Engelberg Center for Health Care Reform at Brookings

FDA Sentinel Initiative Meeting Series

# ISSUE BRIEF

Legal Issues in Active Medical Product Surveillance March 2010

## PANEL 3
## Appropriate Human-Subject Protections for Research Use of Sentinel System Data

*Barbara J. Evans, PhD, JD, LLM*
*Associate Professor of Law*
*Co-director, Health Law & Policy Institute*
*University of Houston Law Center*

This brief explores a hypothetical: What if the Sentinel System were used in research? The Sentinel System when fully developed will be one of the first American examples of nationally scaled health information infrastructure. When embarking on any major infrastructure project, it is prudent to do a bit of planning for all the various ways the infrastructure might be used—including, in this case, the possibility that the Sentinel System eventually may support research as well as public health activities. In the Food and Drug Administration Amendments Act of 2007[1] (FDAAA), Congress called for creation of a postmarket risk identification and analysis system[2] targeted to include health data for 100 million persons by July 2012.[3] FDA is fulfilling this mandate by developing the Sentinel System. Legal scholars read FDAAA as authorizing a rather broad array of uses for the system, including studies to develop better methodologies of risk-benefit analysis and to explore advanced questions about the safety and effectiveness of drugs.[4,5,6] The list of potential uses spans activities that constitute "research" as this term is generally understood in discussions of research ethics and privacy.[7,8,9,10,11,12,13,14]

### What are the ethical considerations in research use of the Sentinel System?

The Sentinel System provides infrastructure that could support observational research. It does not involve interventional research that would pose physical risks to people whose data are used. The risks they face are in the nature of privacy risks and potential affronts to personal dignity such as having one's data used without one's knowledge or approval. It is important, however, to distinguish the question of research ethics from the question of complying with privacy law. The two are not necessarily the same. Privacy laws and regulations set minimal standards of protection that may or may not be all that is required for the ethical conduct of observational research.

Other ethical considerations include the potential consequences, if the Sentinel System were used in scientifically questionable ways and produced spurious or unconfirmed findings that sparked ill-founded changes in patient care. This could create risks for all members of the public including, possibly, the people whose data are in the Sentinel System. Decisions about which queries to run on the Sentinel System are laden with ethical issues as are decisions about when—and how—to communicate study results. *These* decisions—and not just decisions about whether to let data be used—may need to come under the umbrella of ethical oversight.[15] FDAAA calls for a public process for determining which queries warrant access to Sentinel data.[16] The Secretary of Health and Human Services (HHS) is to seek recommendations from the Drug Safety and Risk Management Advisory Committee, or its successor, and other advisory committees as appropriate.[17]

The advent of large-scale pharmacoepidemiological networks—whether one is referring to Sentinel or to similar systems now being developed in Canada,[18] the European Union,[19,20,21] and Japan[22]—will confront bioethicists with novel challenges in applying familiar ethical frameworks. For example:

- It may cease to be a safe assumption that ethics committees, when reviewing observational study proposals, can dismiss the potential for physical risks to the research subjects and focus strictly on privacy concerns. Pharmacoepidemiological networks have a long-term potential to support close-to-real-time learning based on outcomes observed in clinical care. This trend has the potential to compress the cycle in which "clinical care" feeds "outcomes research" which feeds back into "clinical care"—perhaps compressing it to a point where the entire cycle unfolds within the time span of an individual patient's course of treatment. As this occurs, hallowed 20th-century categories (treatment vs. research; public health vs. research; public health vs. individual healthcare, generalizable vs. patient- or community-specific knowledge) will grow blurred—that is, blurrier than they already are.[23] In this not-so-distant future, data network policies—such as policies defining permissible data uses or policies on return of information to patients and physicians—have the potential to confer direct medical benefits or risks on observational study participants. Examples of these risks are that insurers may embrace Sentinel findings as grounds to cut off insurance coverage of drugs people in the system now are taking, or doctors may alter their prescribing patterns if they fear Sentinel data will be discoverable in tort lawsuits.
- Centralized ethical review of research in large data networks may require fresh thinking. The Office for Human Research Protections (OHRP) allows joint Institutional Review Board (IRB) review of cooperative research[24] but has not withdrawn earlier OPRR guidance calling for review by an IRB familiar with the local research context.[25] It is debatable what "local context" means in the setting of nationally scaled health data infrastructures that include disparate data environments (e.g., providers vs. insurers) and span many states with varying privacy requirements.[26]
- Is there a need for special protections for certain vulnerable populations and, if so, how can these protections be administered? Special protections for pediatric research subjects may be difficult to administer to the extent children's data are mixed in with other data in the source databases (e.g., pharmacy purchase records). When doing research in large data networks, are the "vulnerable" populations perhaps different from those that have been viewed as vulnerable in traditional research settings? Are some people "vulnerable" by reason of being more susceptible to re-identification than other people are? Who are these people: those whose genetic information previously has been recorded in forensic databases; those who have dealt with many different providers and insurers? The vulnerable: who are they? That is the question.

Advanced questions like these may require attention in coming years, but this brief focuses on the more basic problem of managing privacy and dignitary risks of research that uses Sentinel data.

**What protections will apply to Sentinel System research?**

FDA already has taken an important step to manage Sentinel System privacy risks. The system as currently planned will employ a distributed network architecture.[27,28] This means that data will remain in their current locations such as academic medical centers, healthcare systems, and medical insurance companies. Identifiable health information will not be transferred beyond the existing privacy firewall of the data environment in which it presently resides.* Studies will be performed by submitting queries to

* To achieve Congress's public health objectives it may be necessary, at some stage, to link individuals' records across the various data environments that participate in Sentinel. For example, monitoring the long-term risks of drugs will require linking people's data across multiple insurance databases so that outcomes can be followed as people change insurers. Data linkage

the respective data environments, each of which will prepare a de-identified, aggregate response for compilation and reporting to the query initiator. This distributed model helps allay ethical and privacy concerns.[29,30] In the early years of operation, only FDA will submit queries and all queries will be for active medical product safety surveillance, a public health activity. In the future, this same distributed model would lend itself to answering research queries as well as public health queries. The question is what human-subject protections would apply to such research.

- In 1981, FDA promulgated its own regulations to protect human subjects.[31] These have been harmonized with the Common Rule[32] but differ in important respects. FDA's human-subject protections were designed for interventional research. They 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."[33] People whose data are in the Sentinel System do not fit this definition, so IRB review and informed consent would not be required under FDA's regulations.
- A diverse group of healthcare data environments will participate in Sentinel. Some may already be implementing the Common Rule with respect to all research at their sites; others may not currently be subject to the Common Rule. FDAAA calls for all participating data environments to follow the HIPAA Privacy Rule, even if they are not already HIPAA-covered entities.[34] However, there is no similar requirement for them to implement the Common Rule.

Whether the Common Rule applies in a given context, such as the Sentinel System, depends on specific facts of the proposed research and how it is funded. There are at least four legal pathways[35] through which Sentinel data might be used in research:

- FDA could submit a research query on its own behalf, funding the research itself.
- FDA could engage external investigators to perform FDA-funded research with Sentinel data. FDAAA lets FDA contract with outside entities, such as academic and commercial researchers, to assist with the analysis and use of postmarket data.[36] Through this mechanism, an external investigator could become FDA's study partner and submit a research query to the Sentinel System.
- FDA could use this same mechanism to contract with an external study partner that is conducting non-FDA-funded research (for example, research funded by a private sponsor that is not subject to the Common Rule).
- Even without FDA involvement, there is a possibility that IRBs and Privacy Boards of the participating data environments could use their existing legal authorities (for example, under the waiver provisions of the HIPAA Privacy Rule) to grant outside parties access to Sentinel data.

When FDA funds research, as in these first two scenarios, the Common Rule seemingly applies: FDA is part of HHS, which implements the Common Rule for all research that it funds. In the last two scenarios, however, it is not so obvious that the Common Rule would apply. Perhaps foreseeing this possibility, FDAAA calls for the Secretary of HHS to convene a committee of experts "to make recommendations on development of tools and methods for the ethical and scientific uses for, and communication of, postmarketing data."[37] Congress has left it in the Secretary's discretion to decide the appropriate framework of ethical protections for Sentinel System research.

---

implies sharing at least some identifying information outside the privacy firewalls of individual data environments. Data linkage, if required, will need to be subject to procedures that afford strong, accountable privacy and data security protections.

**Would the Common Rule require informed consent for Sentinel System research?**

The odds that a privately insured American will have at least some health-related data in Sentinel by 2012 have been estimated at 45%, with slightly lower odds of inclusion (in the 30-40% range) for Medicare beneficiaries and participants in military health programs.[38] Many members of the public remain uncomfortable with any nonconsensual use of their data.[39] One possibility being discussed is to place the Sentinel System under the Common Rule.[40] FDA could do this by promulgating new regulations clarifying that *all* research uses of Sentinel data will be subject to the Common Rule. These regulations would not necessarily have to supplant FDA's existing human subject protections for participants in clinical trials. FDA could leave its existing framework in place and simply embrace the Common Rule in the specific setting of its Sentinel System. Even if the Common Rule applied, however, it does not imply that people whose data are in the Sentinel System would have any control over research uses of their data. The Common Rule, like the HIPAA Privacy Rule, affords multiple pathways for nonconsensual use of data. These include:

- Definitional pathways in which an IRB or Privacy Board makes a determination that the proposed data use is something other than regulated "research" (by reason of being public health practice[41] or exempt research[42] under the Common Rule or healthcare operations[43] under HIPAA or eligible for one of the defined exceptions[44] to HIPAA's privacy authorization requirements).
- The waiver pathway[45] in which IRBs and Privacy Boards approve nonconsensual uses of data after determining that several broadly stated criteria have been met.
- De-identification, coding, and structural pathways which require de-identification or coding of data,[46,47] possibly in combination with segregation of functions (for example, by erecting a firewall between data collection and data analysis) or the use of trusted intermediaries to perform sensitive functions such as code-key management.[48]
- Contractual pathways which include regulator-defined situations in which contracts are a determinative factor in whether a nonconsensual use will be allowed (for example, OHRP guidance allowing nonconsensual release of coded data subject to contractual arrangements to protect the code key;[49] the HIPAA Privacy Rule's verification standards that let private-sector entities receive data on behalf of a public health agency with which they have a contractual relationship;[50] and HIPAA provisions allowing disclosure of limited data sets to researchers subject to a data use agreement[51]).

These pathways require IRBs and Privacy Boards to make highly discretionary determinations—such as whether privacy risks are "minimal" or whether coding procedures are adequate—when deciding whether to approve an unconsented data use. These IRB determinations implicitly have the effect of setting privacy policies for the data environment or network to which they apply.

**Appropriate human-subject protections for research with Sentinel System data**

The point of asking whether the Common Rule applies to the Sentinel System is not to suggest that a *lower* standard of human-subject protections should apply. Rather, the Sentinel System offers an opportunity to implement protections *superior to* those of the Common Rule. The Common Rule was designed in the early dawn of the information age. It was intended primarily for oversight of interventional research. In subsequent years, it has been pressed into service to cover emerging areas of research, including a vast expansion of research with human biological materials (tissue specimens)[52,53] and the post-1980 flowering of observational research[54,55] in "an era of large volumes of data on platforms conducive to analyses."[56] Within the legal community, a critique of these latter uses has emerged.[57,58,59]

This critique is as follows: The Common Rule was never designed to support coercive decisionmaking by IRBs, yet IRBs are put in the position of making coercive decisions when they oversee research in large health data networks. In their oversight of clinical trials, IRBs rarely are required to make a coercive decision. For example, they approve informed consent documents that prospective trial participants are free not to sign if they do not like the terms. Only in rare contexts—such as emergency research—do IRBs waive consent to a clinical trial. Data networks and tissue banks present a starkly different context. Protecting the people whose data and tissues are used in research involves decisions by many different private decisionmaking bodies (such as network administrators, boards and steering committees of network organizations, Privacy Boards, and IRBs):

- Decisions whether a data environment (or specimen repository) should or should not participate in a larger health information network, and on what terms
- Decisions about data security, privacy, and other standards for the network
- Decisions about permissible uses of data in the network and the conditions of such uses (for example, user qualifications, terms of data use agreements, etc.)
- Decisions by IRBs/Privacy Boards to let data and tissues be used under the various pathways for nonconsensual use (see above).

All of these decisions are inherently coercive—at least in a legal sense—insofar as they enable nonconsensual use of people's data or tissues.[60] People whose data are in administrative and clinical databases are captive and potentially vulnerable; they have few viable exit options if they do not like the network's ethical, privacy, or data security arrangements.[61] Most Americans have little choice over the insurers or, in many cases, even the providers and pharmacists with which they must do business.

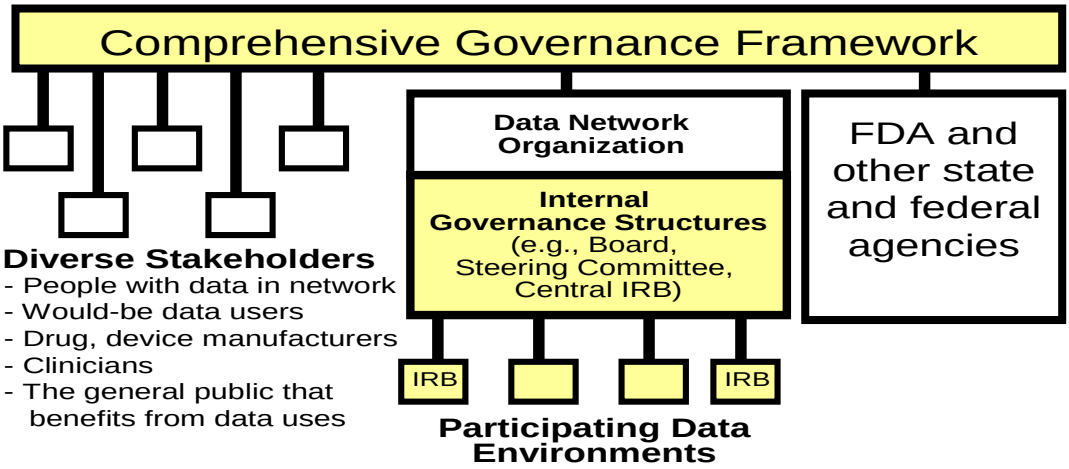
According to the legal critique, the Common Rule and HIPAA Privacy Rule are procedurally "underpowered" for the coercive decisions IRBs and Privacy Boards are called upon to make when overseeing research in a large health data network.[62,63] Moreover, these regulations fail to address the critical roles that other private decisionmakers may play in human-subject protections,[64] leaving important aspects of human-subject protection without any ethical oversight. IRBs and Privacy Boards are not subject even to the most rudimentary norms of procedural fairness, such as the Administrative Procedure Act's[65] requirements for fully independent decisionmakers; reasoned, evidence-based decisionmaking subject to clear, transparent standards; due process rights for affected parties; reviewable records and rights of appeal. Coercive decisionmaking without such norms is legally and ethically problematic. The role of IRBs in approving nonconsensual data use triggers concerns under various analytical frameworks[66,67,68,69] that are applied, in other contexts, to assess the propriety of coercive decisionmaking by private bodies. This situation invites problems of legitimacy and public trust and, possibly, future legal challenges to IRB decisions to approve nonconsensual use of data held in large health data networks.[70] Nationally scaled health information infrastructures—including Sentinel—raise issues that may not be adequately addressed even through rigorous application of regulations such as the Common Rule and HIPAA Privacy Rule. Something better will be needed to protect people whose data are held in these infrastructures.

**Protecting human subjects within the framework of Sentinel System governance**

Answering this challenge will require a framework of controls—known as a governance framework—to ensure that all Sentinel System decisionmakers carry out their responsibilities in a manner that upholds not only ethical principles, but public-regarding norms of due process, transparency, accountability, and decisionmaking that is unbiased, inclusive, and nondiscriminatory. The challenge of designing an appropriate governance framework is not unique to Sentinel; this is a pressing issue for large health data networks more generally. Figure 1[71] shows the complexity of data network governance. Large networks

link data together across diverse data environments (insurers, pharmacy benefit managers, public health agencies, academic medical centers, healthcare providers and other entities that hold data in administrative, clinical, or research databases). Some may have local IRBs or Privacy Boards; others may not. Some network governance proposals call for participating data environments to form a special-purpose legal entity (such as a 501(c)(3) nonprofit corporation) to administer network operations.[72] This network organization would have internal governance structures such as a board or steering committee[73] and might arrange central IRB review[74] of network-wide decisions about data use and privacy policies.

Figure 1. Multiple Levels of Data Network Governance




There is a risk that these lower two layers of governance—local IRBs and central structures of the network organization—may fail to ensure a voice for diverse other stakeholders affected by decisions about data access and network privacy policies. To address this risk, a top layer of governance (shown as "comprehensive governance") may be needed. Over the past 40 years, multilayered governance arrangements of this sort have been widely deployed in many different sectors and decisionmaking contexts as governments in North America and Europe turned to greater use of public-private partnerships to implement major infrastructure projects and social welfare programs.[75] Innovative tools of governance have been developed for these contexts.

*Top-level, comprehensive governance need not imply forming new review bodies and adding cumbersome layers of additional review.* It might, for example, employ tools such as regulatory guidance, procedural guidelines, or decision support structures to help existing decisionmaking bodies, such as local IRBs, do their jobs in a way that enhances public trust. Modern governance structures offer a wide range of attractive options between the two extremes of top-down, command-and-control governmental regulation and pure self-governance (e.g., letting consent waivers be approved by local IRBs staffed primarily with insiders of the participating data environments).[76] These intermediate options might include appointing truly independent IRBs, selected through a public process that considers the views of all stakeholders, to oversee critical aspects of network operations. These options also might include the use of private standard-setting organizations, accreditation bodies, or independent auditors to oversee various aspects of privacy policy development and enforcement. Modern governance frameworks often rely on complex packages of contracts to define duties and rights of the various affected stakeholders. These contracts might include, for example, agreements defining the privacy and data-access policies to be followed by the participating data environments, or data use agreements defining the responsibilities of data users. For example, it would be possible to seek contractual restrictions that prevent participating data environments from using Common Rule/HIPAA waivers to grant third-party access to the Sentinel System, in favor of routing all such decisions through an alternative decisionmaking structure that provides superior due process protections for all network stakeholders—including persons whose data are

in the network, would-be data users, and the public that stands to benefit from the research.[77] In this way, contracts can be used to address gaps in protection that may exist under existing regulations such as HIPAA and the Common Rule.

To be clear: the governance framework would not *supplant* existing regulations but *augment* them to address issues that are specific to the Sentinel System. The task of affording strong, accountable human-subject protections will require careful design of a governance framework, taking full advantage of modern tools of governance that have been developed and used successfully in many other contexts in the four decades since the Common Rule was designed.

## Conclusion

If research is to be conducted with Sentinel System data, developing appropriate human-subject protections would require a major effort that needs to start now. Large health data networks like the Sentinel System are poised to play a crucial role in the learning healthcare system of the 21st century,[78,79] but they present ethical issues that are not adequately addressed by 20th-century human-subject protection frameworks. Addressing these issues will require an intense policy debate of the same scale as the national debate that surrounded the expansion of clinical trial activity during the years 1962 – 1980. At that time, there was a fundamental rethinking of appropriate ethical and regulatory frameworks for clinical-trial-based research. That same intensity of effort is needed now with respect to the greater use of observational methodologies as a source of medical evidence, and with respect to the large health information resources on which these methodologies depend. Sentinel, as the first American example of nationally scaled health information infrastructure, is poised to play a precedent-setting role.

---

1 Pub. L. No. 110-85, 121 Stat. 823 (2007) (codified as amended in scattered sections of 21 U.S.C.).
2 FDAAA § 905(a), 21 U.S.C. § 355(k)(3)(C).
3 21 U.S.C. § 355(k)(3)(B)(ii).
4 21 U.S.C. §§ 355(k)(4)(A), (k)(3)(C)(i).
5 Barbara J. Evans, *Congress' New Infrastructural Model of Medical Privacy*, 84 NOTRE DAME L. REV. 585, 589, 601-02 (2009), http://www3.nd.edu/~ndlrev/archive_public/84ndlr2/Evans.pdf.
6 *See* U.S. FOOD & DRUG ADMIN., U.S. DEP'T OF HEALTH & HUMAN SERVS., THE SENTINEL INITIATIVE 16 (2008) (showing a research component as part of the system's organizational structure).
7 JAMES G. HODGE, JR., & LAWRENCE O. GOSTIN, COUNCIL OF STATE & TERRITORIAL EPIDEMIOLOGISTS, PUBLIC HEALTH PRACTICE VS. RESEARCH 7 (2004), http://www.cste.org/pdffiles/newpdffiles/CSTEPHResRptHodgeFinal.5.24.04.pdf.
8 James G. Hodge, *An Enhanced Approach to Distinguishing Public Health Practice and Human Subjects Research*, 33 J.L. MED. & ETHICS 125, 127 (2005).
9 NAT'L INST. OF HEALTH, U.S. DEP'T OF HEALTH & HUMAN SERVS., PROTECTING PERSONAL HEALTH INFORMATION IN RESEARCH (2004), http://privacyruleandresearch.nih.gov/pdf/HIPAA_Booklet_4-14-2003.pdf.
10 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, http://www.cdc.gov/mmwr/pdf/other/m2e4111.pdf.
11 Ctrs. for Disease Control & Prevention, U.S. Dep't of Health and Human Servs., Guidelines for Defining Public Health Research and Non-research (1999), http://www.cdc.gov/od/science/regs/hrpp/researchdefinition.htm.
12 Office for Prot. from Research Risks, Office for Human 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.
13 Paul J. Amoroso & John P. Middaugh, *Research vs. Public Health Practice: When Does a Study Require IRB Review?*, 36 PREVENTIVE MED. 250 (2003).
14 Dixie E. Snider, Jr. & Donna F. Stroup, *Defining Research When it Comes to Public Health*, 112 PUB. HEALTH REP. 29 (1997).
15 Barbara J. Evans, *Seven Pillars of a New Evidentiary Paradigm: The Food, Drug, and Cosmetic Act Enters the Genomic Era*, 85 NOTRE DAME L. REV. 419, 489 – 91, 508 – 515 (2010).
16 21 U.S.C. § 355(k)(4)(C).
17 *Id*.
18 Canada Institutes of Health Research (CIHR), In Brief: The Drug Safety and Effectiveness Network (DSEN), http://www.cihr-irsc.gc.ca/e/39389.html. *See also*, HEALTH CANADA, MEDICINES THAT WORK FOR CANADIANS: BUSINESS PLAN FOR A DRUG EFFECTIVENESS AND SAFETY NETWORK (2007), http://www.hc-sc.gc.ca/hcs-sss/pubs/pharma/2007-med-work_eff/index-eng.php.

[19] European Network of Centres for Pharmacoepidemiology and Pharmacovigilance (ENCePP), http://encepp.eu; EUROPEAN RISK MANAGEMENT STRATEGY, TWO-YEAR WORK PROGRAMME (2008-09), http://www.emea.europa.eu/pdfs/human/phv/28008907en.pdf.

[20] *See* Welcome to the EU-ADR Website, http://www.alert-project.org/.

[21] *See* EMEA-coordinated PROTECT project has been accepted for funding by the Innovative Medicines Initiative Joint Undertaking, PHARMANEWS (April 30, 2009), http://www.pharmanews.eu/emea/197-emea-coordinated-protect-project-has-been-accepted-for-funding-by-the-innovative-medicines-initiative-joint-undertaking.

[22] Kaoru Misawa, Director, Office of Safety, Pharmaceuticals and Medical Devices Agency (PMDA), *Sentinel Initiative in Japan: Utilization of Electronic Health Information in Pharmacovigilance*, 9th Kitasato University-Harvard School of Public Health Symposium (11-12 September, 2009).

[23] *See supra* notes 7-14.

[24] 45 C.F.R. § 46.114.

[25] OPRR, IRB Knowledge of Local Research Context (Aug. 27, 1998, updated July 21, 2000), http://www.hhs.gov/ohrp/humansubjects/guidance/local.htm.

[26] Jeffrey C. Torres, State Law Ambiguities Confronting Health Database Holders, http://www.brookings.edu/~/media/Files/events/2010/0111_sentinel_workshop/07_Torres.pdf.

[27] FDA, The Sentinel Initiative: Questions and Answers, http://www.fda.gov/oc/initiatives/advance/sentinel/qanda.html, at question 7.

[28] JANET M. MARCHIBRODA, EHEALTH INITIATIVE FOUND., DEVELOPING A GOVERNANCE AND OPERATIONS STRUCTURE FOR THE SENTINEL INITIATIVE 4, 8, 10, 33 (2009), *available at* http://www.regulations.gov/search/Regs/home.html#documentDetail?R=09000064809a82f0 (discussing the proposed decentralized model of Sentinel architecture).

[29] Richard Platt et al., *The New Sentinel Network—Improving the Evidence of Medical-Product Safety*, 361 NEW ENG. J. MED. 645-47 (2009).

[30] Carol C. Diamond, Farzad Mostashari & Clay Shirky, *Collecting and Sharing Data For Population Health: A New Paradigm*, 28 HEALTH AFFAIRS 454, 460 (2009).

[31] 21 C.F.R. pts. 50, 56.

[32] 45 C.F.R. pt. 46, subpt. A.

[33] 21 C.F.R. § 50.3(g) (informed consent regulation); *id.* § 56.102(e) (IRB review).

[34] 21 USC§ 355(k)(3)(C)(i)(I).

[35] *See* Barbara J. Evans, *Authority of the Food and Drug Administration to Require Data Access and Control Use Rights in the Sentinel Data Network*, 65 FOOD & DRUG L.J. 67, 97-100 (2010) (discussing legal pathways for granting Sentinel System use rights).

[36] 21 USC § 355(k)(4)(D)(i)(I)—(V).

[37] 21 USC § 355(k)(3)(B)(iii).

[38] Evans, *supra* note 35, at 72 n.39.

[39] COMMITTEE ON HEALTH RESEARCH AND THE PRIVACY OF HEALTH INFORMATION, INSTITUTE OF MEDICINE, BEYOND THE HIPAA PRIVACY RULE: ENHANCING PRIVACY, IMPROVING HEALTH THROUGH RESEARCH (Sharyl Nass, Laura A. Levit, and Lawrence O. Gostin, eds., 2009), at 66, available at http://www.nap.edu/catalog/12458.html. [hereinafter, "IOM, PRIVACY REPORT"].

[40] *See* KRISTEN ROSATI, AN ANALYSIS OF LEGAL ISSUES RELATED TO STRUCTURING FDA SENTINEL INITIATIVE ACTIVITIES 86–87 (2009), http://www.regulations.gov/search/Regs/contentStreamer?objectId=090000648098bad2&disposition=attachment&contentType=pdf, at 70-77 (discussing implications of Common Rule regulation of the Sentinel System); *see also* Evans, *supra* note 5, at 626-31 (same).

[41] *See supra* notes 7-14.

[42] 45 C.F.R. § 46.101(b).

[43] 45 C.F.R. § 164.501 (defining healthcare operations).

[44] 45 C.F.R. § 164.512.

[45] 45 C.F.R. § 164.512(i) [HIPAA]; *id.* § 46.116(d) [Common Rule].

[46] *See* Office for Human Res. Protections, U.S. Dep't of Health & Human Servs., Guidance on Research Involving Coded Private Information or Biological Specimens 5-6 (Oct.16, 2008) (replacing earlier guidance dated Aug. 10, 2004), http://www.hhs.gov/ohrp/humansubjects/guidance/cdebiol.pdf [hereinafter OHRP 2008 Guidance].

[47] *See* 45 C.F.R. § 164.514(b)(2)(i)(R), (c) (allowing HIPAA de-identified data, which can be disclosed without individual authorization, to be supplied with a code that would allow re-identification).

[48] Barbara J. Evans, *Ethical and Privacy Issues in Pharmacogenomic Research* , *in* PHARMACOGENOMICS: APPLICATIONS TO PATIENT CARE 2ED. 313, 332-34 (Howard L. McLeod et al. eds., 2009).

[49] OHRP 2008 Guidance, *supra* note 46.

[50] 45 C.F.R. § 164.514(h)(2)(i)(C).

[51] 45 C.F.R. § 164.514(c).

[52] Rina Hakimian & David Korn, *Ownership and Use of Tissue Specimens for Research*, 292 JAMA 2500 (2004).

[53] 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, 122 (2006).

[54] Agency for Healthcare Research & Quality, Outcomes Research Fact Sheet (2000) [hereinafter AHRQ, Fact Sheet], http://www.ahrq.gov/clinic/outfact.htm.

[55] Fred D. Brenneman et al., *Outcomes Research in Surgery*, 23 WORLD J. SURGERY 1220 (1999).

[56] Robert M. Califf, *Evolving Methods: Alternatives to Large Randomized Control Trials*, *in* ROUNDTABLE ON EVIDENCE-BASED MED., INST. OF MED., THE LEARNING HEALTHCARE SYSTEM: WORKSHOP SUMMARY 95 (LeighAnne Olsen et al. eds., 2007) [hereinafter IOM, LEARNING HEALTHCARE], *available at* http://books.nap.edu/openbook.php?record_id=11903.

[57] Carl H. Coleman, *Rationalizing Risk Assessment in Human Subject Research*, 46 ARIZ. L. REV. 1, 13–17 (2004).

[58] Evans, *supra* note 5, at 622-25.

[59] Barbara J. Evans, *Inconsistent Regulatory Protection Under the U.S. Common Rule*, 13 CAMBRIDGE Q. HEALTHCARE ETHICS 366, 372 (2004).

[60] Evans, *supra* note 5, at 631.

[61] Evans, *supra* note 35, at 102-03, 110.

[62] Coleman, *supra* note 57.

[63] Evans, *supra* note 35, at 103-06.

[64] Evans, *supra* note 5, at 640-53.

[65] *See* 5 U.S.C.A. §§ 551–59, 701–06.

[66] *See* Jody Freeman, *Extending Public Law Norms Through Privatization*, 116 HARV. L. REV. 1285, 1291, 1342-51 (2003) [hereinafter, "Freeman, *Extending Public Law Norms*"] (identifying factors for assessing whether a given private delegation is problematic in ways that create a need to place the private decisionmaker under special controls to protect the public interest).

[67] *See* Texas Boll Weevil Eradication Found., Inc. v. Lewellen, 952 S.W.2d 454 (Tex. 1997) (enunciating eight factors for assessing whether private decisionmaking is problematic, in the context of a state constitutional case involving coercive decisionmaking by a private board).

[68] *See* Christopher K. Leman, *Direct Government, in* THE TOOLS OF GOVERNMENT: A GUIDE TO THE NEW GOVERNANCE (Lester M. Salamon, ed., 2002), at 61-62 (discussing factors helpful in the closely related context of identifying inherently "governmental" functions that should not be delegated to private actors at all).

[69] *See* U.S. General Accounting Office, Government Contractors: Are Service Contractors Performing Inherently Governmental Functions? Report No GGD-92-11 (1991) and Exec. Office of the President, Office of Management and Budget, Circular No. A-76 (May 29, 2003 as revised), http://www.whitehouse.gov/omb/circulars/a076/a76_rev2003.pdf, at A-2 (enunciating criteria similar to those in Leman's discussion).

[70] Evans, *supra* note 35, at 110-11.

[71] Figure 1 is adapted from Barbara J. Evans, *Building Capacity Within Post-FDAAA Infrastructure*, presentation before Institute of Medicine Forum on Drug Discovery & Development (Sep. 2, 2009), *at* slide 8.

[72] *See* MARCHIBRODA, *supra* note 28, at 11-12.

[73] *Id*.

[74] ROSATI, *supra* note 40, at 76.

[75] For a useful summary of the large literature on governance of public-private collaborations, *see* CATHERINE M. DONNELLY, DELEGATION OF GOVERNMENTAL POWER TO PRIVATE PARTIES: A COMPARATIVE PERSPECTIVE (2007). *See also* DONALD F. KETTL, THE TRANSFORMATION OF GOVERNANCE: PUBLIC ADMINISTRATION FOR TWENTY-FIRST CENTURY AMERICA (2002); Lester M. Salamon, *The New Governance and the Tools of Public Action*, *in* THE TOOLS OF GOVERNMENT: A GUIDE TO THE NEW GOVERNANCE (Lester M. Salamon, ed., 2002); Harold I. Abramson, *A Fifth Branch of Government: The Private Regulators and Their Constitutionality*, 16 HASTINGS CONST. L.Q. 165 (1989); Kenneth Bamberger, *Regulation as Delegation: Private Firms, Decisionmaking, and Accountability in the Administrative State*, 56 DUKE L.J. 377 (2006); Jody Freeman, *The Private Role in Public Governance,* 75 N.Y.U. L. REV. 543 (2000); Jody Freeman, *Collaborative Governance in the Administrative State,* 45 U.C.L.A. L. REV. 1 (1997); Jody Freeman, *Private Parties, Public Functions and the New Administrative Law,* 52 ADMIN. L. REV. 813 (2000); Jody Freeman, *The Contracting State,* 28 FLA. ST. U. L. REV. 155 (2000); Freeman, *Extending Public Law Norms*, *supra* note 66; David M. Lawrence, *Private Exercise of Governmental Power*, 61 IND. L.J. 647, 684 (1986); Gillian E. Metzger, *Privatization as Delegation*, 103 COLUM. L. REV. 1367 (2003); Martha Minow, *Public and Private Partnerships: Accounting for the New Religion*, 116 HARV. L. REV. 1229 (2003); Edward Rubin, *The Myth of Accountability and the Anti-Administrative Impulse,* 103 MICH. L. REV. 2073 (2005); Paul R. Verkuil, *Public Law Limitations on Privatization of Government Functions,* 84 N.C. L. REV. 397 (2006).

[76] Evans, *supra* note 35, at 108-09.

[77] *Id*. at 105-06; Evans, *supra* note 5, at 624-25.

[78] IOM, LEARNING HEALTHCARE, *supra* note 56.

[79] Evans, *supra* note 15, at 479 – 85.