhs.gov/MCBS/Downloads/A04%20Ric%201.pdf); *see also* U.S. Dep't of Health & Human Sevs., Medicare Current Beneficiary Survey (MCBS), http://www.cms.hhs.gov/LimitedDataSets/11_MCBS.asp (last viewed Nov. 14, 2008) (describing the Medicare Current Beneficiary Survey). Other Americans use about thirteen prescriptions per year, according to a 2007 study by the Agency for Healthcare Research and Quality. *See* Press Release, Agency for Healthcare Research & Quality, Drug Spending Increases More Than 2.5 Times in 8 Years (May 16, 2007), *available at* http://www.ahrq.gov/news/nn/nn051607.htm.

I. FDAAA SECTION 905 AS AN INFRASTRUCTURE REGULATORY MANDATE

Section 905 profoundly alters the nature of FDA's regulatory mandate. While continuing its traditional product regulatory and consumer protection duties, FDA also will be an infrastructure regulator charged with overseeing construction and operation of the vast data network just described. This thrusts FDA into the ranks of infrastructure regulators like the old Interstate Commerce Commission (ICC), which regulated railroads; the Federal Energy Regulatory Commission (FERC), which regulates interstate transmission of electricity, oil, and natural gas; and the Federal Communications Commission (FCC), which regulates telecommunications. This does not mean that FDA will fulfill all the same tasks, such as regulation of pricing and industry rates of return, traditionally associated with these other regulators. Nonetheless, section 905 is an infrastructure regulatory mandate.

Prof. Gómez-Ibáñez defines infrastructure as "networks that distribute products or services over geographical space."[32] Americans traditionally have referred to their infrastructure industries as public utilities (such as electricity networks, natural gas transmission and distribution networks, and water systems)[33] and common carriers (such as telecommunications networks, railroads, airlines, trucking, and oil pipelines).[34] Infrastructure is a broader term that includes those industries, but others as well. Modern manifestations include the Internet, high-speed data transmission networks, and distributed computing networks.[35] Not all infrastructure industries exhibit natural monopoly characteristics,[36] which traditionally supplied the rationale for regulating pricing and rates of return.[37] Not all infrastructure networks are public utilities in the sense of having a duty to serve all would-be users at fair rates.[38] FDA's Sentinel System will be a limited-purpose network serving a restricted set of users: FDA and certain

32 JOSÉ A. GÓMEZ-IBÁÑEZ, REGULATING INFRASTRUCTURE 4 (2003).

33 *See* Jim Chen, *The Nature of the Public Utility: Infrastructure, the Market, and the Law*, 98 NW. U. L. REV. 1617, 1617–18 (2004) (reviewing GÓMEZ-IBÁÑEZ, *supra* note 32).

34 *See* Richard A. Posner, *Natural Monopoly and Its Regulation*, 21 STAN. L. REV. 548, 548 (1969).

35 Chen, *supra* note 33, at 1620.

36 Joseph D. Kearney & Thomas W. Merrill, *The Great Transformation of Regulated Industries Law*, 98 COLUM. L. REV. 1323, 1334 (1998).

37 CHARLES F. PHILLIPS, JR., THE REGULATION OF PUBLIC UTILITIES 171–73 (3d ed. 1993).

38 Posner, *supra* note 34, at 607.

outside data users that meet criteria that this Article explores.[39] FDA's public protection mandate does not involve defending the public from monopolistic abuses; it involves protecting the privacy of people whose data are in the network.[40] Thus, price regulation is not central to the agency's infrastructure regulatory mission. The agency may encounter pricing issues in its role as a purchaser/user of Sentinel System data, but not as a regulator of prices in sales to the public.

All major infrastructure development efforts start the same way: a new type of resource is seen as having value, and an infrastructure network is needed to develop the resource and supply it to people who want to use it. In the power industry, the key resource is electricity, and the infrastructure is power generation, transmission, and distribution facilities. In FDAAA, Congress did not define the key resource or the necessary infrastructure. Congress simply determined that certain activities have value; these include certain kinds of postmarket drug safety surveillance[41] and advanced analysis of drug safety data.[42] Congress left it for FDA to define the specific data resources and infrastructure it needs to support those activities.

Based on discussion at public meetings FDA held in 2007,[43] the following can be inferred: in the Sentinel System, the key resource is longitudinal population health data (LPHD)—health data aggregated both longitudinally (so that disparate sources of health data for a given individual can be linked together chronologically to track illnesses, treatments, and outcomes)[44] and horizontally across a large population (so these data can be compared with similar data for other individuals).[45] The needed infrastructure includes information systems to link individual patients' health records longitudinally; to allow data to be queried and compared across large groups of people; and to allow access to the data by authorized users, while protecting the

39 *See infra* Part III.

40 *See infra* Part I.B.

41 FDAAA § 905(a), 21 U.S.C.A. § 355(k)(3) (West Supp. 2008).

42 *Id.*, 21 U.S.C.A. § 355(k)(4).

43 FDA, March 7 Proceedings, *supra* note 10; U.S. Food & Drug Admin., U.S. Dep't of Health & Human Servs., Proceedings, Sentinel Network Public Meeting (Mar. 8, 2007) [hereinafter FDA, March 8 Proceedings], http://www.fda.gov/ohrms/dockets/dockets/07n0016/07n-0016-tr00002.pdf.

44 FDA, March 7 Proceedings, *supra* note 10, at 51–56 (statement of Dr. Marc Overhage); *see also* FDA, March 8 Proceedings, *supra* note 43, at 74 (statement of Dr. Clement McDonald) (discussing the importance and difficulty of linking data longitudinally).

45 *See* FDA, March 7 Proceedings, *supra* note 10, at 23 (statement of Dr. Jeffrey Hill).

privacy of persons whose raw health data are involved.[46] Sentinel System data will not necessarily be transported for central storage on computers at FDA.[47] As currently envisioned, FDA may adopt a decentralized architecture that sends queries to locations where data are stored and returns answers to the user.[48]

The need for new infrastructure does not always imply a need for infrastructure regulation. Unregulated private-sector investors often can supply and operate needed infrastructure, without any problems that go beyond what can be managed by general-purpose laws such as the Sherman Act.[49] Thus, the United States installed a vast network of personal computers without ever having to appoint a federal laptop regulator, although policing of antitrust issues was, at times, required.[50] Two common situations where governmental intervention may be needed are: (1) when barriers—for example, economic or legal—are blocking private-sector development of the needed infrastructure, or (2) when unregulated private infrastructure operation poses problems, such as abuse of vulnerable persons, that are not adequately addressed by general law.[51] Possible responses include regulation to address the industry-specific problems[52] or outright public ownership and operation of infrastructure.[53] The United States has

46 *See* U.S. FOOD & DRUG ADMIN., *supra* note 4, at 13–16 (explaining that the goal of the Sentinel System is to create a national, integrated, electronic system for monitoring medical product safety that still protects the privacy of the persons whose medical data are used in the system).

47 *See* FDA, March 7 Proceedings, *supra* note 10, at 12 (statement of Dr. Janet Woodcock) (explaining that the goal of the Sentinel System is not to create a "grand database," but rather to build on existing database efforts and promote connectivity).

48 *See* U.S. Food & Drug Admin., U.S. Dep't of Health & Human Servs., The Sentinel Initiative: Questions and Answers, http://www.fda.gov/oc/initiatives/advance/sentinel/qanda.html (last visited Nov. 14, 2008).

49 *See* Chen, *supra* note 33, at 1629, 1652, 1707.

50 *See, e.g.*, Massachusetts v. Microsoft Corp., 373 F.3d 1199 (D.C. Cir. 2004) (remedy appeal); United States v. Microsoft Corp., 147 F.3d 935 (D.C. Cir. 1998) (contempt proceeding); New York v. Microsoft Corp., 224 F. Supp. 2d 76 (D.D.C. 2002) (non-settling states' remedy); United States v. Microsoft Corp., 231 F. Supp. 2d 144 (D.D.C. 2002) (Justice Department settlement approval); United States v. Microsoft Corp., 87 F. Supp. 2d 30 (D.D.C. 2000) (conclusions of law), *aff'd in part, rev'd in part en banc*, 253 F.3d 34 (D.C. Cir. 2001) (merits appeal); United States v. Microsoft Corp., 84 F. Supp. 2d 9 (D.D.C. 1999) (findings of fact).

51 *See* PHILLIPS, *supra* note 37, at 172–73; *see also* GÓMEZ-IBÁÑEZ, *supra* note 32, at 20–21; Chen, *supra* note 33, at 1624–28 (reviewing Gómez-Ibáñez's discussion of government regulation of infrastructure operation).

52 Chen, *supra* note 33, at 1628.

53 *See id.* at 1629 (citing GÓMEZ-IBÁÑEZ, *supra* note 32, at 13); Daniela Klingebiel & Jeff Ruster, *Why Infrastructure Financing Facilities Often Fall Short of Their Objectives* 7 (World Bank Policy Research Working Paper, No. 2358, 2000).

consistently rejected the latter option. It is the only nation that maintained private ownership of its major, interstate infrastructure networks throughout the twentieth century.[54] It achieved this through pervasive regulation of private infrastructure networks to address their industry-specific problems. Other nations, many of which began the twentieth century with privately owned infrastructure, nationalized it at mid-century[55] and relied on public ownership of infrastructure in varying degrees.[56] However, as the twentieth century ended, governments worldwide were turning back to private infrastructure ownership subject to some form of infrastructure regulation.[57]

Consistent with U.S. tradition, Congress authorized FDA to engage private entities on a temporary or permanent basis to develop and operate the Sentinel System.[58] The apparent rationale for FDA's regulatory involvement is that private-sector developers, without regulatory intervention, would not be able to supply LPHD of the type and on the scale required: for 25 to 100 million people, with capacity to "drill down" into whole health records on occasion. Two barriers—logistical and legal—stand in their way. The logistical problem is the fragmented way health care is financed and provided in the United States. The average Medicare patient sees six different doctors per year,[59] and Americans change jobs frequently, flitting from insurer to insurer.[60] The raw inputs for making LPHD—basic health data generated during patients' routine interactions with healthcare providers and insurers—are widely scattered. The United States currently lacks infrastructure for linking these data longitudinally. The first solid evidence that a drug or device is harmful sometimes comes from other nations with national healthcare systems, greater coordination and

54 GÓMEZ-IBÁÑEZ, *supra* note 32, at 2; *see also* Chen, *supra* note 33, at 1632 (citing STEPHEN BREYER, REGULATION AND ITS REFORM 181–83 (1982)).

55 GÓMEZ-IBÁÑEZ, *supra* note 32, at 2.

56 *See* Chen, *supra* note 33, at 1634.

57 *See* Klingebiel & Ruster, *supra* note 53, at 7.

58 FDAAA § 905(a), 21 U.S.C.A. § 355(k)(3)(C)(iii) (West Supp. 2008).

59 *Promoting Disease Management in Medicare: Hearing Before the Subcomm. on Health, H. Comm. on Ways & Means*, 107th Cong. 22–23 (2002) (statement of Dr. Gerard Anderson, Director, Robert Wood Nat'l Program P'ship for Solutions: Better Lives for People with Chronic Conditions).

60 *See, e.g.*, M. Susan Marquis & Kanika Kapur, *Employment Transitions and Continuity of Health Insurance: Implications for Premium Assistance Programs*, HEALTH AFF., Sept.–Oct. 2003, at 198, 198–99 (noting that employment is not static and that job turnover due to layoffs or other circumstances results in insurance turnover); *see also* FDA, March 8 Proceedings, *supra* note 43, at 53 (statement of Dr. Clement McDonald) (discussing twenty-percent rate of membership turnover in some HMOs).

continuity of care, and thus better longitudinal linkage of individual health records and better aggregation at the population level.[61]

Linking data longitudinally requires at least some identifying information to establish which data pertain to the same person.[62] Herein lies the legal barrier: under the Health Insurance Portability and Accountability Act (HIPAA) of 1996[63] and related regulations (HIPAA Privacy Rule),[64] it is infeasible for a private, commercial database operator to obtain all the individual authorizations (or waivers of authorization) that would be needed to obtain identifiable information for 25 to 100 million people.[65] Moreover, even if private

61 *See* FDA, March 8 Proceedings, *supra* note 43, at 42 (statement of Dr. Robert M. Califf); *id.* at 23–24 (statement of Dr. Miles Braun).

62 *See supra* note 44 and accompanying text.

63 Pub. L. No. 104-191, 110 Stat. 1936 (codified as amended in scattered sections of 18, 26, 29, 42 U.S.C.).

64 45 C.F.R. pts. 160, 164 (2007).

65 Under the HIPAA Privacy Rule, covered entities such as doctors and insurers need an authorization signed by the patient before they can disclose health data containing patient-identifying information to the private operator. Absent an authorization, they can only supply health data to the private operator in coded form (i.e., with a code number substituted for any information that would allow the patient to be identified). 45 C.F.R. § 164.514(b)(2)(i)(R), (c). Moreover, the coded disclosure would be subject to HIPAA's "minimum necessary" standard, which limits the amount of health data that can be released. *See id.* § 164.514(d). Alternatively, the doctor and insurer could release identified health data to the private operator if their respective HIPAA Privacy Boards or Institutional Review Boards granted a waiver of authorization under the Privacy Rule. *See id.* § 164.512(i). However, it seems highly unlikely that release of identified data to a private operator, whose business model rests on commercial sale of data, could qualify under the criteria for granting a waiver, which include, among other things, that risks to patient privacy be minimal. *See id.* Even if the waiver criteria could be met, the process of obtaining waivers would be unworkably cumbersome for a data network of the scale envisioned by FDAAA. Thus, it appears that a private operator only would be able to receive data from HIPAA-covered entities in coded form. This fact makes it impossible for the private operator to link data from disparate sources longitudinally to create LPHD. Let us suppose the private operator receives coded data relating to a particular patient from two different sources—for example, clinical observations from the patient's oncologist and insurance claims data from the patient's insurer. Each data set would have a different code attached to it—one code generated by the doctor and a separate code generated by the insurer. Without additional identifying information, the private operator would be unable to ascertain that both of these coded data sets relate to the same person. Therefore, the private operator cannot perform the required longitudinal linkage between claims data and clinical observations. The HIPAA Privacy Rule presents a legal barrier to private sector development of the needed infrastructure for supplying LPHD for use in postmarket drug surveillance. By passing section 905 of FDAAA, Congress deemed regulatory intervention to be necessary in order to resolve this barrier and let private sector investment in infrastructure be mobilized.

entities could assemble such a database, it would need ongoing regulation to protect the privacy of persons whose data were included.

The Sentinel System exemplifies Professor Gómez-Ibáñez's view of infrastructure regulation as a response to debilitating transaction costs.[66] High transaction costs can block the development of infrastructure systems when property rights are ambiguous or widely dispersed.[67] Ambiguous property rights are not a major problem in most infrastructure industries.[68] However, widely dispersed property rights can be a problem, for example, in industries that require rights of way to construct facilities.[69] Thus, the Natural Gas Act granted a power of eminent domain to ease transaction costs in assembling rights of way for pipeline projects approved by the Federal Power Commission (FPC) and its successor, the Federal Energy Regulatory Commission (FERC).[70] Under federal law and the law of many states, individuals do not have property rights in their own health data or stored tissue specimens (from which genetic and other health data can be derived).[71] There have been various proposals to recognize such

66 *See* Chen, *supra* note 33, at 1624–25 (citing GÓMEZ-IBÁÑEZ, *supra* note 32, at 20).

67 *See generally* R.H. Coase, *The Problem of Social Cost*, 3 J.L. & ECON. 1 (1960) (analyzing how high transaction costs can affect societal and economic development); Michael A. Heller & Rebecca S. Eisenberg, *Can Patents Deter Innovation? The Anticommons in Biomedical Research*, 280 SCIENCE 698 (1998) (discussing how allocation of private intellectual property rights in genomic discoveries can impede biomedical research); Michael A. Heller, *The Tragedy of the Anticommons: Property in the Transition from Marx to Markets*, 111 HARV. L. REV. 621 (1998) (examining how the allocation of private property rights can raise transaction costs and result in underutilization of resources).

68 GÓMEZ-IBÁÑEZ, *supra* note 32, at 22; *see also* Chen, *supra* note 33, at 1627 (citing Professor Gómez-Ibáñez for the proposition that ambiguous property rights are not a major source of transaction costs in infrastructure projects); Letter from Donald F. Santa, Jr., President, Interstate Natural Gas Ass'n of Am., to the Hon. John Cornyn, Senator (Sept. 20, 2005), *available at* http://www.ingaa.org/cms/15/3560/3634/3665.aspx (noting that pipeline operators successfully negotiate land-use agreements with ninety to ninety-five percent of landowners in proposed pipeline pathways but encounter barriers to access to remaining parcels of land).

69 GÓMEZ-IBÁÑEZ, *supra* note 32, at 5.

70 *See* 15 U.S.C. § 717f (2006).

71 *See* Rina Hakimian & David Korn, *Ownership and Use of Tissue Specimens for Research*, 292 JAMA 2500, 2502–03 (2004). *But see* Lori Andrews, *Who Owns Your Body? A Patient's Perspective on* Washington University v. Catalona, 34 J. L. MED. & ETHICS 398, 400 (2006) (noting that some courts have held that human tissue outside the body can be considered property of the individual or next of kin); Letter from Simon P. Cohn, Chairman, Nat'l. Comm. on Vital and Health Stat., to the Hon. Michael O. Leavitt, Secretary, U.S. Dep't of Health & Human Servs. (Feb. 21, 2008), *available at* http://ncvhs.hhs.gov/080220lt.pdf (recognizing the importance of individual control

property rights. With or without them, individuals already have statutory and regulatory privacy rights that require their specific, individual authorizations before data can be released. These widely dispersed rights for individuals to control access to their health data pose transaction costs similar those encountered in infrastructure industries that rely on physical rights of way.

Congress could have addressed this problem by authorizing FDA to fashion a new privacy rule for use in the context of its Sentinel System. Congress did not take that approach. Instead, Congress mandated that the system must comply with the HIPAA Privacy Rule.[72] How, then, does it help for FDA to become involved? The interplay of FDAAA section 905 with the HIPAA Privacy Rule provides several options[73] through which FDA can make identifiable health data available for private infrastructure operators (PIOs) to use in creating LPHD for use in the Sentinel System. The scope of FDA's infrastructure regulatory mandate becomes clear only when section 905 and the HIPAA Privacy Rule are read together.

The Privacy Rule struck a balance of public and private interests,[74] recognizing that patients' desire to control access to their

---

over disclosures of health data, but not calling for an individual property right in such data).

72 FDAAA § 905(a), 21 U.S.C.A. § 355(k)(3)(C)(i)(I) (West Supp. 2008).

73 In addition to HIPAA's public health exception, 45 C.F.R. § 164.512(b)(1)(i) (2007), the Privacy Rule also contains a "health-oversight exception" that potentially is relevant to the Sentinal System. *Id.* § 164.512(d)(1)(iii). This allows release of data, without patient authorization, to an agency for use in verifying that regulated entities are complying with regulations. Many, but not all, of the activities envisioned in section 905 potentially fit within this HIPAA exception. HIPAA's "FDA exception," 45 C.F.R. § 164.512(b)(1)(ii), is something of a red herring for purposes of section 905. It allows disclosure of identified data without patient authorization for use in postmarket surveillance and certain other activities relating to FDA-regulated products. However, it provides for disclosure of data to the "responsible person"—that is, to the manufacturer of a drug that is subject to FDA regulation—rather than to FDA itself. The FDA exception may be relevant, however, in resolving questions about access to Sentinel System data by product manufacturers. The Privacy Rule, 45 C.F.R. § 164.512(i), provides procedures for waiver or alteration of HIPAA's usual authorization requirements; this provides another avenue for obtaining data without a standard HIPAA authorization. Finally, it might be possible to frame some Sentinel System activities—particularly those that gather data to provide feedback and reports for patients and physicians, as being part of "treatment" or "quality improvement," which are outside HIPAA's authorization requirements.

74 *See* Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. 82462, 82691 (to be codified at 45 C.F.R. pts. 160, 164) (discussing HHS' rationale for balancing benefits of research against privacy risks in the HIPAA Privacy Rule); *see also* Lawrence O. Gostin & James G. Hodge, Jr., *Personal Privacy and Common Goods: A Framework for Balancing Under the National Health Information Privacy Rule*, 86

health data occasionally must give way to important public needs, such as reporting suspected instances of child abuse. Section 164.512 of the Privacy Rule grants various exceptions to the Privacy Rule's usual requirement that individuals must authorize release of their identifiable health information. One is the public health exception, which lets a covered entity (such as a doctor or insurer) disclose a patient's identifiable health data *without the patient's authorization* to a governmental public health agency that is authorized by law to collect such data to prevent or control injury or to conduct public health surveillance and investigations.[75] FDAAA endows FDA with public health responsibilities that appear to fit squarely within this HIPAA exception. For example, FDA is responsible for evaluating and mitigating postmarket drug safety risks,[76] for reporting current drug safety information to physicians and patients,[77] and for taking other steps to reduce drug-related injuries. To carry out these new responsibilities, FDA would be able to collect data for the Sentinel System without patient authorization. Moreover—and this is the crucial point—the so-called verification standards in section 164.514(h) of the Privacy Rule let covered entities disclose data to persons acting on behalf of a public official.[78] This means FDA can appoint external agents—who could be PIOs—to receive any data FDA is entitled to receive.[79] FDA simply needs to provide these PIOs with a written statement on governmental letterhead or other evidence (such as a contract for services) to show they are acting on FDA's behalf.

Through this subtle interplay of Section 905 and the HIPAA Privacy Rule, Congress has transmuted FDA into an infrastructure regulator. FDA has the power, by handing a letter to a PIO, to grant it entry into the business of collecting identifiable health data for use in making LPHD for the Sentinel System. By rescinding the letter, FDA can force the PIO to exit that business. By setting the terms under which it will provide such letters, FDA can set rules to govern how that business is conducted. This is infrastructure regulation in its classic Amer-

---

MINN. L. REV. 1439, 1441, 1470–72 (2002) (suggesting rules for balancing public and private interests that apply to the HIPAA Privacy Rule).

75 45 C.F.R. § 164.512(b)(1)(i).

76 FDAAA § 901, 21 U.S.C.A. §§ 355(o), (p), 355-1 (West Supp. 2008).

77 *Id.* § 915, 21 U.S.C.A. § 355(r).

78 45 C.F.R. § 164.514(h)(2)(ii)(C). The verification standards of section 514(h) apply to any disclosure permitted under subpart E of HIPAA, and therefore apply to disclosures made under the public health exception of 45 C.F.R § 164.512(b)(1)(i).

79 Ctrs. for Disease Control & Prevention, U.S. Dep't of Health & Human Servs., *HIPAA Privacy Rule and Public Health*, MORBIDITY & MORTALITY, WKLY. REP., Apr. 11, 2003, at 1,1, *available at* http://www.cdc.gov/mmwr/pdf/other/m2e4111.pdf.

ican form dating to the Interstate Commerce Act of 1887[80] and subsequently imposed by Congress on the interstate shipping,[81] stockyard,[82] telephone,[83] telegraph,[84] trucking,[85] electricity,[86] natural gas,[87] and aviation[88] industries.[89] This form of infrastructure regulation is variously referred to as the "original paradigm,"[90] discretionary regulation,[91] American public utility regulation,[92] and, in international circles, as the North American model.[93] It persisted in U.S. infrastructure regulation until the final quarter of the twentieth century, when it was partially supplanted by targeted market-based reforms,[94] a new paradigm that places greater reliance on competition among infrastructure providers to protect the public from excessive prices, discrimination in provision of services, and reliability

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

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

82 Packers and Stockyards Act of 1921, ch. 64, 42 Stat. 159 (codified as amended at 7 U.S.C. §§ 181–229b (2006)).

83 Communications Act of 1934, ch. 652, 48 Stat. 1064 (codified as amended at 47 U.S.C.A. §§ 151–614 (West 2001 & Supp. 2008)).

84 *Id.*

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

86 Public Utility Act of 1935, ch. 687, 49 Stat. 838 (codified as amended at scattered sections of 16 U.S.C.).

87 Natural Gas Act of 1938, ch. 556, 52 Stat. 821 (codified as amended at 15 U.S.C. §§ 717–717w (2006)).

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

89 *See* Kearney & Merrill, *supra* note 36, at 1333–34.

90 *Id.* at 1325.

91 Warrick Smith, *Utility Regulators—The Independence Debate*, PUB. POL'Y FOR PRIV. SECTOR, Oct. 1997, at 2, *available at* http://www.ictregulationtoolkit.org/en/Document.1454.pdf (explaining that under a discretionary regulatory scheme a regulatory commission or an individual regulator is granted substantial discretion to set prices and services standards for the regulated firm); *see also* GÓMEZ-IBÁÑEZ, *supra* note 32, at 11–13, 27–32 (describing discretionary regulation as one of the available regulatory alternatives); Chen, *supra* note 33, at 1628 (noting that "most American lawyers" would call discretionary regulation "public utility regulation" (internal quotations omitted)).

92 Chen, *supra* note 33, at 1628.

93 Peter L. Smith & Björn Wellenius, *Mitigating Regulatory Risk in Telecommunications*, PUB. POL'Y FOR PRIV. SECTOR, July 1999, at 2, *available at* http://rru.worldbank.org/documents/publicpolicyjournal/189smith.pdf (citing REGULATIONS, INSTITUTIONS, AND COMMITMENT (Brian Levy & Pablo T. Spiller eds., 1996)).

94 *See* Chen, *supra* note 33, at 1618.

problems[95]—that is, from key risks that had been central to utility regulators' public-interest mandates under the old paradigm.

At its simplest minimum, the original paradigm of infrastructure regulation allows private ownership of infrastructure but grants a regulator the legal authority: (1) to control market entry and exit by entities that will operate and/or use the infrastructure, and (2) to set terms governing how the approved entrants will do business, so as to serve a general public interest and/or to protect a specific vulnerable class. This paradigm is often summarized as involving regulatory control over entry, exit, terms of service, and pricing.[96] However, price regulation is not actually an essential feature of this model. What is essential is that the regulator be subject to some form of congressionally defined mandate to protect the public. In utility industries, the public-interest mandate often happened to include a statutory requirement to ensure "just and reasonable" pricing.[97] Price regulation was merely instrumental to fulfilling that mandate.

A better summary of the original paradigm is that it involves regulatory control over entry, exit, and terms of service, subject to a statutory public-interest standard. The public-interest standard can, but need not, include a mandate to protect against economic harms. Infrastructure safety issues (for example, pipeline safety) also can justify restricting entry into an industry and regulating it on an ongoing basis.[98] Phillips notes that privacy risks have become important in modern infrastructure regulation where, for example, electric utilities possess information about consumers' usage patterns that would be of interest to businesses advertising energy-efficient appliances.[99] Telecommunications regulators long have addressed concerns with privacy of customers' telephone and telegraphic communications and, more recently, have faced many other privacy issues, for example, unwanted telemarketing calls and the privacy implications of new services like caller ID.[100]

Section 905's public-interest mandate focuses on drug safety and privacy issues, rather than economic harms. Section 905's mandate

95 *See* Kearney & Merrill, *supra* note 36, at 1333–40.

96 *Id.* at 1325, 1359–64; *see also* Chen, *supra* note 33, at 1618 (noting that the regulation of infrastructure can be viewed as a "larger legal challenge of disciplining monopoly").

97 *See, e.g.*, Federal Power Act § 205, 16 U.S.C. § 824d(a) (2006) (declaring unlawful any rate charged by a public utility "in connection with the transmission or sale of electric energy" that is not "just and reasonable").

98 *See* PHILLIPS, *supra* note 37, at 60.

99 *Id.* at 562–63.

100 *Id.*

has two parts: (1) a public health benefit standard—the Sentinel System must support specific authorized uses of data in drug safety activities that Congress has determined are in the American public's interest—and (2) a patient protection standard to ensure privacy and ethical protection of persons whose healthcare data are in the network. Consistent with traditional U.S. infrastructure regulatory practice, the statute defines these standards in broad, open-textured language leaving detailed interpretation to the agency's discretion.

A. The Section 905 Public Health Benefit Standard

Congress instructed FDA to develop the Sentinel System for specific, enumerated purposes: to identify drug safety risks based on electronic health data;[101] to report data on serious adverse drug experiences;[102] for active surveillance for risks using the Sentinel System data network;[103] and to identify trends, report adverse events, and export data for further analysis.[104] This further analysis includes advanced studies done in collaboration with outside parties.[105] Some of these studies would be methodological in nature, to improve techniques of risk-benefit analysis and make it timelier.[106] Significantly, however, section 905(a) authorizes "routine access to outside expertise to study advanced drug safety questions"[107] and expressly allows this outside expertise to include academic, private, and other public entities.[108]

This "advanced drug safety question" clause grants FDA wide discretion to allow study of Sentinel System data by commercial and academic users. Such studies would need to be related to drug safety. Notably, section 905 adopts an intriguing definition of "adverse drug experience" that includes not just drug-related injuries, but efficacy problems as well.[109] The Federal Food, Drug, and Cosmetic Act's concept of safety[110] implies a relative comparison of benefits and risks,[111] so safety and efficacy always have been interrelated concepts. Section

101 FDAAA § 905(a), 21 U.S.C.A. § 355(k)(3)(C)(i)(I) (West Supp. 2008).
102 *Id.*, 21 U.S.C.A. § 355(k)(3)(C)(i)(II).
103 *Id.*, 21 U.S.C.A. § 355(k)(3)(C)(i)(III).
104 *Id.*, 21 U.S.C.A. § 355(k)(3)(C)(i)(IV)–(VI).
105 *Id.*, 21 U.S.C.A. § 355(k)(4)(A).
106 *Id.*, 21 U.S.C.A. § 355(k)(4)(A)(i), (iii).
107 *Id.*, 21 U.S.C.A. § 355(k)(4)(A)(ii).
108 *Id.*, 21 U.S.C.A. § 355(k)(4)(A).
109 *Id.* § 901(b), 21 U.S.C.A. § 355-1(b)(1); *id.* § 905, 21 U.S.C.A. § 355(k)(3)(C)(i)(II).
110 Federal Food, Drug, and Cosmetic Act (FFDCA) § 505(d), 21 U.S.C. § 355(d) (2006).

905 makes this explicit by treating failure of expected pharmacological action as a drug-related risk. This gives FDA wide latitude in defining the types of advanced drug safety study that warrant access to Sentinel System data by outside users: any question addressing the safety or efficacy of an FDA-approved drug is potentially included. Appropriate uses of Sentinel System data under this clause might include, for example, academic or commercial research to develop a new pharmacogenetic test to let an existing drug be prescribed more precisely so as to improve its safety or efficacy; or research to aid development of a more effective version of an existing drug, to improve its risk-benefit ratio and therefore improve its safety. FDA will be guided by a public process through which its Drug Safety and Risk Management Advisory Committee, or its successor, make recommendations on priority drug safety questions and on whether such questions should be addressed through use of Sentinel System data, post-approval studies, or clinical trials.[112]

B. The Section 905 Patient Protection Standard

Congress gave FDA several brief, specific instructions related to the privacy of people whose data are in the Sentinel System. These instructions are: (1) FDA must not disclose individually identifiable health information when presenting, or responding to inquiries about, drug safety signals (that is, data that suggest a possible drug safety problem) and trends.[113] (2) When FDA shares Sentinel data with outside data users, these users are under a similar obligation:

111 *See* Douglas C. Throckmorton, Acting Deputy Dir., Ctr. for Drug Evaluation & Research, U.S. Food & Drug Admin., Presentation on Efficacy Biomarkers: Efficacy/Risk Assessment (Oct. 6, 2005), http://www.fda.gov/cder/genomics/presentations_20051006/051006_07_Throckmorton.pdf; *see also* CTR. FOR DRUG EVALUATION & RESEARCH, U.S. FOOD & DRUG ADMIN., MANUAL OF POLICIES AND PROCEDURES § 6010.3 (2007) [hereinafter CDER, MANUAL OF POLICIES AND PROCEDURES], *available at* http://www.fda.gov/cder/mapp/6010.3.pdf (discussing risk factors to include, and not to include, when assessing the risk-benefit ratio for a drug); INT'L CONFERENCE ON HARMONISATION OF TECH. REQUIREMENTS FOR REGISTRATION OF PHARM. FOR HUMAN USE, GUIDANCE FOR INDUSTRY: E2E PHARMACOVIGILANCE PLANNING 2 (2005), *available at* http://www.fda.gov/CBER/gdlns/ichpvp.pdf (explaining that FDA's "decision to approve a drug is based on its having a satisfactory balance of benefits and risks within the conditions specified in the product labeling"); INT'L CONFERENCE ON HARMONISATION OF TECH. REQUIREMENTS FOR REGISTRATION OF PHARM. FOR HUMAN USE, GUIDELINES FOR INDUSTRY: STRUCTURE AND CONTENT OF CLINICAL STUDY REPORTS 35 (1996), *available at* http://www.fda.gov/cder/guidance/959fnl.pdf (outlining the unified standard for reporting risk-benefit data from clinical trials to regulatory authorities).

112 FDAAA § 905(a), 21 U.S.C.A. § 355(k)(4)(C) (West Supp. 2008).

113 *Id.*, 21 U.S.C.A. § 355(k)(3)(C)(i)(I), (k)(4)(B).

they must not disclose individually identifiable health information when reporting drug safety signals and trends or when responding to inquiries, but they may make lawful disclosures for other purposes.[114] Significantly, this instruction would let outside data users *receive* identifiable data from the Sentinel System; it merely restricts their ability to *redisclose* the identifiable information when reporting their study results. (3) Outside data users must be placed under contractual obligations to comply with the HIPAA Privacy Rule and the Privacy Act.[115] Note, though, that outside data users still would have an avenue for redisclosing data—including identifiable data—under the HIPAA Privacy Rule's waiver and alteration provisions,[116] unless FDA imposes further requirements that go beyond this minimal Congressional instruction.[117] (4) Outside data users must continue to observe these privacy obligations after their contracts end, at which time they must return or destroy the data.[118] (5) Outside data users that are part of larger organizations must take measures to protect the security and privacy of the data, and they may not share the data with other components of their organizations without authorization.[119] This seems to envision authorization from FDA, rather than from the persons whose data are involved.

Beyond these minimal requirements, Congress gave FDA a general instruction to establish and maintain Sentinel System procedures that comply with the HIPAA Privacy Rule.[120] As already discussed, the Privacy Rule affords little direct, substantive protection of patient privacy. The Privacy Rule's public health exception is a trap door through which the Sentinel System falls. Since Congress has authorized FDA to conduct public health related activities under section 905, FDA can obtain identifiable health data without individual authorizations and can delegate its right to receive such data to outside parties under the Privacy Rule's verification standards.

The core issues of privacy protection in this system will be: (1) To which—and to how many—PIOs will FDA delegate its authority to receive identifiable raw health data under the HIPAA public health exception? (2) How broadly will FDA construe the statutory purposes for which Sentinel System LPHD can be released—potentially in iden-

114 *Id.* § 905(a), 21 U.S.C.A. § 355 (k)(4)(G)(i).

115 Privacy Act of 1974, 5 U.S.C. § 552a (2006). FDAAA section 905(a) requires compliance with 5 U.S.C. §§ 552 and 552a. *See* 21 U.S.C.A. § 355(k)(4)(G)(i)(II).

116 45 C.F.R. § 164.512(i) (2007).

117 *See* discussion *infra* Part III.C.1.

118 FDAAA § 905(a), 21 U.S.C.A. § 355(k)(4)(G)(iii) (West Supp. 2008).

119 *Id.*, 21 U.S.C.A. § 355(k)(4)(G)(ii).

120 *Id.*, 21 U.S.C.A. § 355(k)(3)(C)(i)(I).

tifiable form—to outside data users? (3) What selection and qualification criteria will FDA apply when choosing PIOs and outside data users? (4) Subject to what policies and on what terms will FDA release data? (5) What processes will FDA follow when making these decisions? (6) Will FDA's procedures result in an open, transparent decisional process that affords due process to all interested parties, thus meriting the public's trust? Congress left these questions—and with them, the true scope and force of the Sentinel System's privacy protections—to FDA's discretion.

Concerning ethical issues (for example, human-subject protections), section 905 instructs FDA to convene a committee of experts in data privacy and security to make recommendations to the Secretary of HHS on "tools and methods for the ethical and scientific uses for, and communication of" Sentinel System data.[121] This scope of work could encompass technical issues such as network security and verification standards; policies regarding release of data to outside users in identifiable, coded, and de-identified form;[122] procedures for coding of data and protection of code keys; and appropriate human-subject protections when Sentinel System data are used in research. Thus, ethical issues were delegated for the agency to address in its sole discretion, subject only to advisory committee input but not subject to any congressionally defined standards. This broad delegation is consistent with the approach Congress has taken when addressing ethical and human-subject protection issues in various other contexts, such as development of regulations to protect human subjects of federally funded biomedical research.[123]

II. Competing Regulatory Objectives in Section 905

FDA already is embroiled in classic infrastructure regulatory problems, including the "fundamental problem in the law of regulated industries"—how to get the infrastructure financed and built and how to govern its use over a time frame so long as to preclude accurate projections of demand, political pressure, and further technological innovation.[124] The Sentinel System amounts to pure greenfield infrastructure development—creating a new type of

121 *Id.*, 21 U.S.C.A. § 355(k)(3)(B)(iii).

122 *See infra* Part III.B.2 for definitions of these terms.

123 *See, e.g.*, Public Health Service Act, 42 U.S.C. §§ 289(a), 300v-1(b) (2000) (authorizing creation of an advisory commission to examine issues in protection of human-subject research and authorizing the Secretary of HHS, based on advice from that commission, to develop appropriate regulations to protect human subjects in certain federally funded research programs).

124 Chen, *supra* note 33, at 1617.

infrastructure that never before has existed in the nation where it is being built. FDA is an experienced product safety regulator but has no staffing or experience that qualify it as an infrastructure regulator. FDA's position is similar to that of new regulators in nations that privatized infrastructure[125] or went through their first rounds of major infrastructure installation[126] after 1980; or of U.S. railroad regulators late in the nineteenth century; or of the FPC in the late 1930s and 1940s when improved steel technology first made long-haul interstate pipelines feasible[127] and led Congress to pass the Natural Gas Act: FDA is charged with ensuring completion and governance of a thing that has no precedent and, even as construction is underway, must hone its own regulatory mission and develop the institutional capacity to carry it out.

FDA's challenge is to wield the discretion it has been granted to achieve three objectives: (1) to protect privacy, (2) while letting the Sentinel System be financed and used, (3) so as to achieve public health benefits. FDA may encounter the "'sharp, often highly emotional, sometimes violent economic and political combat'" that has accompanied new infrastructure development in other contexts,[128] because these objectives clash with one another. The clash of privacy and public health benefits is obvious: if FDA construes advanced drug safety studies broadly, this may enhance the system's public health benefits but erode patient privacy as data are widely disseminated for projects of diminishing marginal benefit. Construing the term too narrowly may protect privacy at a cost of leaving important drug safety issues unaddressed. Using patients' data without their authorization is

125 *See* Mary Shirley, *Why Performance Contracts for State-Owned Enterprises Haven't Worked*, PUB. POL'Y FOR PRIVATE SECTOR, Aug. 1998, at 1, 1–4, *available at* http://rru.worldbank.org/documents/publicpolicyjournal/150shirl.pdf (surveying regulatory methods used to privatize 565 state-owned enterprises in thirty-two countries); *see also* Pierre Guislain & Michael Kerf, *Concessions—The Way to Privatize Infrastructure Monopolies*, PUB. POL'Y FOR PRIVATE SECTOR Oct. 1995, at 1 (discussing the use of concession contracts as a regulatory tool in nations undergoing privatization of infrastructure industries); Mary M. Shirley, *Enterprise Contracts: A Route to Reform?*, FIN. & DEV., Sept. 1996, at 6, *available at* http://www.imf.org/external/pubs/ft/fandd/1996/09/pdf/shirley.pdf (discussing privatization and reform of state-owned infrastructure industries).

126 *See* Klingebiel & Ruster, *supra* note 53, at 9 (explaining that government strategies to induce private investment in infrastructure have often fallen short of intended objectives because of a lack of a conducive environment for private participation in infrastructure or faulty design of the strategies themselves); *see also* Smith, *supra* note 91, at 2–3 (discussing issues facing newly formed regulatory agencies).

127 PHILLIPS, *supra* note 37, at 693.

128 *See* Chen, *supra* note 33, at 1619 (quoting JAMES WILLARD HURST, LAW AND MARKETS IN UNITED STATES HISTORY 21 (1982)).

justified—legally and ethically—only if the data actually serve an important public interest. A crucial aspect of privacy protection is to restrict the uses of data to their narrow, intended purposes. Widespread dissemination of data for other uses would increase patients' exposure to privacy risks.

The extent of integration within the data network is a key policy decision and here, too, there is a clash between privacy and public health benefits. The policy question is how far to go in linking data from disparate sources—for example, claims data from different health insurers—to form complete historical records of individuals' health. One alternative, which minimizes privacy problems, is to keep various insurers' data separate. If an individual happens to have data in two insurance databases, those data would not be linked together to form a comprehensive account of the person's medical history. Each insurer's database would be an island in an archipelago that is the Sentinel System. Targeted queries (such as, "How many people in your database had heart attacks after taking Drug Y?") could be sent to all participating insurers. Each island could report its answer to FDA in anonymized form ("Without naming any names, we had 200 such people."). Summing these responses for the entire archipelago yields total statistics without transferring anyone's individually identifiable health information off the island where it already resides. FDA has suggested that it intends to pursue this approach, at least in the early years of Sentinel System development.[129] As described at a May 2008 press conference, the system's query structure would relay questions for insurers to analyze behind their respective privacy firewalls. Insurers' responses—but not their complete data sets of identifiable claims information—would be conveyed to FDA for centralized compilation and analysis.[130]

This island approach protects privacy, but it may miss important safety information. This is particularly true with respect to latent risks (or benefits) that emerge only after a long time period. Short-duration clinical trials are inherently unable to assess long-range effects. For example, two-year clinical trials cannot assess the risk of taking cholesterol-lowering statins for three or more decades—something many Americans will be doing as chronic health problems appear in ever-younger patients. One of Congress' many goals in approving the Sentinel System was to improve detection of latent risks, which are inherently unknowable at the time FDA approves new drugs. If FDA

129 *See* U.S. Food & Drug Admin., *supra* note 48.

130 *See* Neal Learner, *FDA's 'Sentinel Initiative' for Rx Safety Will Rely Heavily on Large Health Plan Databases*, AIS's HEALTH BUS. DAILY, June 16, 2008.

relies too heavily on the island approach for protecting privacy, the system may fail in this objective. Here is why: Americans under the age of sixty-five change health plans frequently. Many people in this age group are covered by employer-sponsored health plans that shop insurers annually to seek the most economical coverage. If a patient takes Drug Y while in one insurance plan, but switches to another plan before suffering a heart attack, targeted queries of the two database islands will not detect the adverse event. Putting two and two together requires integrating data from both data sets; this linkage entails at least some sharing of identifying information about the patient.

Medicare data will be somewhat helpful in studying long-term risks and benefits. Patients who reach Medicare's threshold age remain in the Medicare system from that point forward, supplying continuous data over time. Yet Medicare patients, due to their advanced age, may not live long enough to experience long-term risks and benefits. Also, Medicare data cannot answer questions about products aimed at younger patients such as acne medications and childhood vaccines.[131] If teenagers' acne medicines increase their risk of skin cancer at age forty-five, we are unlikely ever to know it unless individuals' health records can be linked longitudinally. The needed data are scattered across many different private insurance databases. An island approach to privacy makes it hard to answer questions that easily could have been answered at a higher level of data aggregation. The island approach may be appropriate as a transitional step in the early years of Sentinel System operation, as FDA develops infrastructure and privacy policies to support fully integrated data operations in the future. However, significant integration of data ultimately will be necessary, to fulfill Congress' public health objectives. This integration will entail privacy risk.

There also is a clash between privacy and financing: LPHD have value in many different commercial, research, and public health applications. Once LPHD are created for use in the Sentinel System,

131 *See, e.g.*, FDA, March 7 Proceedings, *supra* note 10, at 66–69 (statement of Dr. Richard Platt) (describing recent efforts to resolve safety questions surrounding a meningococcal vaccine approved in 2005). Vaccination against meningitis was recommended for all adolescents and, during its first fifteen months, 5.7 million doses of the new vaccine were distributed. During this period, there were fifteen spontaneous reports of Guillain-Barré syndrome, an inflammatory neurological condition that can be lethal or paralyzing. Existing vaccine-safety databases allowed follow-up analysis of 100,000 vaccine doses—far too few to distinguish whether the observed rate of Guillain-Barré was vaccine-related or simply background occurrence of this rare condition. *See id.* at 66–69. Medicare data would be useless in this context, since the vaccine is used primarily in adolescents.

the temptation will be to sell these data for unrelated, ancillary uses.[132] Such sales could help defray the costs of system development. Four contractors that proposed NHIN architectures to HHS all have indicated that ancillary sales of data would be needed to help finance system development.[133] The question of ancillary data sales also came up during FDA's March 2007 public meetings to discuss the Sentinel System.[134] Public trust will live or die on how this issue is handled, yet so may the system's financial viability. Congress authorized appropriations of up to $25 million per year in each of the years 2008 to 2012 to implement section 905 and a number of other postmarket drug safety programs in Title IX of FDAAA.[135] The Sentinel System alone is likely to cost much more than that, so FDA is directed to engage private partners who will invest private capital in network development.[136] Relying on private infrastructure financing will leave FDA open to commercial pressures. One can envision a scenario where a PIO is supplying LPHD to FDA for use in its Sentinel System; FDA has come to depend on these LPHD to perform important drug safety surveillance activities; one day, the PIO announces it is losing money and will soon go out of business unless FDA authorizes it to sell LPHD to other users. The pressure will be to approve the ancillary sale to ensure continued availability of FDA's own data supply. Can this conflict be resolved without jettisoning privacy?

Ancillary sales of data may, at first, seem unproblematic from privacy and ethical standpoints, so long as FDA requires PIOs to de-identify the LPHD—or code them in a way that makes it highly unlikely that the purchaser ever could re-identify them—before the LPHD are sold.[137] Purchase and use of de-identified or coded LPHD would not constitute "human-subjects research" under the Federal Policy for the Protection of Human Subjects (Common Rule) which is implemented by HHS[138] and seventeen other federal agencies.[139] HHS's Office for Human Research Protection (OHRP) interprets research with de-identified or coded health data as not being human-subjects research

132 *See, e.g.*, FDA, March 8 Proceedings, *supra* note 43, at 151 (statement of Dr. Alexander Ruggieri) ("People that have these data sources, which are very rich, could potentially be tempted to pursue possible proprietary ventures with them.").

133 *Id.* at 144 (statement of Dr. Kelly Cronin).

134 *Id.* at 144–46; *id.* at 158 (statement of Dr. Richard Platt, discussing the general need for resources to ensure prompt system development and the need for clarity about permissible data uses and requirements for approving such uses).

135 FDAAA §§ 905(d), 908(a).

136 *Id.* § 905 (a), 21 U.S.C.A. § 355(k)(3)(c)(iii) (West Supp. 2008).

137 *See infra* Part II.B.2 for definitions of identified, coded, identifiable, anonymized, and de-identified data.

138 45 C.F.R. § 46.101–.124 (2007).

that requires informed consent.[140] Nor would the sale trigger informed consent requirements under FDA's own human-subject protections,[141] which apply to persons who are in clinical trials but would not, unless amended, apply to patients whose data are in the Sentinel System.[142] Finally, the ancillary sale would not disclose individually identifiable health information under HIPAA, if de-identification and coding are done in accordance with HIPAA standards.[143] Thus HIPAA authorization would not be required.

Still, there is a legal and ethical pitfall that might be called the "provenance problem." The Sentinel System LPHD likely will be created using identifiable health data that were released to PIOs under HIPAA's public health exception. Any uses of those data—and, presumably, of the LPHD derived from them—must serve the statutory public health purpose for which they were released. Congress's sole public health concern in passing section 905 was to create LPHD for use in addressing problems with postmarket safety of FDA-approved products.[144] The HIPAA public health exception would be violated if Sentinel System data were sold or disclosed for ultra vires uses, in other words, uses beyond section 905's narrow statutory purpose. In addition to staying within the scope of section 905, data uses also must satisfy conditions imposed by HIPAA's public health exception itself. Ancillary sales of the PIO's "output" (LPHD, even in de-identified form) may violate the terms under which the PIO received the "inputs" (identifiable raw health data) that were used in generating the LPHD.

Section 905 authorizes a fairly broad range of uses of Sentinel System data, but it will not support unlimited ancillary sales of the data even in de-identified or coded form. To address the provenance problem, FDA will need robust controls to ensure all uses of Sentinel System data, including ancillary sales of LPHD, meet the following criteria:

---

139 *See* Barbara J. Evans & Eric M. Meslin, *Encouraging Translational Research Through Harmonization of FDA and Common Rule Informed Consent Requirements for Research with Banked Specimens*, 27 J. LEGAL MED. 119, 120 n.5 (2006).

140 *See* Office for Human Res. Prots., U.S. Dep't of Health & Human Servs., Guidance on Research Involving Coded Private Information or Biological Specimens 6 (2004), http://www.hhs.gov/ohrp/humansubjects/guidance/cdebiol.pdf [hereinafter OHRP 2004 Guidance].

141 21 C.F.R. pts. 50, 56 (2008).

142 See discussion *infra* Part III.C.3.

143 45 C.F.R. § 164.514(c) (2007).

144 *See supra* notes 101–09.

(1) All data uses must serve the public health purposes of section 905 and, in addition, one of the following must be true:

(2) The proposed data use is within the scope of uses permitted under HIPAA's public health exception, or

(3) The proposed data use is not consistent with HIPAA's public health exception, but the HIPAA Privacy Rule otherwise allows FDA to release the data to outside users and such uses comply with other regulations governing the use of individuals' health data (such as regulations that protect human research subjects).

Unduly restrictive control over ancillary data uses—or unclear policies related to such uses—could render Sentinel System infrastructure unfinanceable. On the other hand, overly permissive controls could subject FDA to challenges, not only by patients whose privacy allegedly was violated, but by commercial LPHD suppliers facing unlawful competition from FDA's Sentinel System in the broader market for LPHD. FDA's LPHD data set, when fully developed, will be bigger and richer than competing, commercially available data sets. If Sentinel System data were sold outside the purposes for which Congress intended them, FDA and its PIOs might put other commercial database operators out of business. Even if privacy advocates are unable to mount effective legal challenges to ultra vires sales, competing commercial database developers may have the wherewithal to do so. Striking the right balance requires a clear understanding of the legal boundaries on release of data to outside users. These boundaries correspond to the three criteria just identified.

III. The Scope of Allowed Data Disclosures Under Section 905

This Part explores the range of data uses that is legally permissible, assuming FDA were to go to the full limit of the authority Congress granted in section 905. Whether, to what extent, and how FDA should exercise this authority are separate questions, discussed later in this Article. This Part will give little comfort to persons concerned about the privacy of their data in the Sentinel System. Section 905 and the HIPAA Privacy Rule would allow FDA to release Sentinel System data to outside users for a fairly wide range of public health and research activities without individual privacy authorizations. Technically speaking, it would be lawful for FDA to release Sentinel System data to outside users in identifiable form, although there is no reason to expect that such disclosures will be commonplace. The more likely scenario is ancillary sales of data that are not identifiable to the data user (such as sales of data in anonymized or coded form). FDA's current framework of human-subject protections does not apply to per-

sons whose data will be in the Sentinel System. Even if FDA were to adopt the Common Rule for the Sentinel System, data still could be released to outside users in anonymized and coded form. Further, the Common Rule provides at least two avenues for releasing data in identifiable form without informed consent.

A. Keeping Data Uses Within the Scope of Section 905

Many Americans wish for medical privacy to mean that their data can never be used or disclosed for any purpose without their consent. Indeed, many members of the public think privacy *does* mean that.[145] In reality, the law has never recognized this form of privacy in situations where it collided important public health objectives.[146] It is a truism that networked health infrastructure threatens to make privacy risks more salient, since the chances of inadvertent or malicious disclosure go up, the farther the data go.[147] Yet, simultaneously, this infrastructure exposes, in stark terms, that medical privacy can carry a mortal cost, if privacy is framed as an inviolable individual prerogative to veto disclosures. Last year, FDA heard testimony that real-time surveillance of insurance claims data for 7 million people could have let cardiovascular risks of Cox-2 painkillers be detected thirty-four months after sales began; with data for 100 million people, the problem could have been spotted in two or three months.[148] The autonomy-based moral center of bioethics does not hold, if respect for autonomy compels us to endure thirty-one avoidable months of Cox-2 casualties. This is not the clinical trials context, where an individual can refuse to participate without jeopardizing discovery for society as a whole. It is a public health context, where holdouts bias the data set and reduce its statistical power for all of us.

---

145 *See* Charity Scott, *Is Too Much Privacy Bad for Your Health? An Introduction to the Law, Ethics, and HIPAA Rule on Medical Privacy*, 17 GA. ST. U. L. REV. 481, 491 (2000) (reporting a 1999 survey showing that ninety percent of Americans believe that sharing health insurance records with other companies is an invasion of privacy).

146 *See* Lawrence O. Gostin, PUBLIC HEALTH LAW 20–21 (2000).

147 *See, e.g.*, Mark A. Rothstein, *Health Privacy in the Electronic Age*, 28 J. LEGAL MED. 487, 489 (2007) (discussing surveys indicating public concern with loss of privacy with widespread adoption of electronic health records); Nicolas P. Terry & Leslie P. Francis, *Ensuring the Privacy and Confidentiality of Electronic Health Records*, 2007 U. ILL. L. REV. 681, 700 (pointing out that systems with less interoperability pose fewer confidentiality and security concerns, but cannot generate the potential health benefits of an interoperable system).

148 FDA, March 7 Proceedings, *supra* note 10, at 70 (statement of Dr. Richard Platt).

The nub of the problem, always, lies in deciding which public health objectives are sufficiently important to override the individual's interest in nondisclosure.[149] Congress has determined that the specific data uses authorized in section 905 meet this measure of importance and are in the American public's interest. Congress delegated to FDA the difficult task of deciding, on a day-to-day basis as concrete study protocols come before it, which ones serve the purposes Congress authorized. As is common in U.S. administrative law, FDA has been given an open-textured, vaguely worded mandate: the agency is to make data available for study of "advanced drug safety questions." In like fashion, section 7(c) of the Natural Gas Act[150] left it for regulators to decide whether a proposed natural gas pipeline meets a vague statutory public-interest standard: the facility must serve "the public convenience and necessity."[151] The FERC (and its predecessor, the FPC) interpreted this standard to mean that proposed pipelines must meet specific criteria, such as being technologically sound, complying with environmental laws, having adequate financial backing, having reasonable costs so that rates will not be out of line with alternatives, etc.[152] Companies wishing to construct a pipeline under section 7(c) must prove to the FERC that their project meets the criteria, in order to receive a Certificate of Public Convenience and Necessity (CPN). Without a CPN, construction of a new facility is unlawful.[153]

In the same way, Congress left it for FDA to decide whether a proposed use of Sentinel data serves the public health purposes of section 905. If FDA decides that it does, then FDA lawfully can grant access to Sentinel System data. One possibility is for FDA to review all proposed uses of Sentinel System LPHD and approve those it deems to be within the scope of section 905. FDA might adopt the procedural device of granting "Certificates of Public Health Benefit" (CPHBs) to approved data uses. PIOs that operate the Sentinel System could release data to a user lawfully only if the user is holding an FDA-approved CPHB. Alternatively, FDA could enunciate criteria defining broad classes of data use that FDA deems to be within the scope of section 905, and let PIOs apply those criteria when granting access to Sentinel System data. This would be similar to the "blanket certifi-

149 *See* Peter D. Jacobson, *Medical Records and HIPAA: Is It Too Late to Protect Privacy?*, 86 MINN. L. REV. 1497, 1498 (2002).

150 15 U.S.C. § 717f(c) (2006).

151 *Id.* § 717f(c)(1)(A).

152 PHILLIPS, *supra* note 37 at 563–65; *see also* John Decker, Note, *Authorization of Natural Gas Pipeline Construction: Moving Decisions from Regulators to the Marketplace*, 12 VA. ENVTL. L.J. 505, 512 (1993).

153 *See* 15 U.S.C. § 717f(c).

cate" approach the FERC adopted in 1982.[154] It allows pipelines to build certain types of new facilities without applying directly to the FERC for project-specific CPNs, provided that they follow certain rules and agree to certain conditions.[155] Under either approach, FDA would define the criteria for approving outside data uses. The difference is whether FDA applies those criteria itself in a centralized review process or allows the criteria to be applied in decentralized decisions by PIOs.

PIOs naturally will want to be able to make as many ancillary sales of de-identified or coded Sentinel System LPHD as possible; however, FDA has a duty to ensure that all data uses are consistent with section 905. Section 905 does not rule out the possibility of ancillary sales. The concept of "advanced drug safety question" in section 905[156] is broad enough to encompass a wide range of studies of drug safety and efficacy. There may be many outside studies in which FDA does not wish to collaborate directly, in the sense of devoting its own personnel and financial resources to the study, which nevertheless fit within this scope. Ancillary sales to persons conducting such studies would be legally permissible. Section 905 allows access to Sentinel System data for "collaborations" between FDA and private and academic entities, but does not specify the precise form of collaboration.[157] Collaboration could include some projects where FDA helps fund a project or involves its own personnel in working closely with outside data users. However, it also might include uses by private or academic entities that are entirely responsible for funding and staffing the research and merely agree to report their findings to FDA at the end of the project. The precise terms of collaboration could be specified in the project-specific CPHB, or in the conditions FDA sets when granting a PIO a blanket certificate to make ancillary sales for classes of use FDA deems to be in the scope of section 905.

One of the important lessons from infrastructure financing is this: getting new infrastructure financed and built does not require regulators to let PIOs do anything they want to do. It merely requires a clear set of rules so that they can factor what they can and cannot do into their financial planning.[158] Financing major infrastructure does

154 Federal Energy Regulatory Commission (FERC) Order No. 234, 47 Fed. Reg. 24,254, 24,266–24,274 (June 4, 1982) (codified as amended at 18 C.F.R. pts 157, 284, 375 (2008)); *see* Decker, *supra* note 152, at 515–16.

155 Decker, *supra* note 152, at 515–16.

156 FDAAA § 905(a), 21 U.S.C.A. § 355(k)(4)(A)(ii) (West Supp. 2008).

157 *See id.*, 21 U.S.C.A. § 355(k)(4).

158 *See* WORLD BANK, GLOBAL DEVELOPMENT FINANCE 2004, at 161–62 (2004), (discussing how policies, institutions, and regulation can impede movement of capital to

not require regulatory permissiveness so much as it requires regulatory predictability. A key issue in protecting privacy and in getting the system financed is this: can FDA enunciate a clear set of criteria defining, in advance, which uses of Sentinel System data are going to be permissible under section 905? In particular, can FDA provide clear guidance on how the agency intends to interpret the phrase "advanced drug safety questions" in FDAAA's section 905? Even if FDA intends to review all proposed data uses itself, rather than giving PIOs blanket authority to make sales subject to FDA-specified criteria, the infrastructure developers still will need to know what the ground rules for approval are going to be. Otherwise, they will not be able to estimate future revenues and the system may not be privately financeable. Members of the public also have a stake in these ground rules: the boundaries of permissible use are the boundaries of their medical privacy.

B. Keeping Data Uses Within the Scope of Public Health Activities

If FDA relies on HIPAA's public health exception to obtain Sentinel System inputs, the criteria for approving external data uses must address two issues: does the use fit within the scope of section 905 as just discussed, and does it also meet additional conditions of the public health exception? The latter question is whether proposed uses of Sentinel System data constitute public health practice or research. There are important ethical and legal distinctions between the two concepts.[159] While ethical norms support using people's health data

developing-country infrastructure), *available at* http://siteresources.worldbank.org/GDFINT2004/Home/20177154/GDF_2004%20pdf.pdf; Phil Burns & Antonio Estache, *Infrastructure Concessions, Information Flows, and Regulatory Risk*, PUB. POL'Y FOR PRIVATE SECTOR, Dec. 1999, at 1, 2, *available at* http://rru.worldbank.org/Documents/PublicPolicyJournal/203burns.pdf (discussing the importance of being able to forecast, ex ante, "asset values, capital expenditure, depreciation, and operating expenditure profiles, along with the cost of capital, in an attempt to deliver ex ante a fair distribution of returns between shareholders and customers").

159 *See* JAMES G. HODGE, JR. & LAWRENCE O. GOSTIN, COUNCIL OF STATE & TERRITORIAL EPIDEMIOLOGISTS, PUBLIC HEALTH PRACTICE VS. RESEARCH 7 (2004), *available at* http://www.cste.org/pdffiles/newpdffiles/CSTEPHResRptHodgeFinal.5.24.04.pdf; NAT'L INST. OF HEALTH, U.S. DEP'T OF HEALTH & HUMAN SERVS., PROTECTING PERSONAL HEALTH INFORMATION IN RESEARCH (2004), *available at* http://privacyruleandresearch.nih.gov/pdf/HIPAA_Booklet_4-14-2003.pdf; Paul J. Amoroso & John P. Middaugh, *Research vs. Public Health Practice: When Does a Study Require IRB Review?*, 36 PREVENTIVE MED. 250, 250–53 (2003); Ctrs. for Disease Control & Prevention, *supra* note 79, at 6–11; James G. Hodge, *An Enhanced Approach to Distinguishing Public Health Practice and Human Subjects Research*, 33 J.L. MED. & ETHICS 125, 127 (2005); Dixie E. Snider, Jr. & Donna F. Stroup, *Defining Research When it Comes to Public Health*, 112 PUB.

in public health practice without their informed consent or privacy authorization, it is far more problematic to bypass individual control over disclosure of data for research. This distinction is reflected in the HIPAA Privacy Rule and in familiar human-subject protection standards such as the Common Rule.

Both the Privacy Rule and the Common Rule conceive research as a systematic investigation aimed at producing generalizable knowledge.[160] Section 905's advanced drug safety studies are likely to involve at least some activities that are in the nature of research. Any intent to conduct research, whether primary or secondary to a public health purpose, tends to support a finding that the activity is research; however, it does not inevitably do so. The Sentinel System LPHD likely will be created using identifiable health data that were released to PIOs under HIPAA's public health exception. This provenance raises a question whether any research use of these LPHD—by FDA, by its collaborators, or by ancillary users—is permissible. Hodge and Gostin point out the need to "unbundle" the various components of a multifaceted public health program for separate ethical assessment.[161] The fact that FDA's research into advanced drug safety questions is part of a broader public health program does not, by itself, make it public health practice.

1. Criteria for Distinguishing Public Health Uses from Research

HIPAA's public health exception is worded in a way that allows various uses, including public health surveillance and public health "investigations."[162] This latter term arguably is broad enough to encompass advanced drug safety studies that produce generalizable knowledge. However, the breadth of this language appears to have never been interpreted by courts, so its scope is legally uncertain. To avoid legal challenges, FDA would need to restrict outside data uses (including ancillary sales) to studies that qualify as public health practice. This still would permit a wide range of data uses, including some activities that produce generalizable knowledge.

HEALTH REP. 29 (1997); Ctrs. for Disease Control & Prevention, U.S. Dep't of Health & Human Servs., Guidelines for Defining Public Health Research and Non-Research (1999), http://www.cdc.gov/od/science/regs/hrpp/researchdefinition.htm; Office for Prot. from Research Risks, Office for Human Research Prots., OPRR Guidance on 45 C.F.R. § 46.101(b)(5): Exemption for Research and Demonstration Projects on Public Benefit and Service Programs, http://www.hhs.gov/ohrp/humansubjects/guidance/exmpt-pb.htm (last visited Nov. 14, 2008) [hereinafter OPRR Guidance].

160 45 C.F.R. § 46.102(d) (2007); *id.* § 164.501.

161 *See* HODGE & GOSTIN, *supra* note 159, at 50.

162 45 C.F.R. § 164.512(b)(1)(i) (2007).

Hodge and Gostin have restated the question of generalizability as whether the activity in question produces findings that are generalizable beyond the community whose data are involved (research) or merely produces findings that are of benefit within that community (public health practice).[163] Nationally scaled data networks like the Sentinel System offer interesting possibilities for interpreting this distinction. At the conceptual limit, where one-hundred percent of the present and future drug consuming "community" is in the data set, benefits of studying the data are completely internal to that community, and all data uses seemingly would be public health practice, requiring no privacy authorization. If the data set were smaller, these same studies would be research, producing results generalizable beyond the study population; thus individual authorization would be required. The larger a network data set grows, the less it requires acquiescence of the people in it, when research is defined in terms of generalizability. Large health databases achieve an ethically ironic economy of scale: at the limit of their massiveness, when they swallow up the private health data of everybody, they achieve their utmost ethical purity. Research uses of Sentinel System data that involve large data sets may produce findings that redound principally to the benefit of the population involved. If so, this tends to support a finding that the activity is public health practice, not requiring a privacy authorization for the research.

However, no single criterion definitively distinguishes public health practice from research. Various criteria have been proposed in literature and in regulatory guidances.[164] Hodge and Gostin, surveying these sources, suggest an enhanced decisional framework that deemphasizes traditional distinctions, such as whether the activity is carried out by a private-sector or governmental entity, whether the results will be published, whether the activity is a response to an urgent public health crisis, and whether the source of funding is public or private.[165] Given the prevalence of public/private partnerships for conducting traditional governmental functions,[166] these old distinc-

163 HODGE & GOSTIN, *supra* note 159, at 51.

164 *See supra* note 159.

165 HODGE & GOSTIN, *supra* note 159, at 48–50.

166 *See, e.g.*, Jody Freeman, *Collaborative Governance in the Administrative State*, 45 UCLA L. REV. 1, 1 (1997); Jody Freeman, *The Contracting State*, 28 FLA. ST. U. L. REV. 155, 164–76 (2000); Jody Freeman, *The Private Role in Public Governance*, 75 N.Y.U. L. REV. 543, 543 (2000); Morton J. Horwitz, *The History of the Public/Private Distinction*, 130 U. PA. L. REV. 1423, 1423 (1982); Sidney A. Shapiro, *Outsourcing Government Regulation*, 53 DUKE L.J. 389, 389 (2003); Note, *Public-Private Partnerships and Insurance Regulation*, 121 HARV. L. REV. 1367 (2008).

tions are no longer good indicators of whether an activity is public health practice. Hodge and Gostin recommend a different set of criteria. Some of these criteria relate to the general character of section 905 advanced drug safety studies, while others would need to be assessed at the level of specific data use proposals.

For section 905's advanced drug safety studies, there is very specific legal authority for FDA to export Sentinel System data to outside users for such studies,[167] and a corresponding duty for FDA to see that the studies are carried out. This specificity tends to support a finding that the studies are public health practice.[168] HIPAA's public health exception requires data uses to be authorized by law. While "authorized by law" is not a defined term in HIPAA, HHS has construed it as including actions that are permitted by law as well as actions that are required by law.[169] Additionally, FDA's responsibility to protect persons whose data are in the Sentinel System arises from the agency's general ethical and legal duties as a public health authority rather than through an individualized relationship as would exist between a principal investigator and research subjects. This tends to support a finding that Sentinel System research is public health practice rather than research.[170] Finally, advanced drug safety studies with Sentinel System data will not involve experimentation in the sense of introducing experimental products into test subjects. This also tends to support a finding that it is public health practice rather than research.[171]

FDA would need to apply the remaining criteria at the level of specific proposals to use Sentinel System data: (1) If findings are generalizable beyond the community included in the study, this tends to support a finding that the activity is research rather than public health practice.[172] However, as just discussed, studies with large, inclusive data sets may tend to qualify as public health practice under this criterion. (2) Public health activities are premised on improving the health of participants, as opposed to research activities where there may be no expectation of benefit for the individual research

167 FDAAA § 905(a), 21 U.S.C.A. § 355(k)(4), (k)(4)(A)(ii) (West Supp. 2008).

168 *See* HODGE & GOSTIN, *supra* note 159, at 50–51.

169 Ctrs. for Disease Control and Prevention, *supra* note 79, at subsection titled "Disclosures for Public Health Purposes"; *see also* Standards for Privacy of Individually Identifiable Health Information, 64 Fed. Reg. 59,918, 59,929 (proposed Nov. 3, 1999) (proposing rules to protect the privacy of individually identifiable health information, including procedures and authorized and required uses of such information).

170 *See* HODGE & GOSTIN, *supra* note 159, at 51.

171 *See id.* at 52.

172 *Id.* at 51.

subject.[173] Drug safety studies are quite likely to benefit the persons whose data is used, since many of them have an established history of taking the particular drug under study or have a condition for which that drug is widely prescribed. Many advanced drug safety studies will satisfy this criterion, although this, also, needs to be assessed on a case-by-case basis. (3) Persons in the Sentinel System database are not selected by researchers in the same way human research subjects are screened and selected prior to collecting data about them. Instead, people in the database self-select by choosing to be treated with a drug that later generates an advanced drug safety question. This supports a finding of public health practice.[174] However, this, too, is a question best addressed in the context of particular studies. If the study design employs control groups or randomly selects data records to eliminate bias, it may be research rather than public health practice.[175] (4) While publication of results is not a dispositive factor, studies that intend to supply data for use in meeting FDA's drug safety reporting obligations would be more likely to qualify as public health practice.[176]

It is likely that many advanced drug safety studies will qualify as public health practice. However, it may be difficult for FDA to enunciate clear criteria, in advance, for distinguishing public health practice from research. Unless the agency can enunciate such criteria, it should not delegate authority for PIOs to make their own decisions about permissible ancillary sales. FDA may be able to specify certain broad classes of activity that unquestionably qualify as public health practice, and PIOs could be granted blanket authority to release data for those classes of activity without direct FDA review of each proposed data use. However, FDA still would need to perform case-by-case reviews of proposed data uses that do not fit in the allowed categories. It is therefore likely that FDA will need a centralized review process, at least for the ambiguous cases, and possibly for all proposed data uses if clear criteria cannot be enunciated in advance. Moreover, if FDA does grant blanket authority to PIOs, FDA will need effective reporting and auditing procedures to make sure PIOs do not make ancillary sales that go beyond the approved classes of use.

173 *Id.* at 52.
174 *Id.* at 52–53.
175 *See id.* at 53.
176 *Id.* at 49.

2. Release of Identifiable Data Under HIPAA's Public Health Exception

It is common practice, when public health agencies release data under HIPAA's public health exception, to take steps to reduce privacy risks to the persons whose data are involved.[177] These steps often include anonymizing the data (removing names and other overtly identifying information, such as patient numbers) or coding it. Multiple, conflicting terminologies are used to characterize the degree of linkage between data and individuals' identities.[178] In this Article, I will use "anonymized" to refer to data that have had patient identifiers completely and irrevocably removed before disclosure, such that future re-identification would be impossible. Anonymized data are of limited use in drug safety studies, since anonymization makes it impossible to correlate research findings with subsequent clinical observations.[179] In this Article, the term "coded"[180] refers to data that have

177 *See* Myra Moren et al., *Living With the HIPAA Privacy Rule*, 32 J.L. MED. & ETHICS 73, 76 (2004) ("In spite of the Privacy Rule's public health exemptions, provider organizations have concerns about releasing data.").

178 The HIPAA Privacy Rule recognizes two major categories of informational linkage: identified health information (which generally requires a signed authorization before it can be used by or disclosed to others) and de-identified health information (which can be disclosed and used without an authorization). However, HIPAA de-identified health information can be coded in a way that allows re-identification or can be supplied without such a code. *See* 45 C.F.R. § 164.514(b)(2)(i)(R), (c) (2007). Thus, HIPAA in effect has three categories: (1) identified; (2) de-identified but coded; and (3) de-identified and uncoded. De-identifying data under HIPAA requires either certification by a statistician that the risk of re-identification is very small, *id.* § 164.514(b)(1), or removal of eighteen specific types of information, some of which (such as dates of treatment) is potentially useful in drug safety studies, *id.* §164.514(b). HIPAA's concept of de-identification is potentially more stringent than the concept of "anonymyzation" reflected in other commonly used terminologies. *See* OHRP 2004 Guidance, *supra* note 140, at 6–7. For examples of other common terminologies, see INT'L CONFERENCE ON HARMONISATION OF TECH. REQUIREMENTS FOR REGISTRATION OF PHARM. FOR HUMAN USE, GUIDANCE FOR INDUSTRY: E15 DEFINITIONS FOR GENOMIC BIOMARKERS, PHARMACOGENOMICS, PHARMACOGENETICS, GENOMIC DATA AND SAMPLE CODING CATEGORIES 4–7 (2008) [hereinafter ICH GUIDANCE], *available at* http://www.fda.gov/cber/gdlns/iche15term.pdf; NAT'L BIOETHICS ADVISORY COMM'N, 1 RESEARCH INVOLVING HUMAN BIOLOGICAL MATERIALS i tbl.1 (1999), *available at* http://www.bioethics.gov/reports/past_commissions/nbac_biological1.pdf; Pharmacogenetics Working Group, *Terminology for Sample Collection in Clinical Genetic Studies*, 1 PHARMACOGENOMICS J. 101 (2001).

179 *See* Evans & Meslin, *supra* note 139, at 126–28.

180 My use of "coded" to imply segregation of code keys from the data user corresponds to terminology developed by the National Bioethics Advisory Commission in 1999. *See* NAT'L BIOETHICS ADVISORY COMM'N, *supra* note 178, at i tbl.1. The requirement that code keys be segregated from data users is also consistent with OHRP's

been stripped of overtly identifying information (such as names or patient identification numbers) and labeled with a code, with the code key inaccessible to the data user.[181] Segregating code keys from data users renders data unidentifiable, by which term I mean "unidentifiable by the data user."[182] Data users, acting alone without cooperation of the code key holder, would not be able to link coded data to specific individuals. If data users do have access to the code key or other information from which they could trace data to particular individuals, the data would be considered "identifiable," that is, identifiable by the data user. "Fully identified" data, in this Article, are data that have been conveyed to the data user with overtly identifying information such as names or patient numbers. Fully identified data are a subset of identifiable data.

HIPAA's public health exception allows Sentinel System data to be shared with outside users without privacy authorizations, provided that the use qualifies as public health practice. Although many public health agencies do anonymize or code data when making such disclosures, HIPAA's public health exception does not require them to do so.[183] A matter of great concern is that HIPAA's public health excep-

---

current policy for unconsented use of coded specimens and health data under the Common Rule. *See* OHRP 2004 Guidance, *supra* note 140, at 2–4. It also is consistent with the HIPAA Privacy Rule's standard for determining whether coded data or specimens can be treated as de-identified; this standard requires nondisclosure of code keys. *See* 45 C.F.R. § 164.514(c).

181 FDA's new International Conference on Harmonisation (ICH) terminology recognizes two subcategories of coding, one of which segregates code keys from the investigator/data user. The other does not necessarily do so. *See* ICH GUIDANCE, *supra* note 178, at 4–5. In ICH terminology, "double-coded" data are coded twice, and the data user has no access to at least one of the code keys. The data user, acting alone, would not be able to re-identify double-coded data, so these data would qualify as "coded" in the sense envisioned in this Article. ICH also recognizes a category of "single-coded" data, for which the investigator/data user may have access to the code key. If the investigator has code-key access, ICH "single-coded" data would not qualify as "coded" under my terminology or under the National Bioethics Advisory Commission terminology or under OHRP's 2004 Guidance, nor could it be considered "de-identified" under the HIPAA Privacy Rule. *See id.*

182 In other contexts, such as in determining whether informed consent is required under the Common Rule, "identifiable" data are generally understood to mean "identifiable by the data user," for example, the data may be coded, so that the data user does not receive overtly identifying information such as the names or social security numbers of people who are in the database, but the data user has access to the code key and could re-identify the data without enlisting the cooperation of any third parties (such as FDA, the PIO, or a trustee that holds the code key). Under the Common Rule, coded data are not regarded as identifiable by the data user if the data user has no access to the code key. *See* OHRP 2004 Guidance, *supra* note 140, at 3–4.

183 *See supra* note 73.

tion technically would allow release of Sentinel System data to outside users in identifiable or even fully identified form. Section 905 also would allow this, provided the outside data users comply with certain conditions (such as, not redisclosing identifiable information when reporting their findings, and agreeing to be bound by the HIPAA Privacy Rule and other provisions that deter redisclosure).[184] Thus, FDA has legal authority to allow release of identifiable data to outside data users.

It is doubtful that FDA intends to approve release of identifiable data as a routine matter, since identifiable data are not really needed for many types of advanced drug safety study. Most study objectives can be achieved with coded, rather than identifiable, data.[185] Coding of data affords a high degree of privacy protection if coding is properly done, with segregation of code keys from data users and with enforceable penalties for mishandling the code keys. Coding generally renders patients unidentifiable by investigators who are working with their data, as well as by others who might come into possession of the data via the investigators.[186] At the same time, coding lets research findings be correlated with subsequent clinical observations and would let FDA, or its code-key trustee, trace data back to individual patients when follow-up observations or data collection are required. FDA's policy on outside uses of Sentinel System data should require use of coded data, rather than data that are identified or identifiable by investigators, whenever this is consistent with study objectives.

Identifiable data occasionally are needed, for example, if the purpose of a study is to screen Sentinel data to find suspected cases of a particular adverse drug reaction and then follow up directly with patients or their physicians to ascertain reasons for the problem. Given the important interests at stake when a proposed study needs identifiable data, FDA should maintain tight control over approval of such requests and should provide ongoing oversight of each such study. Release of identifiable data is not suitable for a blanket-certificate approach that lets PIOs make their own decisions to release identifiable data subject to FDA-approved criteria. Each such request should be separately and directly approved by FDA. Essential characteristics of public health practice are direct performance or oversight by a governmental public health authority (or its authorized partner)

184 *See supra* Part I.B.

185 *See* Evans & Meslin, *supra* note 139, at 127.

186 *Id.*

and accountability to the public for its performance.[187] To the extent that HIPAA's public health exception allows release of identifiable data, the agency should remain directly accountable to the public for those releases.

C. Ensuring Ethical Research Use of Sentinel System Data

The scope of advanced drug safety studies under section 905 is broad enough to include activities that will not qualify as public health practice and would have to be regarded as research. Releasing Sentinel System data for research presents ethical issues when data have been obtained under HIPAA's public health exception. Section 905 instructs FDA to convene a committee of experts to advise the Secretary on ethical issues surrounding the use and communication of data.[188] Whether to allow research with Sentinel System data is an obvious item to include on that committee's agenda.[189] If research is deemed to be ethically permissible, then the Privacy Rule's waiver provision,[190] described below, supplies a legal basis for releasing data to researchers. If FDA pursues this course, several follow-up questions need to be addressed: (1) Would release of data for research under HIPAA's waiver provision violate public trust and, if so, should FDA implement a waiver process that affords better protections than the Privacy Rule requires? (2) What should FDA's policy be regarding research with data in identified or identifiable, coded, and anonymized form? (3) What framework of human subject protections should FDA adopt for research uses of Sentinel System data? These questions are discussed below.

1. HIPAA Provisions for Waiver of Privacy Authorization

The Privacy Rule contemplates that data in public health databases sometimes will be released for use in research; this can include release of data in identified or identifiable form. An Institutional Review Board (IRB) or Privacy Board of the HIPAA-covered entity that holds the data can waive or alter HIPAA's usual authorization requirement.[191] A waiver allows data to be used with no individ-

187 *See* HODGE & GOSTIN, *supra* note 159, at 8.

188 FDAAA § 905(a), 21 U.S.C.A. § 355(k)(3)(B)(iii) (West Supp. 2008).

189 FDA's proposed organizational structure includes a research component, so this decision already may have been made. *See* U.S. FOOD & DRUG ADMIN., *supra* note 4, at 16.

190 45 C.F.R. § 164.512(i) (2007).

191 *See id.* § 164.512(i)(1)(i).

ual authorization at all. An alteration lets data be used subject to modified procedures for obtaining individual authorizations.[192]

The body (either an IRB or Privacy Board) that approves the waiver must document that the research poses minimal privacy risks.[193] For this purpose it is sufficient that there be an "adequate plan" to protect the identifiers from improper use and disclosure; an "adequate plan" to destroy identifiers at the earliest opportunity consistent with research objectives (which could mean "never," so long as justification is given for retaining the identifiers indefinitely); and "adequate" written assurances that the data will not be reused or disclosed.[194] Also, it must be documented that the research would be impracticable without the waiver and without access to the identifiable health data.[195]

The glaring issue here is, "Whose IRB or Privacy Board has the power to make these decisions?" Under HIPAA, an IRB or Privacy Board constituted by any HIPAA-covered entity that lawfully holds data has the power to approve a waiver.[196] Section 905 requires outside data users to agree, contractually, to become HIPAA-covered entities.[197] As such, they would have the power to grant waivers. Thus there is little real privacy protection in section 905's requirement for outside parties to agree to comply with the HIPAA Privacy Rule. To earn any public trust, FDA must go beyond this minimal requirement. FDA should require all PIOs and outside data users to relinquish their rights to exercise HIPAA's waiver provision to redisclose Sentinel System data. This is absolutely necessary with respect to releases of identified or identifiable data. It also may be desirable with respect to releases of coded data, although there are other ways to address pri-

192 An example of an alteration would be to use passive ("opt-out") consent. This involves giving some form of public notice of plans to use data in a particular research study. For example, this might include publishing notice of the research study in newspapers or on websites known to be frequented by persons whose data the researcher wishes to use. The notice describes the data ("all claims submitted to XYZ insurance company between 2004 and 2006"). It then provides a contact address or telephone number to which insured persons can respond if they do not want their data used in that study. If they fail to reply, it is presumed that their data may be used in the study. There are non-U.S. examples of passive consent procedures and at least one reported U.S. example where passive consent was used under HIPAA's alteration provisions. *See* Benjamin Littenberg & Charles D. MacLean, *Passive Consent for Clinical Research in the Age of HIPAA*, 21 J. GEN. INTERNAL MED. 207 (2006).

193 45 C.F.R. § 164.512(i)(2)(ii).

194 *Id.* § 164.512(i)(2)(ii)(A)(1)–(3).

195 *Id.* § 164.512(i)(1)(ii)(B)–(C).

196 Ctrs. for Disease Control & Prevention, *supra* note 79, at 5–6.

197 FDAAA § 905(a), 21 U.S.C.A. § 355(k)(4)(G)(i)(I) (West Supp. 2008).

vacy concerns with coded data (for example, by adopting human-subject protections for the Sentinel System that set clear standards for coding and handling of code keys).[198] At a minimum, FDA should centralize and control the process for exercising HIPAA's waiver provision to approve research uses of identifiable or fully identified data.

Even if FDA centralizes this function in its own IRB or Privacy Board, there still are problems due to procedural weaknesses of the Privacy Rule itself. If the Privacy Rule currently enjoys public trust, it is a fragile trust that rests on the public's ignorance of what its waiver provisions actually allow. FDA would be well advised to implement a more formal and transparent waiver-approval process than the Privacy Rule requires. Under the Privacy Rule, an IRB that is approving a waiver must follow the usual procedural norms of the Common Rule for IRB decisionmaking.[199] The Common Rule lets decisions be made in nonpublic proceedings by simple majority voting of a group that may be—and usually is—staffed primarily by insiders of the entity that holds the data,[200] subject only to scant and occasional oversight by an external regulator.[201] HIPAA Privacy Boards, also staffed primarily by insiders, proceed in their usual manner although, when granting waivers, they are required to have a majority of their members present and include at least one person who is not an insider of the entity that is releasing the data.[202] This lone non-insider does not have a veto and can easily be outvoted. Moreover, HIPAA allows an alternative, expedited procedure where the Privacy Board chair can approve a waiver

198 See *infra* Part III.C.2.

199 45 C.F.R. § 164.512(i)(2)(iv)(A) (2007).

200 *See id.* §§ 46.103(b)(3), 46.108(b).

201 *See* OFFICE OF INSPECTOR GENERAL, U.S. DEP'T OF HEALTH & HUMAN SERVS., INSTITUTIONAL REVIEW BOARDS: A TIME FOR REFORM 9, C-3, C-4 (1998) [hereinafter OIG, IRB A TIME FOR REFORM], *available at* http://www.oig.hhs.gov/oei/reports/oei-01-97-00193.pdf (indicating that FDA aims to inspect IRBs that operate under FDA's regulations once every five years); OFFICE OF INSPECTOR GENERAL, U.S. DEP'T OF HEALTH & HUMAN SERVS., INSTITUTIONAL REVIEW BOARDS: THEIR ROLE IN REVIEWING APPROVED RESEARCH 3 (1998) [hereinafter OIG, IRB ROLE IN REVIEWING], *available at* http://www.oig.hhs.gov/oei/reports/oei-01-97-00190.pdf (estimating that 2,000–5,000 IRBs are in operation at academic medical centers and research institutions in the U.S.); OFFICE OF INSPECTOR GENERAL, U.S. DEP'T OF HEALTH & HUMAN SERVS., PROTECTING HUMAN RESEARCH SUBJECTS 8, 9, 16 (2000) [hereinafter OIG, HUMAN RESEARCH SUBJECTS], *available at* http://www.oig.hhs.gov/oei/reports/oei-01-97-00197.pdf (finding on-site and spontaneous reviews of IRBs operating under the Common Rule are extremely rare, with only eighteen site visits between 1990 and April 1996; one such visit between April 1997 and May 1998; and ten visits between June 1998 and March 2000).

202 45 C.F.R. § 164.512(i)(2)(iv)(B) (2007).

acting alone or can appoint one or more individuals to make the decision.[203]

FDA simultaneously will be acting as regulator of Sentinel System privacy and as a major consumer of Sentinel System data.[204] These dual roles imply a conflict of interest. Since ancillary sales of data help defray costs of system operation, they could reduce the cost of data FDA acquires for its own uses. If FDA's own IRB or Privacy Board is in charge of approving waivers to enable ancillary sales, FDA's conflict of roles will, at the very least, pose problems of public perception. This is all made worse by the procedural weakness of HIPAA's waiver provisions, which fall far below basic due process norms expected in other infrastructure regulatory contexts where a regulator is making determinations that have mandatory effect on the public and which prejudice the interests of affected parties.[205] People whose data are released under HIPAA's waiver provisions are entitled, if they come forward and request it, to receive a brief accounting of such releases after the releases occur.[206] They have no predeprivation due process right to be notified that a waiver is under consideration. They have no right to be heard before the waiver is approved, nor are they entitled to receive notice that their data have been released, even after the fact. Finally, there is scant reviewable record of IRB or Privacy Board deliberations or of the criteria applied when determining that privacy protections were "adequate" and privacy risks were "minimal." To merit public trust, FDA must implement a waiver process that goes considerably beyond what the Privacy Rule requires.

2. FDA Policy on Research Use of Identified, User-Identifiable, Coded, and Anonymized Data

Section 905 and the Privacy Rule allow release of data in identifiable form to outside parties. If the data use qualifies as public health practice, such releases are lawful under HIPAA's public health exception.[207] If the data use is research, the additional step of approving a waiver is required.[208] In practice, most IRBs and Privacy Boards considering a waiver likely would not regard privacy risks as "minimal" when identifiable data are involved; thus they would not grant the

203 *Id.* § 164.512(i)(2)(iv)(C).

204 *See supra* Part II.

205 *See* GÓMEZ-IBÁÑEZ, *supra* note 32, at 19 (discussing the need for elaborate procedural safeguards in coercive regulatory decisionmaking).

206 45 C.F.R. § 164.528 (2007).

207 *See id.* § 164.512(b)(1)(i).

208 *See supra* Part III.C.1.

waiver. As a point of law, however, identifiable data can be released under HIPAA's waiver provision. This could occur if the party receiving identifiable data had given convincing assurances that the data would be handled carefully, and the IRB or Privacy Board was satisfied that privacy risks were indeed "minimal."[209] HHS's Office of Civil Rights, which administers the HIPAA Privacy Rule, has never provided clear guidance on specific conditions that must be met in order for privacy risks to be minimal. OHRP, which administers similar waiver provisions under the Common Rule, also has never clarified the term. Its meaning is left to discretion of IRBs and Privacy Boards which, as noted, have conflicts of interest and operate with little transparency or public accountability.[210]

Ethical and privacy considerations demand that release of identifiable data from the Sentinel System should be the rare exception, rather than a common occurrence, as already discussed.[211] If FDA adopts a decentralized decisional model that allows PIOs to make ancillary sales of data for research use subject to FDA-approved criteria, FDA still should maintain centralized control over releases of identified data and data that would be identifiable by the data user. At most, PIOs should only have discretion to release data in anonymized form or in coded form, subject to clear requirements to segregate code keys from the data recipients and subject to effective auditing and enforcement. All releases of Sentinel System data, in whatever form, should be subject to an FDA-approved framework of human-subject protections.

3. Human-Subject Protections in Research with Sentinel System Data

For readers desiring a short cut through this discussion, which is technical in nature, the conclusions are: FDA currently has no framework of human-subject protections for research with Sentinel System data. FDA may wish to consider adopting the Common Rule for this purpose. However, even if FDA does adopt the Common Rule, there still are avenues for release of anonymized, coded, identifiable, and identified data without informed consent when necessary to support FDA-authorized research with Sentinel System data.

FDA's current research ethical framework does not define "human subjects" in a way that supports meaningful distinctions among data that are fully identified, identifiable by researchers,

209 *See supra* notes 193–95 and accompanying text.
210 *See supra* notes 200–01 and accompanying text.
211 *See supra* Part III.B.2.

coded, or de-identified/anonymized.[212] Moreover, FDA's human-subject protections, in their current form, would not apply to section 905 advanced drug safety studies. FDA's regulations were designed for clinical trials and define "human subject" as "an individual who is or becomes a participant in research, either as a recipient of the test article or as a control."[213] Persons whose data are in the Sentinel System do not meet this definition, so their informed consent is not required.[214] Nor does IRB review appear to be required. FDA's IRB regulation is identical to the Common Rule in terms of how IRBs are constituted and what functions they perform.[215] However, FDA's IRB regulation does not define circumstances that trigger an IRB review. Instead, provisions elsewhere in FDA's regulations invoke IRB review in specific relevant contexts.[216] At present, there are no provisions

212 *See* Evans & Meslin, *supra* note 139, at 138.

213 21 C.F.R. § 50.3(g) (2008) (informed consent regulation); *id.* § 56.102(e) (IRB review).

214 In recent years, similar problems have surrounded the status of persons whose tissue specimens are used in FDA-regulated research. *See* Evans & Meslin, *supra* note 139, at 138. In 1999, FDA attempted to construe its regulations as requiring informed consent for the use of coded or identified tissue specimens in medical device research. *See* DIV. OF BIORESEARCH MONITORING, U.S. DEP'T OF HEALTH & HUMAN SERVS., GUIDANCE FOR FDA STAFF: REGULATING *In Vitro* Diagnostic Device (IVD) Studies 4 (1999), http://www.fda.gov/cdrh/comp/ivdreg.pdf. In doing so, FDA relied on a definition of "human subject," elsewhere in its investigational device exemption regulations, that includes persons "on whose specimen" research is performed. 21 C.F.R. § 812.3(p) (2007). However, there is no definition anywhere in FDA's regulations that includes persons on whose data research is performed. FDA's 1999 Guidance was challenged as amounting to a de facto amendment of FDA's informed consent regulation without proper administrative procedures. Evans & Meslin, *supra* note 139, at 143–62. In 2006, FDA issued a new Guidance that lets researchers who do not wish to follow the 1999 Guidance voluntarily opt into a regime that lets coded specimens be used in research without informed consent, provided certain steps are taken to protect the privacy of people whose specimens are used. *See* Guidance on Informed Consent for *In Vitro* Diagnostic Device Studies Using Leftover Human Specimens That Are Not Individually Identified 71 Fed. Reg. 23,924, 23,924–25 (Apr. 25, 2006); OFFICE OF IN VITRO DIAGNOSTIC DEVICE EVALUATION & SAFETY, U.S. DEP'T OF HEALTH & HUMAN SERVS., GUIDANCE ON INFORMED CONSENT FOR *IN VITRO* DIAGNOSTIC DEVICE STUDIES USING HUMAN SPECIMENS THAT ARE NOT INDIVIDUALLY IDENTIFIABLE (2006), http://www.fda.gov/cdrh/oivd/guidance/1588.pdf. This 2006 Guidance, which applies only to medical device research and not to drug research, is generally consistent with OHRP's policy on research use of coded tissue specimens. *See* OHRP 2004 Guidance, *supra* note 140. However, FDA did not address the issue of research with coded health data, either in medical device research or more generally.

215 21 C.F.R. § 56 (2008).

216 *See, e.g.*, *id.* § 312.23(a)(1)(iv) (requiring sponsors' commitment to IRB review of clinical studies in the context of investigational new drug applications); *id.*

expressly requiring IRB review when Sentinel System data are used in research.

There is much to be said for having FDA adopt the Common Rule to govern research uses of Sentinel System data. This need not disrupt FDA's continued use of its existing human-subject protections in clinical trials. FDA could implement the Common Rule solely for use in the Sentinel System. Doing so would facilitate collaborations with academic entities already subject to the Common Rule, whether because their studies of Sentinel System data are being federally funded or because they have signed a Federalwide Assurance that places all of their research under the Common Rule.[217] Adopting the Common Rule also would avoid the appearance that different types of data in the Sentinel System are entitled to different levels of human-subject protection: Medicare data are supplied by HHS and HHS implements the Common Rule;[218] are data from other sources, such as private health insurers, entitled to any less protection? Finally, the Common Rule's definition of "human subject" appropriately recognizes that privacy risks to research subjects vary, depending on the amount of identifying information researchers receive about them.[219] It supports meaningful distinctions among identified, identifiable-by-the-researcher, coded, and de-identified data.[220] This is a crucial concept for purposes of managing risks to persons whose data are included in a data network.

If FDA did place the Sentinel System under the Common Rule, would the Common Rule require informed consent of people whose data are used in advanced drug safety studies? For research with anonymized or coded data, the answer clearly is, "No." The Common

---

§ 314.50(d)(3)(i) (requiring a statement that each study was conducted in compliance with IRB regulations as part of the application for FDA approval of a new drug).

217 *See* Evans & Meslin, *supra* note 139, at 134–38; *see also* OIG, IRB ROLE IN REVIEWING, *supra* note 201, at B-1 (estimating that seventy-five percent of research funded by the National Institute of Health is carried out at research institutions that have voluntarily agreed to apply the Common Rule to all research at their institutions).

218 *See* 45 C.F.R. § 46.101–.124 (2007).

219 *See* OHRP 2004 Guidance, *supra* note 140, at 2–4; *see also* 45 C.F.R. § 46.102(f) (defining human subject as "a living individual about whom an investigator . . . conducting research obtains (1) data through intervention or interaction with the individual, or (2) identifiable private information"); *id.* § 46.101(b)(4) (exempting human subject research involving the collection or study of information "that is publicly available or . . . is recorded by the investigator in such a manner that subjects cannot be identified, directly or through identifiers linked to the subjects" from human subject research protection under the regulations).

220 *See* Evans & Meslin, *supra* note 139, at 140–41.

Rule, interpreted by OHRP's 2004 Guidance, would not require informed consent for such releases, provided code keys are inaccessible to the outside data user.[221] This same Guidance sets standards for coding and protection of code keys.[222] Sentinel System procedures would need to meet or exceed those standards. FDA may, in fact, wish to set higher standards. OHRP's 2004 Guidance relies heavily on contractual assurances that code keys will be protected and lacks clear provisions for auditing and enforcing performance of the contracts.[223] The Sentinel System's coding standards should include credible mechanisms to reassure the public that standards actually are being enforced.

The remaining question is whether the Common Rule requires informed consent for release of data in identified or identifiable form. The answer is, "Not necessarily." The Common Rule generally does require informed consent for research with data that are identifiable by the research investigator.[224] However, the Common Rule provides four different legal pathways for unconsented use of such data. Two of the pathways are not entirely serviceable in the context of Sentinel System advanced drug safety studies. However, the other two pathways would support unconsented release of identifiable (or identified) data for such studies.

The two pathways that appear not to work are the Common Rule exemptions[225] most frequently invoked when there is a need to arrange unconsented research use of identifiable data. One of these, the exemption at 45 C.F.R. § 46.101(b)(4), allows unconsented research with existing data in identifiable form, provided the investigator records information in a way that would not let subjects be reidentified. At first glance, this seems to match what section 905 allows: outside parties conducting advanced drug safety studies may use identifiable data from the Sentinel System, but may not report results in a way that includes identifiable information.[226] The problem is that OHRP has construed "existing" data to mean data that existed at the time the IRB approved the exemption—that is, prior to the start of the study.[227] Thus the section 46.101(b)(4) exemption would not support advanced drug safety studies that intend to use data received

221 OHRP 2004 Guidance, *supra* note 140, at 4–6.

222 *Id.*

223 *See id.* at 3.

224 *See id.* at 2–6.

225 45 C.F.R. § 46.101(b)(4)–(5) (2007).

226 FDAAA § 905(a), 21 U.S.C. § 355(k)(4)(G)(i) (West Supp. 2008).

227 *See* Letter from Kristina C. Borror, Div. of Compliance Oversight, Office for Human Research Prots., U.S. Dep't of Health & Human Servs., to Daniel E. Ford,

into the Sentinel System after the studies commence. This precludes correlation of research findings with subsequent clinical observations. Technically, there are ways around this problem; for example, FDA could establish a continuously active IRB that re-approves section 46.101(b)(4) exemptions on a daily basis, so as to include newly "existing" data that have been added to the Sentinel System since the prior day. This would be lawful but cumbersome.

The Common Rule also has a public benefit exemption, at section 46.101(b)(5), that is similar in spirit to HIPAA's public health exception. Unfortunately, the two are not coextensive in terms of the types of study they allow. The Common Rule allows unconsented use of identifiable data in "research," but the permissible types of research are directed more at studying and evaluating public benefit programs themselves, rather than developing generalizable knowledge to further the public health objectives of such programs.[228] Section 905 advanced drug safety research falls into that latter category. Advanced drug safety studies are instrumental to FDA's public health practice, but they are not a study of FDA's public health practice itself. The Office for Protection from Research Risks (precursor of OHRP) provided guidance on application of this exemption.[229] It is a question of interpretation whether section 905 advanced drug safety studies meet the criteria provided in that guidance, but it appears that they would not.

Again, these problems do not affect research use of coded data, since unconsented use of coded data already is allowed under the Common Rule without resorting to its section 46.101(b) exemptions.[230] These problems only affect release of identifiable data. The Common Rule does, however, offer two additional pathways for unconsented research with identifiable data. First, the Common Rule's waiver and alteration provisions[231] are very similar to those in the HIPAA Privacy Rule. In any situation where HIPAA authorization can be waived, it is highly likely that informed consent also can be

---

Vice Dean for Clinical Investigation, Johns Hopkins Univ. Sch. of Med., et al., at 4 (July 17, 2007), *available at* http://www.hhs.gov/ohrp/detrm_letrs/YR07/jul07d.pdf.

228 *See* 45 C.F.R. § 46.101(b)(5).

229 *See* OPRR Guidance, *supra* note 159.

230 *See* OHRP 2004 Guidance, *supra* note 140, at 3–4.

231 *See* 45 C.F.R. § 46.116(d). To grant a waiver under the Common Rule, an IRB must determine that: (1) the research involves no more than minimal risk (including privacy related risks); (2) waiver or alteration will not adversely affect rights and welfare of subjects; (3) the research could not practicably be carried out without waiver or alteration; and (4) where relevant, subjects will receive additional pertinent information after participation. *Id.*

waived. Second, if FDA adopts the Common Rule for the Sentinel System, 45 C.F.R. § 46.101(d) lets department or agency heads exempt specific research activities or classes of activity from some or all of the provisions of the Common Rule. This exemption could be invoked for specific advanced drug safety studies that require identifiable data. Given the important privacy interests that are at stake when identifiable data are released to outside parties, this requirement of high-level agency approval arguably gives the decision the dignity it deserves.

IV. The Coercive Nature of Decisions Allowing Access to Sentinel System Data

FDA's decisions approving access to Sentinel System data by PIOs and outside data users will have coercive effect on people whose data are involved. Despite its long regulatory history, FDA has surprisingly little experience making decisions that have mandatory effect on the public. FDA's signature regulatory function—approving new products for sale—is enabling rather than coercive, both for the product sponsor and for the public. No one is forced to take FDA-approved drugs. In contrast, coercive governmental power is an essential characteristic of public health law.[232] The same is true of infrastructure regulation; for example, FERC approval of a new pipeline forces some people to have steel pipe in their back yards. Operating in relatively uncontentious decisional terrain where its actions had only optional public effect, FDA never had to develop the level of procedural safeguards expected when regulators flex coercive powers. Public trust in the Sentinel System can exist only if FDA implements credible safeguards now. "If the government's unique and coercive powers are to be used against members of society, then the public is understandably anxious that coercion will be used fairly and only for important public purposes. The well-warranted price of using coercion in a democracy is usually elaborate procedural safeguards . . . ."[233]

It may be helpful, here, to explain the degree to which FDA traditionally has relied on voluntary acquiescence of the entities it regulates, rather than coercive regulatory power. Denying a product approval obviously has major impact on the product's sponsor, but the decision is not coercive in the sense of interfering with vested rights, since there is no right to have one's product approved. FDA's

232 *See* Gostin, *supra* note 146, at 5, 18–20.

233 Gómez-Ibáñez, *supra* note 32, at 19.

authority to withdraw a previously-granted drug approval[234] comes closer to being coercive, since the sponsor may have made large manufacturing and marketing investments in reliance on the approval. Here, as one might expect, FDA implements robust procedural safeguards: the sponsor receives prior notice and opportunity for a hearing.[235] An approval can be summarily suspended by the Secretary of HHS if the drug poses an "imminent hazard," but even here the sponsor has an opportunity for an expedited hearing.[236] The Secretary cannot delegate the authority to decide that a summary suspension is warranted, although authority to conduct the expedited hearing is delegated to FDA.[237] Decisions to withdraw an approval are subject to judicial review.[238]

In practice, FDA rarely has invoked its authority to withdraw approvals,[239] instead tending to press manufacturers voluntarily to stop selling injurious products,[240] which they often would do to limit tort liability even absent any pressure from FDA. Except for infant formulas[241] and medical devices since 1990,[242] FDA has no authority to order product recalls and, again, relies heavily on voluntary recalls by the manufacturer.[243] Once a drug is approved, FDA imposes various inspection, monitoring, and reporting requirements[244] many of which are only voluntary.[245] The largely-voluntary reporting mechanisms on which FDA was relying, prior to FDAAA, were estimated to detect only one to ten percent of all adverse drug reactions.[246] Only since passage of FDAAA in 2007 has FDA had the power to compel a

234 21 U.S.C. § 355(e) (2006). A complete list of grounds for withdrawal is set forth at 21 C.F.R. § 314.150 (2008).

235 21 U.S.C. § 355(e); 21 C.F.R. § 314.150(a).

236 21 U.S.C. § 355(e).

237 *Id.*; *see also* Geoffrey M. Levitt et al., *Human Drug Regulation*, *in* 2 FUNDAMENTALS OF LAW AND REGULATION 159, 178–79. (David G. Adams et al. eds., 1999).

238 21 U.S.C. § 355(h) (2006).

239 Levitt et al., *supra* note 237, at 178.

240 I. Scott Bass, *Enforcement Powers of the Food and Drug Administration: Drugs and Devices*, *in* 2 FUNDAMENTALS OF LAW AND REGULATION, *supra* note 237, at 55, 70–74.

241 21 U.S.C. § 350a(e)(1) (2006).

242 Safe Medical Devices Act of 1990 § 8, 21 U.S.C. § 360(h)(e)(2006).

243 Bass, *supra* note 240, at 70.

244 *See* 21 C.F.R. § 314.80–.81 (2008).

245 *See* Wood et al., *supra* note 8, at 1851, 1853.

246 *Frontline Interview with Paul Seligman* (PBS television broadcast Nov. 4, 2002) (transcript available at http://www.pbs.org/wgbh/pages/frontline/shows/prescription/interviews/seligman.html (citing the one to ten percent figure for all adverse events but noting that the system was estimated to detect between one-third to one-half of all serious adverse events).

change in product labeling[247] or to condition the sale of a drug on specific measures to mitigate safety risks.[248] Until then, these steps required a willing manufacturer. FDAAA also broadened FDA's authority to force manufacturers to conduct postmarket studies and clinical trials.[249] Prior to FDAAA, the agency claimed it had such authority[250] but applied it very hesitantly. There was just one context where FDA clearly did have statutory authority to require postmarket studies[251]—to confirm the effectiveness of drugs approved under the agency's accelerated approval program.[252] Even here, FDA relied on voluntary compliance by manufacturers and notoriously failed to require timely commencement or completion of the studies it "required" manufacturers to conduct.[253] FDA has surprisingly little experience wielding coercive power even with respect to manufacturers of the products it regulates and certainly not with respect to the public.

There is only one context where FDA previously has made decisions with coercive effect on the public: waiver of informed consent for certain kinds of clinical trials. FDA's section 50.24 waiver provi-

247 FDAAA § 901(a), 21 U.S.C.A. § 355(o)(4) (West Supp. 2008) (letting FDA notify manufacturers of safety information it believes should be included in drug labeling). Following a period of response and discussions with the manufacturer, FDA may order the safety information to be included. *See id.*, 21 U.S.C.A., § 355(o)(4)(B)–(D)(E).

248 *See id.* § 901(b), 21 U.S.C.A. § 355-1(a)(1)–(2) (authorizing FDA to require risk evaluation and mitigation strategies for newly and already approved drugs). FDA may require such strategies to include conditions for marketing and sales, such as restrictions on how, where, and by what type of professional the drug may be prescribed or requirements that patients receive monitoring or testing to manage risks. *See* 21 U.S.C.A. § 355-1(f)(3) (West Supp. 2008); *see also* FDAAA § 902(a), 21 U.S.C.A. § 352(y) (West Supp. 2008) (allowing drugs to be considered misbranded if manufacturers fail to comply with such restrictions).

249 *See* FDAAA § 901(a), 21 U.S.C.A. § 355(o)(3) (West Supp. 2008) (allowing FDA to require postmarket studies or clinical trials of drugs with known or suspected safety problems); *id.* § 902(a), 21 U.S.C.A. § 352(z) (allowing drugs to be regarded as misbranded if manufacturer fails to conduct required postmarket studies).

250 FDA claimed the power to require postmarket studies was implicit in the agency's power to enforce the FDCA and to require drug companies to provide data bearing on whether previously granted approvals should be withdrawn. *See* 21 U.S.C.A. §§ 355(k); 371(a) (West 1999 & Supp. 2008), *see also*, Levitt et. al, *supra* note 237, at 179.

251 New Drug, Antibiotic, and Biological Drug Product Regulations; Accelerated Approval, 57 Fed. Reg. 13,234, 13,236 (proposed Apr. 15, 1992); New Drug, Antibiotic, and Biological Drug Product Regulations; Accelerated Approval, 57 Fed. Reg. 58,942, 58,953–54 (codified as amended at 21 C.F.R. pts 314 & 601).

252 21 C.F.R. § 314.540 (2008).

253 *See* Susan Okie, *What Ails FDA?*, 352 NEW ENG. J. MED. 1063, 1064 (2005).

sions[254] are not at all like those of the Common Rule and HIPAA Privacy Rule,[255] which allow unconsented use of people's health data if an IRB deems privacy risks to be minimal. FDA has never allowed waivers of this type. However, FDA does let informed consent be waived in clinical trials to test new products intended for use in patients with serious, life-threatening medical emergencies.[256] Patients who would be candidates for testing these products typically are so seriously ill—often, they are unconscious—that they cannot give consent to be treated with an experimental product. Unless consent is waived, such products could not be tested in human subjects and their safety and efficacy would remain unknown. FDA allows IRBs to waive consent for such trials if various conditions are met.[257] For example, there must be a prospect that the product may directly benefit the particular patient.[258] There also must be consultations with representatives of the communities where the research will be carried out[259] and public disclosure of plans to draw research subjects from emergency patients in those communities.[260]

Emergency consent waivers typically are approved by IRBs at the institutions conducting the research. However, FDA ultimately decides whether to allow clinical trials to go forward.[261] FDA's internal procedures require all trials involving a waiver of informed consent to receive centralized review by FDA's own Division of Scientific Investigations.[262] In this respect, FDA's waiver procedures are far superior to those of the Common Rule and HIPAA Privacy Rule. The latter two rules let private, potentially conflicted decisionmakers—IRBs and Privacy Boards—grant waivers with no centralized review, before the research goes forward, by a publicly accountable governmental body. IRBs and Privacy Boards are not subject even to the most rudimentary procedural norms of regulatory decisionmaking,

254 21 C.F.R. § 50.24 (2008).

255 See *supra* Parts III.B.1 & III.C.3.

256 21 C.F.R. § 50.24(a)(1).

257 *Id.* § 50.24(a)(1)–(7).

258 *Id.* § 50.24(a)(3).

259 *Id.* § 50.24(a)(7)(i).

260 *Id.* § 50.24(a)(7)(ii).

261 If the experimental product is a drug, the drug's sponsor submits an Investigational New Drug (IND) application to FDA at least thirty days before the trial is set to begin. 21 C.F.R. § 312.40 (2008). FDA has thirty days to object to the IND, after which the IND becomes effective and the clinical trial may begin. If FDA is not satisfied with the proposed plan, FDA can impose a clinical hold that delays the trial until FDA's concerns are satisfactorily addressed. *Id.* § 312.42.

262 *See* CDER, MANUAL OF POLICIES AND PROCEDURES, *supra* note 111, § 6030.8, at 4–5.

such as the Administrative Procedure Act's[263] requirements for reasoned, evidence-based decisionmaking; independent decisionmakers; due process rights for affected parties; reviewable records; and rights of appeal.[264] FDA correctly regards the approval of consent waivers to be a coercive regulatory determination which should not be delegated entirely to private organs of the entities FDA regulates.

That said, FDA's centralized review process for consent waivers lacks the procedural formality and transparency that are needed to merit public trust. FDA promulgated its emergency research waiver provision in 1996[265] and in the following decade received about sixty requests to conduct clinical trials under waivers.[266] Inexperienced in making coercive decisions, FDA drew heavily on lax procedural norms that had characterized human-subject protections since the 1960s. These norms grew out of informal Policies for the Protection of Human Research Subjects first issued by the National Institutes of Health (NIH) in 1966.[267] These informal policies were hastily incorporated in regulations promulgated on May 30, 1974 by the Department of Health, Education, and Welfare[268] (predecessor of HHS) in reaction to a well-publicized scandal with the Tuskegee Syphilis Study.[269] Two months later, a National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research was established under the National Research Act of 1974.[270] It met from 1974 to 1978 and was followed by the President's Commission for the Study of Ethical Problems in Medicine and Biomedical and Behavioral Research in the early 1980s.[271] The Common Rule rests on design

263 Ch. 324, 60 Stat. 237 (1946) (codified as amended at scattered sections of 5 U.S.C.).

264 *See* 5 U.S.C.A. §§ 551–559, 701–706 (West 2007 & Supp. 2008); Carl H. Coleman, *Rationalizing Risk Assessment in Human Subject Research*, 46 ARIZ. L. REV. 1, 13–17 (2004); Barbara J. Evans, *Inconsistent Regulatory Protection Under the U.S. Common Rule*, 13 CAMBRIDGE Q. HEALTHCARE ETHICS 366, 372 (2004).

265 Protection of Human Subjects; Informed Consent, 61 Fed. Reg. 51,498, 51,498 (Oct. 2, 1996) (codified as amended at 21 C.F.R. pts. 50, 56, 312, 314, 601, 812, 814).

266 Conduct of Emergency Clinical Research; Public Hearing, 71 Fed. Reg. 51,143, 51,143 (Aug. 29, 2006).

267 *See* OFFICE FOR HUMAN RESEARCH PROTS., U.S. DEP'T OF HEALTH & HUMAN SERVS., INSTITUTIONAL REVIEW BOARD GUIDEBOOK intro., pt. A (1993), *available at* http://www.hhs.gov/ohrp/irb/irb_introduction.htm.

268 *Id.*

269 *See generally* JAMES H. JONES, BAD BLOOD: THE TUSKEGEE SYPHILIS EXPERIMENT (2d ed. 1993) (detailing the history of the experiment and its consequences).

270 Pub. L. No. 93-348, §§ 201–205, 88 Stat. 342, 348–51 (expired May 18, 1979 pursuant to § 204 (e)).

271 *See* OFFICE FOR HUMAN RESEARCH PROTS., *supra* note 267, intro. pt. A.

concepts from this era.[272] FDA's own human-subject protections,[273] first issued in 1981, were later harmonized with the Common Rule and share many of its provisions.[274]

Both regulations were originally designed for use in interventional research—clinical trials where subjects are directly involved, rather than studies involving only their tissues or data. As applied to interventional research, the regulations afford two main protections: (1) the assurance that someone other than the research investigator—an IRB—will review the risks of research and make a discretionary determination whether those risks comply with stated regulatory standards[275] and (2) an opportunity for subjects to give their informed consent prior to the research intervention.[276] A certain amount of procedural laxity was tolerable in IRB decisionmaking precisely because the vulnerable class—human research subjects—had the right of informed consent. Research subjects were not actually forced to rely on the IRB to protect them; ultimately, they could protect themselves by refusing to participate in the research.

This same procedural laxity ceased to be acceptable when IRB review was extended to other contexts, such as approving waivers for research with health data and for emergency research. Here, there is no opportunity for individual self-protection; IRB decisions do have coercive effect. To rely on closed, informal procedures is equivalent to letting insiders in a back room at the power company decide whether consumers' rates satisfy the Federal Power Act's "just and reasonable" standard, or letting insiders of a pipeline company decide that building a forty-eight-inch diameter pipeline through your back yard serves the public convenience and necessity, without your having

272 *See* OIG, IRB A TIME FOR REFORM, *supra* note 201, at 3; *see also* ROBERT J. LEVINE, ETHICS AND REGULATION OF CLINICAL RESEARCH 324 (2d ed., 1986).

273 21 C.F.R. pts. 50, 56 (2008).

274 OIG, HUMAN RESEARCH SUBJECTS, *supra* note 201, at 8.

275 Both the Common Rule and FDA regulations adopt an identical two-part standard: (1) risks should be minimized to the extent consistent with sound research, and (2) risks should be reasonable in relation to anticipated benefits, if any, to the research subjects and the importance of the knowledge that may reasonably be expected to result from the research. 45 C.F.R. § 46.111(a)(1)–(2) (2007) (Common Rule); 21 C.F.R. § 56.111(a)(1)–(2) (2008) (FDA regulations).

276 *See* NAT'L BIOETHICS ADVISORY COMM'N, 1 ETHICAL AND POLICY ISSUES IN RESEARCH INVOLVING HUMAN PARTICIPANTS ii, iv, xi (2001), http://www.bioethics.gov/reports/past_commissions/nbac_human_part.pdf (identifying the twin protections of IRB review and informed consent); *see also* Coleman, *supra* note 264, at 7, 10 (citing problems with the sufficiency of informed consent as a protective mechanism, and arguing that insufficiency of consent creates a need for more robust procedures for IRB decisionmaking).

an opportunity to participate and comment. The FERC reviews applications for certificates of public convenience and necessity in formal proceedings, noticed and open to the public and offering due process protections to all affected groups.[277] Consent waivers warrant a level of procedural formality more like that of a FERC section 7(c) certification proceeding than a traditional IRB meeting. Instead, the waiver provisions of the Common Rule, the HIPAA Privacy Rule, and FDA regulations all failed to incorporate the enhanced procedural protections that coercive decisions require. FDA partially addressed this problem by requiring centralized, prior review of research involving waivers.[278] However, FDA procedures afford less than a full set of due process protections.[279]

Quite predictably, FDA's emergency-research waiver provisions generated controversy, culminating in a 2006 scandal over clinical trials of a blood substitute, PolyHeme, intended for use in injury victims who had lost substantial quantities of blood.[280] Since the product could be stored in ambulances and was compatible with all blood types, it offered promise as a way to keep accident victims alive in field settings where regular blood transfusions were unavailable. The clinical trials took place in thirty-two communities in eighteen states.[281] People injured and unconscious in those communities were at risk to receive PolyHeme unless they wore, at all times, a blue brace-

277 *See* 18 C.F.R. § 157.5–.21 (2008).

278 *See* CDER, MANUAL OF POLICIES AND PROCEDURES, *supra* note 111, § 6030.8, at 4–5.

279 *See id.* FDA's review of clinical trials involving an exception from informed consent under 21 C.F.R. § 50.24 includes review by FDA's Division of Scientific Investigation (DSI) of the IRB's plans for community consultation and public disclosure within the communities where the research will be carried out. *Id.* at 5. However, FDA has never enunciated a clear standard regarding what forms of community consultation will be considered adequate, nor does decisionmaking follow basic norms of notice, transparency of decisions, and opportunities for the public to appeal before research goes forward.

280 For critiques of the PolyHeme trial, see Letter from Senator Charles E. Grassley, Chairman, Senate Comm. on Fin., to Michael Leavitt, Secretary, U.S. Dep't of Health & Human Servs. (Mar. 13, 2006), *available at* http://finance.senate.gov/press/Gpress/2005/prg031306.pdf; *see also* Karla F.C. Holloway, *Accidental Communities: Race, Emergency Medicine, and the Problem of PolyHeme*, AM. J. BIOETHICS, May 2006, at 7, 12–16 (citing the trial as an example of systematic racial bias in prehospital emergency medical care); Ken Kipnis et al., *An Open Letter to Institutional Review Boards Considering Northfield Laboratories' PolyHeme Trial*, AM. J. BIOETHICS, May 2006, at 18, 18 (claiming that "there is a serious ethical flaw" in the trial).

281 Letter from Senator Grassley, *supra* note 280, at 2.

let stating, "I decline the Northfield PolyHeme® Study."[282] Use of PolyHeme would continue not only in transit to the hospital but for several hours afterward, when standard blood transfusions would have been available. Earlier trials of another blood substitute product had caused serious injuries among some patients who received it.[283] FDA's required community consultation process allegedly failed to supply adequate information to the affected public and many people were unaware a study was taking place.[284] Even those who were aware objected to the notion that they should be burdened with wearing a bracelet to avoid unconsented treatment with a potentially dangerous product.[285]

In retrospect, the PolyHeme trial did not cause widespread injuries,[286] but it drew attention to the coercive nature of consent waivers. FDA held public hearings shortly after the scandal in 2006.[287] Comments filed by members of the public, though not a scientific sample, suggest a lack of public trust. Asked whether the criteria for approving studies under the section 50.24 waiver provisions were adequate, comments ranged from, "No they are not adequate. There will always be somebody to push the limits for 'THE GOOD OF SOCIETY' "[288] to "This really scares me and gives me visions of Mengele and the

282 Press Release, U.S. Senate Comm. on Fin., Grassley Questions FDA's Sanction of Blood Substitute Study Without Informed Consent 2 (Feb. 23, 2006), *available at* http://www.senate.gov/~finance/press/Gpress/2005/prg022306a.pdf.

283 *See* Charles Natanson et al., *Cell-Free Hemoglobin-Based Blood Substitutes and Risk of Myocardial Infarction and Death*, 299 JAMA 2304, 2307 tbl.2 (2008) (discussing risks of PolyHeme and four other blood substitutes); *id.* at 2310 (pointing out that FDA let PolyHeme trials go forward despite adverse events in previous trials of other blood substitutes).

284 *See* Letter from Senator Grassley, *supra* note 280, at 2.

285 *See* Press Release, U.S. Senate Comm. on Fin., *supra* note 282, at 1.

286 *See* Natanson et al., *supra* note 283 at 2307, 2310 (indicating some increase in the relative risk of mortality and serious adverse events, although noting questions about the statistical significance of these increased risks).

287 *See* U.S. Food & Drug Admin., U.S. Dep't of Health & Human Servs., Public Hearing on Emergency Research and Human Subject Protections (Oct. 11, 2006) http://www.fda.gov/ohrms/dockets/dockets/06d0331/06d-0331-tr00001-vol4.rtf; *see also* U.S. Food & Drug Admin., U.S. Health & Human Servs., 2006D-0331: Guidance for Institutional Review Boards, Clinical Investigators, and Sponsors, Exception from Informed Consent Requirements for Emergency Research (Jan. 31, 2007), http://www.fda.gov/ohrms/dockets/dockets/06d0331/1.htm (cataloguing documents relevant to the hearings including comments from consumers and other concerned parties).

288 Sandra Sells, FDA Comment No. EC30 (Sept. 21, 2006), http://www.fda.gov/ohrms/dockets/dockets/06d0331/06D-0331-EC30.htm.

Nazis."[289] Public distrust was a perfectly predictable consequence of applying informal procedural norms, developed for use in nonmandatory decisionmaking, to a new context where decisions have coercive effect.

Section 50.24 emergency consent waivers affect, at most, a few hundred people per year. The public, as a whole, may not feel threatened by emergency-research waivers. People risk becoming involved in emergency research only if they get into a serious medical emergency; none of us ever thinks that will happen to us. The Sentinel System is a different story. It involves 100 million people, who need only visit a doctor's office, fill a prescription, or file an insurance claim to risk being placed in the Sentinel database. This risk is palpable to all members of the public, who have no means to self-protect and are entirely reliant on FDA's decisional processes to protect their rights.

V. LESSONS FROM OTHER INFRASTRUCTURE REGULATORY CONTEXTS

Framing Sentinel System privacy as a bioethical problem may not be the best way to achieve solutions that will earn public trust. The field of bioethics offers no good answer to the question, "What is a proper framework for coercive decisionmaking?" Contemporary bioethics starts from the premise that autonomous individuals ought not be coerced.[290] When coercion does become necessary, as in vari-

289 Lillian Kehoe, FDA Comment No. EC11 (Sept. 11, 2006) http://www.fda.gov/ohrms/dockets/dockets/06d0331/06D-0331-EC11.htm.

290 The field of bioethics, as it developed in the 1950s and 1960s, drew heavily on a Kantian, atomistic concept of autonomy that conceives individuals as self-reliant, self-governing, and individualistic. *See* ALFRED I. TAUBER, PATIENT AUTONOMY AND THE ETHICS OF RESPONSIBILITY 13 (2005). The concept is similar to Fallon's "ascriptive" autonomy, which entails each person's sovereignty over his or her moral choices. Richard H. Fallon, Jr., *Two Senses of Autonomy*, 46 STAN. L. REV. 875, 890–93 (1994). At the birth of bioethics, the field was principally concerned with the rights of patients as against physicians in a paternalistic healthcare system; strong assertions of individual autonomy were an antidote to imbalances of power in that relationship. *See* TAUBER, *supra* at 15–16; *see also* DAVID J. ROTHMAN, STRANGERS AT THE BEDSIDE 258 (1991) ("Patients are also likely to be sparing with the deference and trust they accord to physicians . . . , reserving for themselves critical decisions about treatment."). Balancing individual rights against broader public interests has not been a major focus of bioethical thought. The notion, "Individuals are free to enjoy their rights, so long as they do not encroach on the rights of others," embodies an atomistic concept of autonomy, as Tauber has noted. Tauber, *supra* at 119 (citing GRACE CLEMENT, CARE, AUTONOMY, AND JUSTICE (1996)). Yet the atomistic concept of autonomy poses a problem: it offers no account of why and when the moral sovereignty of the individual should yield to public interests. It leaves policymakers with Aleinikoff's "external-scale" problem—the search for an external, objective set of values by which to balance

ous public health and other regulatory contexts, bioethics may have little to offer beyond, "Coercion is wrong." That is not the question here. In passing FDAAA, Congress made a determination that coercion is necessary to reduce the carnage of drug-related injuries;[291] respect for autonomy does not require us to let individuals control the secrecy of their medical records at a cost of injuries and death to others. The question now is how to promote legitimacy and public acceptability of decisions to use and disclose Sentinel System data. The available options, at this point, are either to press Congress for repeal of FDAAA, or else to focus on creating robust institutional protections for individuals within what is, unabashedly, a coercive regulatory framework. Framing the question as, "What institutional protections are appropriate?" lets policy be informed by norms of coercive decisionmaking in other regulatory contexts. The objective of this Article was to pose this question, rather than to answer it, but below I present a few thoughts about directions in which answers may lie.

A. Industry Structure

FDA must weigh the appropriate structure for the industry that supplies LPHD to the Sentinel System. This is crucial not as a matter of economic regulation, but because industry structure affects privacy. Certain critical functions—in particular, the longitudinal linkage of patients' health data—require access to identifiable information; other functions do not. Privacy may best be protected by eschewing vertical integration, segregating key functions that use identifiable health information as inputs, and sharply restricting the number of PIOs licensed to perform those key functions. Having fewer PIOs

competing interests. *See* T. Alexander Aleinikoff, *Constitutional Law in the Age of Balancing*, 96 YALE L.J. 943, 962–63, 975 (1987). The atomistic concept of autonomy, embraced by 1960s-era bioethicists, has no internal scale. Only more recently, after 1980, have bioethicists begun to explore alternatives, such as a view of autonomy as "not merely an internal, or psychological characteristic but also an external, or social one," with individuals achieving autonomy in cooperation rather than in isolation. *See* TAUBER, *supra* at 120–22 (quoting CLEMENT, *supra*, at 22). This latter view eventually may allow bioethicists to wield questions that require balancing of individual and societal interests. However, such inquiries remain poorly developed in the field of bioethics at this time.

291 *See, e.g.*, J. Lazarou et al., *Incidence of Adverse Drug Reactions in Hospitalized Patients*, 279 JAMA 1200, 1200 (1998) (estimating that 0.32% of prescriptions written kill the patient, placing adverse drug reactions between the fourth and sixth leading causes of death at U.S. hospitals; another 6.7% of prescriptions result in injuries serious enough to put the patient in the hospital or prolong the stays of already hospitalized patients).

means fewer employees handling patients' sensitive health data and, therefore, fewer chances for inadvertent or malicious disclosure. Reducing the number of PIOs also facilitates meaningful auditing and enforcement, which often have been lacking in other privacy and human-subject protection contexts where regulators are spread too thinly.[292] However, structural alternatives must be weighed in light of second-order problems each may cause. For example, granting monopolies in key infrastructure functions may require further regulation to manage bottlenecks, ensure reliability of service, and prevent abuses of monopoly power.

B. Contracts vs. Rules to Set Regulatory Standards

FDA faces a major decision on how to enunciate standards, terms, and conditions to govern PIOs and data users. One alternative is contract-based regulation, which sets standards via contracts negotiated with the respective PIOs and data users. The major alternative is to set generally applicable standards through rulemaking (rule-based regulation). Rule-based regulation was part of the original paradigm of American infrastructure regulation. It sometimes is called "discretionary" regulation,[293] since the regulator exercises discretion in interpreting the rules and applying them to specific fact situations. However, I prefer the term "rule-based regulation" in the U.S. setting, where contract-based regulation typically is implemented by appointing a regulatory agency to represent the government in contract negotiations.[294] When this is true—as in the Sentinel System—contract-based regulation still involves regulatory discretion, when the regulator decides whether to accept or reject various contract terms. The choice between contract- and rule-based regulation is merely a choice of how the regulator's discretion will be exercised.

The Sentinel System raises two separate questions: (1) whether standards should be set via individually negotiated contracts, via generally applicable rules, or through a combination of both approaches; and (2) whether FDA should retain centralized control over key discretionary decisions (such as deciding whether a given data use fits within the scope of section 905), or delegate at least some discretion

292 *See supra* note 201 and accompanying text.

293 *See, e.g.*, GÓMEZ-IBÁÑEZ, *supra* note 32, at 12–13, 30–32; Chen, *supra* note 33, at 1628.

294 *See* Guislain & Kerf, *supra* note 125, at 1, 3–4. When contract-based regulation is implemented in foreign settings, it sometimes involves direct negotiation of regulatory contracts between the private infrastructure operator and the government, without necessarily creating a special-purpose industry regulatory agency to oversee negotiation and ongoing oversight of the contract.

for PIOs and data users to interpret standards own their own. As to this first question, FDAAA does not constrain FDA's choice. Section 905 expressly authorizes FDA to negotiate contracts with PIOs and data users.[295] However, section 905 amends a preexisting statute, the Federal Food, Drug, and Cosmetic Act, which already imbues FDA with broad general rulemaking and adjudicative authority.[296] Thus, FDA is free to use either approach or a mix of the two. There is extensive literature and experience bearing on the advantages and disadvantages of contract- and rule-based regulation.[297]

The most serious problem with contract-based regulation is contractual incompleteness[298]—that is, the impossibility of foreseeing and providing for every future contingency at the time contracts are being negotiated. Particularly in new infrastructure industries, it is difficult to anticipate changes in the multiparty relationship among PIOs, the regulator, users of infrastructure services, and the general public.[299] Rule-based regulation allows flexibility to set broad, open-textured standards and rely on later interpretations by the regulator to fill gaps and adapt standards to changing circumstances.[300]

Other potential problems with contract-based regulation are inconsistency and problems with transparency. Different PIOs may be subject to different contract terms, and it may be difficult for the public to ascertain what the standards are, when standards are dispersed in multiple, separate contracts. Even if FDA chooses to rely on contracts to set some of the business and financial terms governing PIOs, public trust will be enhanced by using generally-applicable rules to establish core privacy protections. Chen has noted the risk of collusion between governmental bodies and PIOs, particularly at the point when contracts come due for renegotiation; this collusion can sell out the interests of the people.[301] Contract negotiations are, in this respect, riskier than rule-based regulation in that they involve the exercise of discretion but without the procedural and other safeguards that typically are built into a rule-based scheme.[302]

---

295 FDAAA § 905(a), 21 U.S.C.A. § 355(k)(3)(C)(v), (k)(4)(F) (West Supp. 2008).

296 *See, e.g.*, 21 U.S.C. § 371 (2006).

297 *See, e.g.*, GÓMEZ-IBÁÑEZ, *supra* note 32, at 28, tbl.2.1 (comparing the two approaches).

298 *See* Chen, *supra* note 33, at 1628 (citing Oliver Hart & John Moore, *Incomplete Contracts and Renegotiation*, 56 ECONOMETRICS 755 (1988)).

299 *See id.* (citing GÓMEZ-IBÁÑEZ, *supra* note 32, at 11–12, 27–30).

300 *See id.*

301 *See id.* at 1649.

302 *Id.* at 1649–50.

FDA should not be enslaved by the modern trend toward contract-based regulation. This trend reflects, in part, widespread use of contract-based regulation in foreign settings.[303] There, private investors often distrust rule-based regulation, fearing that the government will opportunistically change the rules after investments are made or fearing that judicial oversight of regulators will be weak.[304] Contract- and rule-based systems both have good, stable track records in the United States, so FDA should be able to attract private investors under either approach, provided the underlying regulatory standards are well conceived. The modern critique of rule-based regulation in the United States has tended to center on the fact that it can be cumbersome and inefficient.[305] However, this critique arose late in the twentieth century, when the challenge was to optimize use of already-built infrastructures, rather than to get new infrastructures built.[306] Chen notes that rule-based regulation actually may be the more efficient alternative under the economic conditions that prevailed earlier in the twentieth century,[307] that is, when major new infrastructures were being built. When FDA is overseeing new infrastructure development, rule-based regulation may be the best way to address uncertainties and problems with contractual incompleteness. Even proponents of contract-based regulation, such as Gómez-Ibáñez, acknowledge that rule-based regulation has enjoyed practical success in such contexts.[308]

A perceived disadvantage of rule-based regulation is that it entails burdensome regulatory procedures to constrain the regulator's ongoing exercise of discretion.[309] However, this should not be a decisive factor in the choice between contract- and rule-based regulation for the Sentinel System, since elaborate procedural protection of the public interest will be needed, either way. Contract-based regulation has been widely and successfully used in industries, like energy and telecommunications, where the public interest standard is directed toward protecting the public from economic harms. It is relatively straightforward to set rates or rate formulas via contract terms. How-

303 *See generally* Shirley, *supra* note 125 (surveying the effectiveness of contract-based regulation in 565 infrastructure privatizations).

304 GÓMEZ-IBÁÑEZ, *supra* note 32, at 15; Chen, *supra* note 33, at 1620–21; Smith & Wellenius, *supra* note 93, at 2–3.

305 *See, e.g.*, Chen, *supra* note 33, at 1631 (noting the public utility regulation has been criticized as raising questions of "indeterminacy and inefficiency").

306 *Cf. id.* at 1620–21 (discussing the changes in infrastructure priorities from the nineteenth to twentieth centuries).

307 *Id.* at 1633, 1650.

308 GÓMEZ-IBÁÑEZ, *supra* note 32, at 353–56; *see also* Chen, *supra* note 33, at 1631–33.

309 Chen, *supra* note 33, at 1669.

ever, the Sentinel System's public-interest standard involves subtle judgments about the scientific value of proposed data uses and the acceptability of various degrees of privacy risk. These standards will be difficult to reduce to explicit contract language, and rule-based regulation very well may emerge as the superior alternative.

C. Degree of Centralization of Discretionary Decisions

This Article already has taken the position that certain key decisions—particularly those involving release of identifiable data—must remain under centralized FDA control.[310] The concern was that decentralized decisionmaking could erode public trust due to its reliance on conflicted decisionmakers (local IRBs and Privacy Boards). Whether to decentralize decisionmaking is not just a matter of conflicts of interest, however. This choice also can affect the quality of regulatory decisions. Decentralization may be the better option, when decisions turn on information that is more readily available in the local context. Centralization is generally better when decisions require comparisons among multiple alternatives that may not all be visible to local decisionmakers.

The core concept of section 905's public-interest standard is that coercive disclosure of people's private health information is warranted only when the proposed data use offers significant public health benefits. Implementing this standard implies comparing the relative merits of various proposed uses of data, so that the public is not exposed to privacy risks for marginally beneficial studies.[311] Thus, decisions about permissible data uses and ancillary sales of Sentinel System data should not be decentralized to PIOs. Each PIO's perspective is limited to the discrete set of proposed uses that happen to come before it. Individual PIOs are not in a position to rank proposals on the national scale that is required, to ensure people's privacy is jeopardized only for the highest-valued uses. It may be possible, however, for FDA to specify certain categories of data use that unquestionably do have high priority. PIOs might be granted limited discretion to allow sales that fit clearly within those categories. However, defining the permissible categories is a high-level task requiring centralized coordination—and therefore one that should be done by FDA.

310 *See supra* Part III.B.2.

311 *See supra* Part I.A.

D. Ensuring Independence and Legitimacy of Regulatory Decisionmaking and Adequate Resources for Credible Regulatory Oversight

Independence is fundamental to the legitimacy of a regulator's decisions. 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 adequate, stable funding to support regulatory activities—"to foster the requisite expertise to underpin those arm's-length relationships."[312]

IRBs and Privacy Boards make heavy use of voluntary staffing by insiders of the institutions being regulated and, having no independent source of funding, usually depend on the regulated institutions for their operating budgets. Lacking independence, they lack legitimacy in contexts that require them to make coercive decisions.[313] The Sentinel System will not merit public trust if FDA delegates decisionmaking to IRBs and Privacy Boards of the PIOs and data users.[314] Even centralizing decisions in FDA's own IRB or Privacy Board will not ensure their legitimacy, unless these bodies have the attributes of independence.[315] As already noted, FDA is conflicted by its dual roles as a consumer of Sentinel System data and privacy regulator. For many years, FDA enjoyed a reputation as one of the most trusted regulatory agencies in the United States.[316] However, in 2006, the Institute

312 Smith, *supra* note 91, at 1.

313 An arm's length relationship between regulatory decisionmakers 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*, PUB. POL'Y FOR THE PRIVATE SECTOR, Apr. 1999, at 2 box 1, *available at* http://rru.worldbank.org.documents/publicpolicyjournal/175 bacon.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 decisionmaking bodies were in place: was there a regulator that was separate from the regulated companies and from political authorities?).

314 *Cf.* Richard Shelby, *Accountability and Transparency: Public Access to Federally Funded Research Data*, 37 HARV. J. ON LEGIS. 369, 370 (2000) ("Transparency and accountability in government are two principles crucial to securing public trust.").

315 *See* Smith, *supra* note 91, at 1.

316 U.S. Food & Drug Admin., U.S. Dep't of Health & Human Servs., FDA Protects the Public Health; Ranks High in Public Trust (Feb. 2002), http://www.fda.gov/opacom/factsheets/justthefacts/1fda.pdf (reporting results of an independent survey, conducted in 1999, which found high levels of public trust in FDA).

of Medicine found the agency's credibility seriously tarnished by a perceived lack of transparency and public accountability, failure to follow through with proposed initiatives, and slowness requiring compliance by its regulated entities.[317] The public is unlikely to trust FDA to protect Sentinel System privacy unless the agency scrupulously adheres to norms of regulatory independence and legitimacy.

One option is to segregate functions within FDA, so that oversight of privacy is separate from the divisions within FDA that are users of Sentinel System data. This approach may or may not be credible to the public. Privacy and ethical oversight divisions within HHS agencies have, historically, been underfunded, lightly staffed, and relatively disempowered within the agencies of which they are components.[318] OHRP, which administers the Common Rule, has only thirty-four personnel[319] to oversee decisions by 3,000 to 5,000 IRBs and a nationwide portfolio of NIH-funded research valued at $28 billion annually, eighty-three percent of which is awarded via 50,000 grants to over 3,000 remote universities, medical schools, and research institutions.[320] At this staffing level, auditing, enforcement, and oversight are necessarily light.[321] HHS' Office for Civil Rights (OCR), which administers the HIPAA Privacy Rule under similar constraints, did not impose a single civil fine and prosecuted only two criminal cases in its first three years of operation.[322] For comparison, the FERC has 1295 personnel[323] and the FCC has 1814[324]—levels more in line with a credible oversight effort. An independent privacy-protection body,

317 COMM. ON THE ASSESSMENT OF THE U.S. DRUG SAFETY SYS., *supra* note 13, at 17–18.

318 OFFICE OF INSPECTOR GENERAL, U.S. DEP'T OF HEALTH & HUMAN SERVS., THE FOOD AND DRUG ADMINISTRATION'S OVERSIGHT OF CLINICAL TRIALS, 10–18 (2007), *available at* http://www.oig.hhs.gov/oei/reports/oei-01-06-00160.pdf (discussing factors, including resource and data constraints, that undercut FDA's ethical oversight of clinical trials).

319 Office for Human Research Prots., U.S. Dep't of Health & Human Servs., Staff Directory, http://www.hhs.gov/ohrp/about/staff.html (last visited Nov. 14, 2008).

320 Nat'l Inst. of Health, U.S. Dep't of Health & Human Servs., NIH Overview, http://www.nih.gov/about/NIHoverview.html (last visited Nov. 14, 2008).

321 *See supra* note 201 and accompanying text.

322 Ron Stein, *Medical Privacy Law Nets No Fines*, WASH. POST, June 5, 2006, at A1.

323 Fed. Energy Regulatory Comm'n, U.S. Dep't of Energy, Frequently Asked Questions, http://www.ferc.gov/o12faqpro/default.asp?Action=Q&ID=17 (last visited Oct. 6, 2008) (reporting a full year 2006 budget of $220 million and 1295 employees).

324 Office of Managing Dir., Fed. Commc'ns Comm'n, 2007 Annual FCC Employee Survey Responses 2, http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-280549A1.pdf (last visited Nov. 14, 2008) (reporting 1814 employees as of November 2007).

whether within or outside FDA, can earn credibility only if it is adequately funded and staffed.

If FDA follows the model of OHRP and OCR and assigns a handful of people to oversee the privacy of 100 million Americans, the public rightly will perceive that privacy is being taken lightly. On the other hand, huge regulatory staffs do not guarantee meaningful protection, and the public is reluctant to bear their costs. Smart regulation, rather than big regulation, may be the right approach. An example of smart regulation is HHS's reliance on qui tam[325] actions as a means of detecting and policing Medicare fraud.[326] An enormous staff of regulatory auditors would be required to detect fraud in the complex healthcare setting. HHS leverages the efforts of its own auditors by empowering employees of healthcare institutions and other industry insiders, who ultimately are in the best position to detect fraud when it is occurring, to initiate qui tam actions against entities suspected of violating the Civil False Claims Act.[327] HHS may elect to join such actions and carry them forward, but the person originating the suit is allowed to share in the sums recovered.[328] FDA might devise similar incentives to encourage insiders of PIOs and data users to keep their eyes open and report privacy violations, thus leveraging the efforts of its own oversight personnel.

"To be autonomous, regulatory agencies must first have their own resources—from their own funding resources."[329] FDA as a whole has been under severe budgetary pressure in recent years.[330] It seems implausible that the agency will divert resources from its already-

325 31 U.S.C. § 3730(b)–(d) (2006).

326 *See* Dan McGuire & Mac Schneider, *Health Care Fraud*, 44 AM. CRIM. L. REV. 633, 389 (2007) ("Qui tam actions are a growing method of healthcare fraud enforcement. In 1993 there were 132 qui tam actions and by 2003 this number had jumped to approximately 3260.").

327 31 U.S.C. § 3730 (2006).

328 *See id.* § 3730(d).

329 Antonio Estache, *Designing Regulatory Institutions for Infrastructure—Lessons from Argentina*, PUBLIC POLICY FOR THE PRIVATE SECTOR, May 1997, at 1, *available at* http://rru.worldbank.org/documents/publicpolicyjournal/114estac.pdf.

330 *See, e.g.*, Michael D. Green, *Statutory Compliance and Tort Liability: Examining the Strongest Case*, U. MICH. J.L. REFORM 461, 476 (1997) ("FDA is woefully underfunded for its mandate, which includes regulatory oversight of products that account for more than twenty-five percent of all American consumer purchases . . . . 'It is glaringly apparent that FDA cannot now execute all of its statutory responsibilities within the limitations of existing resources.'" (quoting ADVISORY COMM. ON FOOD & DRUG ADMIN., FINAL REPORT 11 (1991))); Alicia Mundy, *Congress Presses FDA on Budget Woes, Investigative Arm*, WALL ST. J., June 11, 2008, at A19 ("Members of Congress are questioning the management and priorities of [FDA's criminal investigation wing], in the context of FDA budget problems.").

underfunded core functions to ensure robust oversight of Sentinel System privacy. During the past fifteen years, the problem of funding regulatory agencies has been a focus of attention both in developed and developing nations.[331] The challenge is to harness private sector funds to reduce reliance on governmental appropriations to support regulatory oversight, without undermining the regulator's independence.[332]

One widely used approach is user fees, in which regulated entities pay fees for specific oversight services that the regulator provides.[333] FDA relies heavily on user fees to fund its drug and device approval processes.[334] User fees generate problems—real and perceived—with the regulator's independence, in situations where the regulator's underlying duty is to protect the public rather than the commercial entities that are paying its fees. For this reason, FDA should avoid funding its privacy-protection functions with user fees paid by PIOs, data users, and others whose interests may be adverse to those of the public. A better approach, from the standpoint of preserving independence, is used by some U.S. infrastructure regulatory agencies. This approach levies small fees that are spread broadly among members of the protected class, for example, the people who consume goods and services that the regulated industry supplies. The FERC is funded, in part, by a small surcharge amounting to a couple of cents added to the price of every thousand cubic feet of natural gas that is transported through an interstate pipeline.[335] The charge is collected and remitted to the FERC by pipelines, which include it in their rates,

331 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 4–7 (Oct. 8, 2003), http://www.oocur.org/Proceedings/Presentations/RiviereSmith1.pdf (detailing regulatory funding in the Bahamas).

332 *See supra* notes 312–14 and accompanying text.

333 *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 FDA's use of user fees).

334 *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).

335 *See* 18 C.F.R. § 382.101, .202 (2008) (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).

but ultimately is paid by gas consumers.[336] The regulator is not beholden to the industry, but to the consumers whose interests it protects. Moreover, the regulator is not captive to any particular constituency since diverse stakeholders (for example, industrial and residential consumers) all contribute to its support, and fees are not tied to particular matters that the regulator is asked to resolve.

By analogy, Sentinel System privacy oversight could be funded by charging patients a few cents on any healthcare transaction that generates health records or insurance claims. These fees could be gathered by healthcare providers and insurers for remittance to FDA. The costs of privacy oversight would be paid by the protected class, patients. Privacy regulators' budgets would not be dependent on the PIOs and data users they are regulating. Some scholars may object that privacy is a right, and the public should not have to pay for privacy protection. However, the alternatives are for privacy protection to go unfunded, to be funded by entities with adverse commercial interests, or to be funded at inadequate levels through governmental appropriations. Given these alternatives, paying a small fee for meaningful privacy protection may make sense to members of the public. Experience in other industries suggests the public is quite willing to pay for privacy—for example, many airline passengers voluntarily pay a fifteen dollar booking fee to telephone their credit card numbers directly to airline ticketing agents, rather than sending this sensitive information over the Internet.[337]

E. Appropriate Risk Sharing to Support System Financing and Privacy

Financial constraints pose the greatest single threat to Sentinel System privacy. FDA will come under pressure to allow wider data sales to help defray costs of system development. Governmental appropriations are unlikely to be adequate to pay for the system entirely. The financing plan will depend, in part, on revenues from other data users. PIOs face risks in making large, up-front, asset-specific investments,[338] because their ability to make future data sales is

336 *See id.* § 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.").

337 A fifteen dollar fee may in fact be conservative for today's travel industry, as, for instance, Delta and United Airlines both now charge a twenty-five dollar fee for reservations made by phone. Delta Airlines Official Website, http://delta.com (last visited Nov. 14, 2008); United Airlines Official Website, http://united.com (last visited Nov. 14, 2008).

338 Chen, *supra* note 33, at 1624 (defining asset specificity as "the relative difficulty of transferring assets intended for use in one transaction to other uses").

uncertain. To get the Sentinel System built, FDA must resolve these risks just enough to let private investment go forward, without abandoning the agency's duty to protect people's privacy. This is a classic infrastructure financing problem and FDA should draw on lessons other infrastructure regulators have learned when solving similar problems in other industries.

FDA has two basic tools for reducing the risks private investors face. One tool is money and the other is privacy policy. FDA could agree to pay a price in its future purchases of LPHD for FDA's own use that is high enough to repay the investments PIOs will be making to develop infrastructure for supplying the LPHD. Then, no ancillary data sales would be needed, and FDA could adopt a privacy policy that forbids them. The problem with this approach is that FDA does not have that much money;[339] Congress has not given FDA enough money to "buy" privacy outright. At the other extreme, FDA could adopt a permissive privacy policy that lets PIOs make any ancillary data sale they want to make. This obviously would breach FDA's duty to protect individual privacy.[340]

To resolve this dilemma, FDA needs to deploy its available funds skillfully. "Skillful" means exploring options other than direct public financing of the Sentinel System infrastructure. Payments for FDA's purchases of LPHD are a form of direct public financing. If FDA relies solely on this mechanism, the money will run out, and the system still will not be built. At that point, FDA will face enormous pressure to adopt a lax privacy policy to ensure completion of the system. To avoid this outcome, FDA must deploy funds in ways that achieve what inarticulately is called "additionality"—in other words, each dollar FDA puts forward should unlock additional funds from other, private financing mechanisms. FDA needs to develop a multifaceted Sentinel System infrastructure financing facility,[341] which might, for example, include loan guarantees to ensure PIOs will repay private borrowing, or risk guarantees to address specific uncertainties that

339 *See supra* note 135 and accompanying text (discussing limitations of Congress' appropriations for the Sentinel System).

340 *See supra* Part I.B (discussing FDA's duty to protect the privacy of individuals in the Sentinel System).

341 Anand Chandavarkar, *Infrastructure Finance: Issues, Institutions, and Policies* (The World Bank Policy Research Working Paper No. 1374, 1994), *available at* http://www-wds.worldbank.org/external/default/WDSContentServer/IW3P/IB/1994/11/01/000009265_3970716141904/Rendered/PDF/multi_page.pdf (analyzing the distinctive features of infrastructure financing and the principle issues for policymakers to address); *see also* Klingebiel & Ruster, *supra* note 53 (presenting case studies of infrastructure financing facilities at various stages of development).

threaten to block private financing. Direct contractual obligations for FDA to pay for Sentinel System LPHD may be part of the financing facility, but they only should be one part of it.

A related question is whether revenues from approved outside data uses and ancillary sales should flow entirely to the PIO, or whether a portion of these revenues should be harnessed to help fund system development and cross-subsidize FDA's own public health uses of Sentinel System data. FDA may wish to explore tariffication strategies that identify several different classes of users and grant them access on different terms and conditions, including graduated fees for access to Sentinel System data. This strategy would be similar to the approach long used by American public utilities, in which a published tariff defines several groups of similarly situated customers (for example, industrial electricity consumers, small commercial users, and households) and sets pricing, terms, and conditions of service for each group.[342] Different groups pay different prices, but the similarly situated customers within each group are treated alike.[343] By analogy, researchers conducting the highest-priority drug safety studies might receive free access to Sentinel System data, subject to their agreement to make results available for FDA to share with physicians and patients. Academic researchers who agree to place their research findings in the public domain might be charged a lower fee than commercial users who desire to patent their discoveries. User groups that are deemed to pose the greatest threats to privacy could be charged higher fees that help defray the cost of extra regulatory oversight, compliance monitoring, and enforcement activities that will be required to reassure the public that these data users are not compromising individual privacy.

Designing infrastructure financing facilities is a highly developed art that has been extensively plied since 1990 in developing economies where public funds are scarce and private investors are hard to recruit.[344] FDA should not reinvent the wheel. It should draw on the vast expertise resident at agencies such as the U.S. Agency for International Development, the U.S. Export-Import Bank, and the Organiza-

342 *See* PHILLIPS, *supra* note 37, at 438–41 (discussing permissible discrimination among user classes in utility rate design); William H. Lawrence & John H. Minan, *Financing Solar Energy Development Through Public Utilities*, 50 GEO. WASH. L. REV. 371, 407 (1982).

343 *See* Lawrence & Minan, *supra* note 342, at 407.

344 *See generally* INFRASTRUCTURE NETWORK, THE WORLD BANK, INFRASTRUCTURE: LESSONS FROM THE LAST TWO DECADES OF WORLD BANK ENGAGEMENT (2006) (discussing efforts to design infrastructure financing in various countries since the late 1980s).

tion for International Cooperation and Development (the World Bank). A key question will be, "Which risks should FDA bear, and which should be borne by the PIOs?" Sentinel System risks are partly commercial and partly political. Commercial risks include uncertain demand for the new infrastructure services, construction delays and cost overruns, unexpected operating and maintenance expenses, changes in availability and cost of inputs and outputs, and contractor insolvency.[345] Political risks arise when governmental policies interfere with private investors' plans.[346] Political risks could arise if FDA failed to provide clear, stable rules and policies on which PIOs can depend; if FDA reneged on its commitments to PIOs; if FDA neglected privacy issues, risking a public backlash that could shut the system down or severely limit its use; or if key laws and regulations such as the HIPAA Privacy Rule changed in ways that undercut investors' original business assumptions.

A basic rule of infrastructure financing is that commercial risks are best borne by private investors.[347] Governments should not use their limited funds to absolve private investors of commercial risk.[348] For example, a major commercial risk is the uncertain market for LPHD. Sentinel System LPHD is a new product and nobody really knows how many users actually would want to purchase it if it were available. A key political risk is that PIOs may locate willing buyers ready to purchase LPHD, only to find that FDA construes its privacy policy in a way that prevents the sale from going forward. It is appropriate for FDA to deploy its funds to protect PIOs against the latter risk, but not the former one. Using FDA's available funds to compensate investors for risks associated with a vigorous privacy protection policy is a worthy expenditure of public funds. Using FDA's funds to protect PIOs from their own erroneous market projections is not.

Many of the political risks facing Sentinel System investors are within FDA's control. FDA can reduce political risks by enunciating clear privacy policies at the outset, so investors can accurately estimate which sales they can and cannot make. FDA should not waste the public's funds guaranteeing political risks that could have been eliminated by fixing gaps and uncertainties in FDA's own privacy policy.[349]

345 Klingebiel & Ruster, *supra* note 53, at 1 n.1.

346 *See id.*

347 *See, e.g.*, Mateen Thobani, *Private Infrastructure, Public Risk*, FIN. & DEV., Mar. 1999, at 50, 53, *available at* http://www.imf.org/external/pubs/ft/fandd/1999/03/pdf/thobani.pdf ("Whether the potential benefits of private provision of infrastructure are fully realized depends on how governments allocate the risks.").

348 *See id.*

349 *See* Klingbiel & Ruster, *supra* note 53, at 4.

FDA should focus its funds to address the residual risks that will remain even after policy has been made as clear as it possibly can be. Assume FDA adopts a policy that allows ancillary data sales for certain categories of research that meet specified criteria. The residual risks are that FDA's policy might change, or that FDA might construe its existing policy in a novel way that rejects data uses that investors believed would be permissible. FDA appropriately could provide risk guarantees to protect investors from these latter, residual risks. However, it should not waste public funds insuring investors from risks that could have been inferred from the agency's clearly stated policy. Clearly-stated rules satisfy the public's need for transparency. They also reduce the uncertainties investors face and will reduce FDA's costs in attracting private capital. A clear privacy policy, backstopped by appropriate risk guarantees, is key to getting the system financed without jettisoning the protection of medical privacy.

CONCLUSION

In 1969, Richard Posner observed that industries providing essential infrastructure have always been, at the time their construction began, at the frontiers of technological progress.[350] In authorizing development of the Sentinel System infrastructure, Congress, for the first time in seventy years, saw the need for a major new national infrastructure and appointed a federal agency to oversee its development. FDA is, in many respects, an accidental infrastructure regulator, thrust into a new role that is strikingly different from its longstanding product safety mandate. Fortunately, the challenges now facing the agency are not new ones. In the United States, infrastructure needs have "shifted from roads, sewers, and basic electrical grids to high-speed data communication networks, but the development of infrastructure continues to follow longstanding economic and political rules."[351] Few strands of American law are as well developed, or as respected internationally, as our long tradition of infrastructure regulation which has, in a wide variety of industry contexts, harnessed private capital to build new infrastructures to serve defined public interests while still protecting vulnerable classes. Congress has framed Sentinel System privacy as an infrastructure regulatory problem. Framing the problem this way opens the door to solutions that draw on this rich legal tradition. Decisions allowing use of Sentinel System data can enjoy legitimacy and public acceptability, if decisions are made within

350 *See* Posner, *supra* note 34, at 549.

351 Chen, *supra* note 33, at 1620.

a framework of appropriate institutional protections. The question now is what, precisely, those protections ought to be.