

5-1-2014

Biobanking as a Model for Balancing Patient and Research Interests

Hyosung Julie Shin

Follow this and additional works at: http://scholarship.shu.edu/student_scholarship

Recommended Citation

Shin, Hyosung Julie, "Biobanking as a Model for Balancing Patient and Research Interests" (2014). *Law School Student Scholarship*. Paper 571.

http://scholarship.shu.edu/student_scholarship/571

Biobanking as a Model for Balancing Patient and Research Interests

Hyosung (Julie) Shin

I. Introduction

The key to a property regime is considered to be to give control, and power, to the person holding the property right.¹ Traditionally, a paper version of patient health records had been regarded as property of the health care providers. Adopting an electronic health records (“EHR”) in recent years, however, stirred a discussion on ownership of data that are made available for easy transfer and access. Recent debates on data ownership in EHR involved the question of who owns the EHR data, and whether the public or private ownership of data would be more beneficial for the future. This article will discuss the current positions on the question and will focus on the tension between public and private use of the protected health record data especially in the context of the field of research. The article proposes the creation of an EHR database available for the record-based research purpose, based on the model of U.K. biobank project to ensure effective balancing between private interest in protecting individual privacy and public interest in promoting the beneficial use for the public. To that end, it will look to the cases of the U.K. and Icelandic biobank models as possible examples for the EHR database for the purpose of research use.

In Part II, this paper will outline what the current laws cover or do not cover on data ownership issue. In Part III, this paper will summarize the recent major debates on the issue of data ownership, and will try to reframe the question of data ownership in the context of health

¹ Lawrence Lessig, *Code and Other Laws of Cyberspace*, 160 (1999).

information exchange landscape. In Part IV, this article will look at the specific provisions in HIPAA related to use of EHR data for research purposes. In Part V, this paper will discuss the success and failure of the national biobanks in the U.K. and Iceland, and will propose what elements could be incorporated into the EHR database for the research purpose.

II. Current Laws: Relevant Provisions

Although EHRs represent a substantial improvement over fragmented, geographically dispersed, illegible, and uncoordinated paper records, they pose new dangers as well. Like all computerized records, networked EHRs are difficult to secure, and the information in EHRs is both particularly sensitive and particularly valuable for commercial purposes.² The existing federal statute, the Privacy rules under Health Insurance Portability and Accountability Act of 1996 (“HIPAA”)³, seem to fall short on addressing the particular problems that are raised by EHRs.

A major purpose of the Privacy Rule is to define and limit the circumstances in which an individual’s protected health information may be used or disclosed by covered entities. A covered entity may not use or disclose protected health information, except either: (1) as the Privacy Rule permits or requires; or (2) as the individual who is the subject of the information (or the individual’s personal representative) authorizes in writing.⁴ A covered entity must

² Jane Barone, *Property as Control: the Case of Information*, 18 MICH. TELECOMM. TECH. L. REV. 367, 367 (2012), available at <http://www.mttl.org/voleighteen/baron.pdf>

³ Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub. L. No. 104-191, 110 Stat. 1936 (codified as amended in scattered section of 18, 26, 29, 42 U.S.C.); see also HIPAA Security Rules, 45 C.F.R. §§ 164.302 - .318 (2011).

⁴ 45 C.F.R. §164.502(a).

disclose protected health information in only two situations: (1) to individuals (or their personal representatives) specifically when they request access to, or an accounting of disclosures of, their protected health information; and (2) to HHS when it is undertaking a compliance investigation or review or enforcement action.⁵

a. What Information Is Protected

The Privacy Rule protects all “individually identifiable health information “ held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral. The Privacy Rule calls this information “protected health information (PHI).”⁶ “Individually identifiable health information” is information, including demographic data, that relates to:

- The individual’s past, present or future physical or mental health or condition,
- The provision of health care to the individual, or
- The past, present, or future payment for the provision of health care to the individual,

and that identifies the individual or for which there is a reasonable basis to believe can be used to identify the individual.⁷ There are no restrictions on the use or disclosure of de-identified health information.⁸ De-identified health information neither identifies nor provides a reasonable basis to identify an individual.

⁵ 45 C.F.R. § 164.502(a)(2).

⁶ 45 C.F.R. § 160.103

⁷ 45 C.F.R. § 160.103.

⁸ 45 C.F.R. §§ 164.502(d)(2), 164.514(a) and (b).

b. Who Is Covered

Health plans that are individual and group plans that provide or pay the cost of medical care are covered entities.⁹ Health plans include health, dental, vision, and prescription drug insurers, health maintenance organizations (“HMOs”), Medicare, Medicaid, Medicare+Choice and Medicare supplement insurers, and long-term care insurers (excluding nursing home fixed-indemnity policies). Two types of government funded programs are not health plans: (1) those whose principal purpose is not providing or paying the cost of health care, such as the food stamps program; and (2) those programs whose principal activity is directly providing health care, such as a community health center, or the making of grants to fund the direct provision of health care.

Every health care provider, regardless of size, who electronically transmits health information in connection with certain transactions, is a covered entity. These transactions include claims, benefit eligibility inquiries, referral authorization requests, or other transactions for which HHS has established standards under the HIPAA Transaction Rule. The transmission must be in connection with a standard transaction..¹⁰

Health care clearinghouses are entities that process nonstandard information they receive from another entity into a standard (i.e., standard format or data consent), or vice versa.¹¹ In most instances, health care clearinghouses will receive individually identifiable health information only when they are providing these processing services to a health plan or health

⁹ 45 C.F.R. §§ 160.102, 160.103.

¹⁰ 45 C.F.R. §§ 160.102, 160.103. The transaction standards are established by the HIPAA Transaction Rule at 45 C.F.R. Part 162

¹¹ 45 C.F.R. § 160.103

care provider as a business associate. In such instances, only certain provisions of the Privacy Rule are applicable to the health care clearinghouse's uses and disclosures of protected health information.¹²

c. "Permitted Use" Provision.

A covered entity is permitted, but not required, to use and disclose protected health information, without an individual's authorization, for the following purposes or situations: (1) To the Individual (unless required for access or accounting of disclosures); (2) Treatment, Payment, and Health Care Operations; (3) Opportunity to Agree or Object; (4) incident to an otherwise permitted use and disclosure; (5) Public Interest and Benefit Activities; and (6) Limited Data Set for the purpose of research, public health or health care operations.¹³

The debates on the privacy of the EHR systems arise from the tension, which exists in the statutes, between the efforts to protect the privacy interests of the individuals and the efforts to maximize the benefits of use of EHRs for the public.

III. Debates on Ownership of the Electronic Health Record Data

Many scholars, such as Marc Rodwin, tried to solve the problem of dividing the responsibility of controlling among the players of the EHRs by looking at the current property law. Rodwin starts his proposition based on the assumptions that whoever owns patient data will determine whether its benefits can be tapped. Currently, the law does not clearly define property

¹² 45 C.F.R §§ 164.500(b).

¹³ 45 C.F.R. § 164.502(a)(1).

interest in patient data. In most states, the law treats patient medical records as physical property that physicians and hospitals own, and it allows patients and insurers access to records.¹⁴ Health law, privacy, and intellectual property scholars have all suggested that the river of information created by integrated, networked EHRs and other data systems must somehow be controlled,¹⁵ and many of these scholars have considered whether “property” might provide such control.¹⁶ These debates focusing on ownership of the EHR data had been polarized into roughly two opposite positions; pro-access v. pro-privacy.

a. Pro-Privacy

Although there are some fine differences, many pro-privacy scholars see the propertization of the EHR data as an effective way to solve the problem of balancing the need for privacy and access. They argue that the best way to induce patient and providers to share the individual data they create is to help them unlock the value of that data and share in the benefits derived from letting others use it.¹⁷ Mark Hall, in his article, notices that the medical privacy rights grow out of the special nature of the relationships between patients and clinicians¹⁸ and that it is difficult to anticipate and specify all the conditions needed to allow the free flow of medical information since this depends on who possesses and controls the information and on its variety of potential uses. Thus, he argues that building these rights and protections into the legal

¹⁴ Marc A. Rodwin. *Patient Data: Property, Privacy & the Public Interest*, 36 AM. J.L. & MED. 586, 587-588 (2010).

¹⁵ Jessica Litman, *Information Privacy/ Information Property*, 52 STAN. L. REV. 1283, 1286 (2000).

¹⁶ Mark A. Hall, *Property, Privacy, and the Pursuit of Interconnected Electronic Medical Records*, 95 IOWA L. REV. 631 (2010).

¹⁷ Web Memorandum from Edmund F. Haislmaier, Heritage Foundation, Health Care Information Technology: Getting the Policy Right (June 16, 2006), available at http://www.heritage.org/research/healthcare/upload/wm_1131.pdf at 3.

¹⁸ Sonia Suter, *Disentangling Privacy from Property: Toward a Deeper Understanding of Genetic Privacy*, 72 GEO. WASH. L. REV. 737, 773 (2004).

status of the information itself is an advantage.¹⁹ Mark A. Hall, for example, suggested that patients be allowed to license rights to medical information for purposes of stimulating market development of EHR. The fact that property law provides a strong legal basis for seeking injunctive remedies against infringements²⁰ is another appealing factor for propertization of the EHR data.

Although he does not explicitly advocates for the private propertization of the EHR data, Mark Rothstein strongly supports the individuals' power to control, which is comparable to the right to decide what is done to their bodies, over their health information generated by medical encounters, regardless of whether their information have been deidentified.²¹

b. Pro-Access

Scholars who advocate for the pro-access position argue that treating patient data as private property precludes forming comprehensive databases required for many of its most important public health and safety uses.²² They contend that there is no need for new incentives to compile patient data since the patient data are being generated as part of the physicians and medical facilities' work to provide medical care and to comply with health care regulations.²³ Marc Rodwin argues that not only that public ownership is more efficient, but also that without public ownership it will be very difficult and perhaps impossible to aggregate population-wide

¹⁹ Mark A. Hall, *Property, Privacy, and the Pursuit of Interconnected Electronic Medical Records*, 95 IOWA L. REV. 631 (2010).

²⁰ Pamela Samuelson, *Privacy as Intellectual Property*, 52 STAN. L. REV. 1125, 1149 (2000).

²¹ Mark A. Rothstein, *Is Deidentification Sufficient to Protect Health Privacy in Research?*, 10 AM. J. BIOETHICS 3, 8 (2010).

²² Marc A. Rodwin. *Patient Data: Property, Privacy & the Public Interest*, 36 AM. J.L. & MED. 586, 588 (2010).

²³ Rodwin, at 600.

patient data. Referring to the discussion in the field of biomedical research, he describes what happens when ownership of basic building blocks for innovations is divided among numerous parties. In one example of patenting of genetic sequences²⁴, it showed how companies' patenting gene sequences associated with diseases that are key to genetic testing research is impeding research on curing genetic diseases by forcing potential researchers to go through negotiation process for obtaining patents from individual patent holders. Scholars such as Rodwin contend that private ownership of patient data would probably preclude its most valuable uses by fracturing population data.²⁵

They also predict that the proptertization of the electronic health data will increase the cost to the users of the data since some provider or organizations may demand exorbitant prices to purchase or use data that they control.²⁶ In addition, unlike some pro-privacy scholar's argument, treating personal data as private property would not increase privacy protection since individuals lose their control over their personal health data when they transfer their property interest in data.²⁷

c. Criticism on the Property as a Framework for Resolving the Problem

Recently, these past debates of who owns the data were brought under criticism by many other scholars and practitioners in the field. Dan Orenstein, SVP and General Counsel of Athena Health, wrote, "the interest is the data should be the data itself and, and more important,

²⁴ Jordan Paradise, Lori B. Andrews & Timothy Holbrook, *Intellectual Property: Patents on Human Genes: An Analysis of Scope and Claims*, 307 *SCIENCE* 1566 (2005).

²⁵ Rodwin at 606.

²⁶ Rodwin at 607.

²⁷ Samuelson at 1135.

aggregated data across multiple records that provides meaningful insight about what care protocols work, enables caregivers to communicate better with patients, enables researchers to more expediently identify patients to participate in studies, and achieves better public health reporting and analysis, among other uses.”²⁸ Jane Baron casts a doubt on the property as a framework for discussing the control over the EHR data on more fundamental level, pointing out that:

Property is a contested concept, and debates over whether property is a useful legal frame in which to organize various participants’ interests in the information in EHRs only exposes the lack of agreement about what property is. She contends that it is hard to see how the problem of information control can be “fixed” by resort to a legal regime whose substance and scope are pervasively disputed.²⁹

Baron argues that in an increasingly interconnected world, we need to make difficult choices about how power and control should be allocated and most likely shared among a variety of parties. The concept of “property” alone cannot tell us how to make those choices, she says.³⁰ According to her, in the end, patients will have those powers – and only those powers – that are consistent with the needs of a workable health system such as system operability or the

²⁸ Dan Orenstein, Our Brave New World: EMR and the “Ownership” of Health Information, <http://www.athenahealth.com/blog/2012/04/17/our-brave-new-world-emr-and-the-%E2%80%9Cownership%E2%80%9D-of-health-information/> (last visited Oct. 9, 2012).

²⁹ Jane Baron, *Property as Control: the Case of Information*, 18 MICH. TELECOMM. TECH. L. REV. 367, 390 (2012).

³⁰ *Id.* at 410.

government's interest in public health. Whether or not those powers resemble the powers we associate with "ownership" of "property."³¹

Controlling information of all kinds requires hard choices. Individuals legitimately worry about what the world might come to know about them and how the world might come to know it. But individuals' concerns are but one part of a very large equation. With respect to EHRs, that equation includes considerations of health policy and public health. Individuals should be granted some power to control their personal information. But the concept of property alone cannot tell us how much, or what kind, of power.³²

IV. Permitted Use Without Consent for Public Interest and Benefit Activities

The Privacy Rule permits use and disclosure of protected health information, without an individual's authorization or permission for the following 12 national priority purposes³³:

- Required by Law
- Public Health Activities
- Victims of Abuse, Neglect or Domestic Violence
- Health Oversight Activities
- Judicial and Administrative Proceedings
- Law Enforcement Purposes

³¹ *Id.* at 412.

³² *Id.* at 418.

³³ 45 C.F.R. § 164.512.

- Decedents
- Cadaveric Organ, Eye, or Tissue Donation
- Research
- Serious Threat to health or Safety
- Essential Government Functions
- Workers' Compensation

However, realizing societal benefits from permitting disclosure without consents for above purposes does not automatically grant a controversy-free pass for disclosure of EHR data for the covered entities. Subordinating individual freedom to the common good because individuals profit from societal initiatives is consistent with the philosopher Jean-Jacques Rousseau's theory of social consent. Rousseau spoke of a social contract by which individuals willingly give up freedom and autonomy to enjoy the advantages of living in society.³⁴

Public policy already places the common good ahead of concerns about privacy and autonomy in establishing a large number of reporting requirements. Physicians are required by law to report to authorities cases of particular infectious diseases, including tuberculosis, sexually transmitted diseases, infection by bioterrorism agents, and new epidemic illnesses.³⁵ However, even with greater focus on the principle of promoting the public good, concerns about the privacy vulnerabilities of EHR data, when disclosed for those purposes, should be taken seriously. The answer to the question of how to balance individual privacy and the public

³⁴ Jean-Jacques Rousseau, *On the Social Contract*, 52-53 (Roger D. Masters ed., Judith R. Masters trans., St. Martin's Press 1978).

³⁵ John C. Moskop et al., *From Hippocrates to HIPAA: Privacy and Confidentiality in Emergency Medicine – Part I: Conceptual, Moral, and Legal Foundations*, 45 ANNALS EMERGENCY MED. 53, 57 (2005).

interests and benefits becomes especially murky when it comes to situations that are specified in the above listed “permitted use without consent” situations. The provisions exempting certain situations under HIPAA Privacy Rule are in some cases not effective and seem to need more specific guidance to provide for the covered entities and to warrant more uniform results.

a. Context 1: Law Enforcement Purposes

Due to the nature of the use of health data for a specific case, the disclosure of the protected health data to law enforcement purpose almost always involves identified health information, which demands more sensitivity in handling them. Under the current system, however, the question of whether the individual health information data should be released or not is being reviewed case-by-case basis often either by law enforcement authority and the healthcare providers, sometimes resulting unfair results for a patient about whom the health record was created.

In a 2010 case, *Turk v. Oiler*³⁶, a patient’s data was released by the health care provider without consent to a law enforcement official and the data was used against him in prosecuting him for unlawful possession of a weapon while being on recovery from drug abuse. The police officer happened to be a friend of the family member who had a grudge against the patient, and found a weapon in the plaintiff’s trunk when he conducted a routine search of the car after stopping him for minor violation of the traffic rule. In this case, the court found against the hospital for the plaintiff who argued his position based on state law patient-doctor confidentiality. But only a few years later, the same hospital lost its motion to quash the criminal subpoena

³⁶*Turk v. Oiler*, 732 F.Supp.2d 758 (N.D.Ohio, Aug. 11, 2010).

which was from a United States Attorney out of state. This time the court noted that federal law doesn't recognize the doctor-patient privilege and stated that the hospital should produce the patient records.³⁷

Although these cases are only a part of the examples where protected health data are disclosed for law enforcement purposes, it shows how confusing it can be to navigate among the current laws in the field. The current language of the HIPAA Privacy Rule can seem to allow broad discretion to the healthcare provider and law enforcement authority in deciding which in deciding which protected health data can be released. The usual privileges and perception of law enforcement authorities and their activities often create even more room for law enforcement authorities to exercise their judgment. In reality, the healthcare providers tend to cooperate in releasing protected health data under their care to law enforcement authority often without much questioning and applying specific compliance standards.³⁸ In the midst of confusion and lack of clear rule on which information is to be released under what circumstances, the patient health information remains vulnerable for unwanted disclosure without them knowing it often for their disadvantage. However, the detailed rules outlining the conditions that warrant the fair disclosure of protected health information of the individuals seem to be too complex and infeasible given the diversity of the various occasions that law enforcement authorities and healthcare providers face every day.

b. Context 2: Research

³⁷ *Report on Patient Privacy*, Vol. 12, No. 5, 7 (May 2012).

³⁸ *PHI and HIPAA Disclosures to Law Enforcement: a Roller-Coaster Rule*, Report on Patient Privacy, May 2012, AISHealth.com, http://aishealth.com/sites/all/files/marketplace_pdf_samples/samplerpp.pdf (last visited Oct. 15).

Another area where the tension between patient privacy and public benefits appears prominent is in the context of record-based research. In their article, Sharona Hoffman and Andrew Podgurski contend that when human beings are not subject to any physical or psychological testing in researched, and only their records are scrutinized, the value of the common good should prevail over individual interests.³⁹ The argument for use of protected health data for research purpose is more convincing than any other public benefits use purposes since the benefit of the research goes back to the patients whether indirectly or directly in a long run. However, an individual patient pause to answer to the immediate question of whether to release one's protected health data for research purpose or not.

The first reason for the pause is the concern for the privacy violation. A popular mechanism for addressing concerns about privacy in research context is to de-identify the patient health data. The HIPAA Privacy Rule details the requirements for de-identification and specifies the eighteen types of identifiers to be removed.⁴⁰ Compliance with these de-identification specifications eliminates a variety of obligations of covered entities under the Privacy Rule, including providing a notice of privacy practices, requiring an authorization for uses other than treatment, payment, and health care operations, and restricting use of the information beyond health care. Deidentified health records are outside the definition of "protected health information" under the HIPAA Privacy Rule and therefore are exempt from federal privacy protections.⁴¹ Mark A. Rothstein, in his article, contends that there should be added protection

³⁹ Sharona Hoffman & Andy Podgurski, *Balancing Privacy, Autonomy, and Scientific Needs in Electronic Health Records Research*, Case Research Paper Series in Legal Studies, Working Paper 2011-2012 (April, 2012) at 124.

⁴⁰ 45 C.F.R. § 164.514(b)(2)(i) (2010).

⁴¹ 45 C.F.R. § 164.514(a).

and rules in the regulatory system for providing more protection for deidentified information.⁴²

He equates the individual's health information, whether the data is identified or de-identified, to biological specimens generated by medical encounters which he views as an extension of the person's "body" itself.

Extending the protection over to the de-identified data, however, can bring an unfavorable impact of adding burdens on the research community; e.g., by increasing costs of securing additional individual consents and employing more complex technological steps of de-identifications sometimes risking the value of the records for research. The cost of additional measures to protect individual privacy in de-identified health records should be carefully balanced against the potential public benefits that can be realized without them.

The second concern is the difficulty controlling and tracking the use of the data upon release. As a norm, consent need not be sought for non-interventional research.⁴³ Ordinarily, biomedical research protocols require institutional review board (IRB) approval, and patients must authorize the release of identifiable information to researchers under the HIPAA Privacy Rule. However, the federal regulations that require IRB review and participant consent, known as the Common Rule,⁴⁴ cover only research on human subjects, not research using de-identified electronic health records. Even when there are doubts on the efficacy of the patient consents on giving actual notice to the patients over the extent of the use of the individual health data, as the current law stands, the consent seems to be the preferred form of having the individual patients

⁴² Mark A. Rothstein, *Is Deidentification Sufficient to Protect Health Privacy in Research?* 3 AM. J. BIOETHICS, 3 (2010).

⁴³ *Id.* at 128.

⁴⁴ See *Federal Policy for the Protection of Human Subjects ('Common Rule')*, U.S. Dep't Health & Hum. Servs., <http://hhs.gov/ohrp/humansubjects/commonrule/index.html> (last visited Oct. 1, 2012).

on notice of the use of their personal health data in research. According to the IOM, public opinion polls show that “a significant portion of the public would prefer to control all access to their medical records via informed consent.”⁴⁵ The study conducted through telephone interviews of 1,193 patients, focused on research using samples of genetic material.⁴⁶ It found that 81% of respondents wanted to know about research if their samples would be identifiable, and 72% wished to be informed if the samples would be anonymous.⁴⁷ Of those wanting to know about research involving either identifiable or anonymized samples, 57% would require that their permission be sought, and 43% would be content with notification alone.⁴⁸

Without a consent mechanism, the patients are left without any opportunities to accept or object the risks of dignitary harms.⁴⁹ As Mark Rothstein has argued, these harms include group stigmatization, inadvertently supporting medical developments that one finds morally objectionable, and enabling commercial enterprises to garner large profits in which data subjects do not share.⁵⁰ However, enforcing more strict and extensive informed consent mechanism may result in selection bias, and it can be costly and burdensome.

V. A New System for Solving the Problem?

Although the property framework on which their propositions are based on is currently considered out of fashion, the models to balance privacy and access to EHR data proposed by

⁴⁵ Comm. On Health Research & the Privacy of Health Info.: the HIPAA Privacy Rule, IOM, *Beyond the HIPAA Privacy Rule: Enhancing Privacy, Improving Health Through Research* 247 (Sharyl J. Nass et. al. eds., 2009) at 268.

⁴⁶ Sara Chandros Hull et al., *Patients' views on Identifiability of Samples and Informed Consent for Genetic Research*, 8 AM. J. BIOETHICS 62, 64 (2008).

⁴⁷ *Id.* at 65.

⁴⁸ *Id.* at 66.

⁴⁹ Hoffman and Podgurski at 107.

⁵⁰ Rothstein at 6-7.

many scholars on ownership issue still seem valuable for drawing a blueprint especially for permitted use without consent for public interest and benefit activities. Among various scholars who had written on the topic of EHR data ownership, two scholars envisioned the systems that might effectively balance the privacy of the patients and the public interests and benefits that can be realized from the use of EHR data.

Mark Hall, who is one of the strongest proponents for private propertization of the EHR data, proposes granting to patients property rights in their medical data sufficient to commercialize it, subject to the government's traditional authority over public health. In his model, patients are allowed to monetize their access and control rights by assigning them to a trusted and regulated intermediary who may then place those rights in a stream of commerce that determines their value and best use.⁵¹ His model limits the individual patients' rights in their medical data that can be linked to them personally only, not to data that is "anonymized/deidentified" data. This model would give patients more power to decide initially which data about themselves will be disclosed and which will not by giving them rights to negotiate license terms with the compiler or custodian.

Although Hall's model seems economically more efficient and seems to offer more incentives for both patients and data compilers to create electronic health databases, it would not be able to solve the problem of balancing between protecting privacy interest of the individual and the public benefits interests. Initially based on the patient consents, the health records included in the databases under Hall's model would be likely to be biased and not high enough

⁵¹ Hall at 631.

quality to be used by researchers and public health officials to draw scientifically valid conclusions.⁵²

Another prominent scholar in the field, Marc Rodwin, proposes that federal law require providers, medical facilities and insurers to report key patient data in anonymized and de-identified form to public authorities, which will create aggregate databases to promote public health, patient safety, and research. Public authorities, according to this model, should also make this data available for private entities to develop data derived services, subject to public oversight.⁵³ Rodwin's system will allow more power for the government to define the scope of data use for public interest and benefits. The biggest criticism for his model is the cost of constructing and operating a mega-database containing duplicate copies of all of the health data in the United States, in addition to heightened regulatory burden on the federal agencies such as the HHS, which would own the data under his proposal.⁵⁴

According to Evans, one solution for the cost of constructing and operating a mega-database might be found in the "distributed network architecture." In a distributed network, an individual's health information is not moved to a central database for storage and analysis; rather it continues to be stored at its original location. Under one design, parties wishing to use the data send queries to the data holders and records that meet the queries could be conveyed in identifiable form to network coordinating center (a "trusted intermediary) that would perform longitudinal linkage of data received from the various data holders. The trusted intermediary would use the linked data to compile lists of patients whose records meet the queries. These lists

⁵² Barbara Evans, *Much Ado About Data Ownership*, 25 HARV. J.L. & TECH. 69, 96 (2011).

⁵³ Rodwin at 589.

⁵⁴ Evans at 97-98.

then could be de-identified and conveyed to the investigator for use in the study.⁵⁵ Distributed architectures avoid the need to invest in duplicative storage capacity, thus saving the cost of operating a mega-database, because data reside with the original data holders and are not redundantly stored at a central location.⁵⁶ Also, federal regulation could require the general public, public entities or researchers to pay a usage fee to HHS for using such distributed network.⁵⁷

All the proposals discussed above are, however, on a rather theoretical level, and it would be in vain to discuss them without anchoring them to possible practical examples. In her article, Jane Baron has noted that much of the commodification debate concerning EHR data has played out in connection with the issue of self-ownership in a literal sense.⁵⁸ Much of the problems associated with EHR data use for public interests originate from the fact that the nature of the EHR data is personal and that the person to whom the specific data pertain fears for losing control over what is “part” of herself. Also bio-samples are more useful when it is in a collective form. In these respects, personal biological samples and genetic data share many of the same characteristics in common with EHR data when it comes to their use for the public interest, especially in research context.

VI. Biobanks as a Model

Considering the similarities both bio-sample and data and EHR data share in common in the research context, it would be helpful to look at the examples of biobanking as a model for the

⁵⁵ *Id.* at 100.

⁵⁶ *Id.* at 101.

⁵⁷ *See* similar proposals in the research context. Hoffman and Podgurski at 137.

⁵⁸ Baron at 401.

U.S. EHR infrastructure for balancing the patient and public interests in research context. Two of the most famous examples in biobanking models are those from Iceland and U.K.

a. Icelandic Health Sector Database (“HSD”)

The Icelandic national biobank, Health Sector Database (“HSD”), was started with a proposal by DeCODE Genetics, an American corporation with an Icelandic subsidiary. DeCode Genetics secured the license to create and operate the HSD in 2000 from the Icelandic government. The HSD was purported to link the health data with genetic and genealogical records of 300,000 Icelanders. The Health Sector Database Act, which authorized the creation of the HSD, authorized the transfer of all medical record data to the licensee for commercial development without the express consent individuals, thereby invoking a controversial rule of “presumed consent.” The patients are presumed to have consented to the transfer of their data unless they expressly opt-out within a set period of time. In the Icelandic Biobank model, the individual data collected is protected by independent parties, and the committees on ethics and data protection monitor matching of the data with the data from other preexisting database. The transfer of national health records to deCODE Genetics never took place, and the database was never built, due to the legal and ethical controversy over informed consent and the commodification of health information.⁵⁹ Although the Icelandic Biobank was widely regarded as an example of failed attempt to build a nation-wide biobank, it drew an international attention and provided a preliminary base for planning and building a biobank on a national level.

⁵⁹ David E. Winickoff, *Partnership in U.K. Biobank: a Third Way for Genomic Property?*, 35 J.L. Med. & ethics 440, 442.

One of the lessons to be learned from the Icelandic biobank project was that we need a careful preplanning for harmonizing different interests at stake that various parties have on the data to be included in the mega database to be built. In Icelandic biobank project, there were many of those interests that were not carefully screened out and channeled before actual transferring of the data started.⁶⁰

b. U.K. Biobank

The U.K. biobank took into consideration the failure of the Icelandic HSD example, and carefully laid out the plan for constructing their biobank. Paul Martin, a sociologist of science and technology at the University of Nottingham, submitted a written memorandum outline the particular challenges of the new commercial involvement in genetic worldwide, stating:

The recent experience of events in Iceland concerning the activities of deCODE genetics and the proposed creation of the Icelandic Health Sector Database highlight the need for transparency in decision making, widespread consultation and public debate, and strong oversight mechanisms. Such an approach to policy in the U.K. could help ensure that genetic databases are well supported, function in an ethical manner and provide genuine benefits.⁶¹

⁶⁰ See Gísli Pálsson, BIOBANKS GOVERNANCE IN COMPARATIVE PERSPECTIVES, 46-49 (Herbert Gottweis and Alan Petersen eds., 2008) (discussing various hindering oppositions from the Medical Associations, doctors in private practices, technology personnel and the public delaying the process of actual transferring of the data to the HSD.).

⁶¹ Winickoff at 442 (quoting P. Martin, Memorandum, *The Industrial Development of Human Genetic Databases*, October 2000, written evidence to Select Committee on Science and Technology).

As a major national health resource, and a registered charity in its own right, with the aim of improving the prevention, diagnosis and treatment of a wide range of serious and life-threatening illnesses – including cancer, heart diseases, stroke, diabetes, arthritis, osteoporosis, eye disorders, depression and forms of dementia. U.K. Biobank recruited 500,000 people aged between 40-69 years in 2006-2010 from across the country to take part in this project.⁶²

Unlike in Icelandic biobank project, the U.K. Biobank project was established by a medical charity and governmental agencies and is hosted by an academic institution with the support by the National Health Service. The project tried to solve the controversy over ownership of the data in the biobank by framing the issue from the partnership perspectives instead of the property point of view. In 2001, the House of Lords Science and Technology Committee issued a report entitled *Human Genetic Databases: Challenges and Opportunities*. After summarizing testimonies regarding the property aspects of the prospective U.K. Biobank project, the report states that “in common with most of our witnesses, we do not regard ownership of biological samples as a particularly useful concept with respect to human genetic databases.” Furthermore, it states that “we prefer the notion of *partnership* between participants and researchers, for medical advance and the benefit of others, including future generations.”(*Emphasis added*)⁶³ This new conceptual framework may well be applied to the EHR data context as well. Under this partnership framework, the entities involved in the project are regarded as guardian of the data in partnership with the researchers and the donors/patients instead of the owner or the licensee of the data.

⁶² *About UK Biobank*, UK BIOBANK, <http://www.ukbiobank.ac.uk/about-biobank-uk/> (last visited Nov. 29).

⁶³ Winickoff at 442 (quoting House of Lords Science and Technology Committee, *Human Genetic Databases: Challenges and Opportunities*, 4th Report, Session 2000-2001, Chap. 7, paragraph 7.16.)

The partnership model is useful in that its focus is how the resource of the database – i.e., EHR data – should be managed rather than who owns and controls it. The U.K. Biobank further eliminated the room for unnecessary debates on the ownership of the data and property rights for the data in the database by choosing a nonprofit charity organization form as a managing entity. The U.K. Biobank functions as a “trusted intermediary,” a “public authority” middleman, and an IRB all at the same time without the need to answer the theoretical questions on the ownership and control over the data. By involving private, academic and government entities from the planning stages, the U.K. Biobank carefully sorted out various interests of each entity and found the compromising position among them, and screened out the possible drawbacks early on in the project.

Notably, the project developed a public Ethics and Governance Framework (EFG) to set standards for the project, and to ensure that safeguards are in place for scientifically and ethically approved research.⁶⁴ It is noteworthy that the U.K. Biobank project tried to slow down the process of realizing the national database by taking various precautions. First, it elicited outside comments from various sources. For instance, the Ethics and Governance Framework went through a public consultation process. In addition, the project intentionally progressed over a period of time – i.e., 7 years -- instead of trying to create a mega database immediately. After years of preplanning, a pilot project started by recruiting up to three thousand patients for the

⁶⁴ *UK BIOBANK Ethics and Governance Framework: Summary of Comments on Version 1.0* (May 2004). <http://www.ukbiobank.ac.uk/wp-content/uploads/2011/07/EGF-consultation-2004.pdf?phpMyAdmin=trmKQIYdjjnQIqJ%2CfAzikMhEnx6> (last visited Nov. 29, 2012).

first stage of the study.⁶⁵ It was only after the success of the pilot project and gradual recruiting of half a million donors over years that the Biobank finally opened its doors to the researchers.⁶⁶

The creation of the EHR database for the research use can benefited with the similar approach of the U.K. Biobank with careful preplanning for the project. Instead of burdening the already overworked government entities and IRBs, the U.S. can also create a non-profit organization where the private non-profit organizations, government entities and academic institutions participate as partners for the common purpose of creating an EHR database for the use of record-based research. As in the example of the U.K. Biobank, the U.S. EHR database for the research purpose can start from the small scale pilot project slowly and progress over time to a more extensive research resource. Creating such database for the research purpose is not without precedents in the U.S. since in 2003, seven disease organizations in this country created the Genetic Alliance BioBank, an initiative that collects, stores, and distributes biospecimens and clinical data to researchers studying certain diseases.⁶⁷

Planning and starting a pilot project for EHR database for the record-based research will be relatively easier than those for the biobanks with the advent of various EHR databases that are already in place and more compliance with the meaningful use requirement for increased interoperability. The record-based research does not expose the patients to any physical or psychological testing in research, which often led some scholars to advocate for applying more

⁶⁵ UK Biobank vanguard project begins, Medical Research Council, <http://www.mrc.ac.uk/Newspublications/News/MRC002005> (last visited Nov. 29, 2012).

⁶⁶ *UK Biobank Opens to Researchers*, BBC NEWS: HEALTH, Mar. 29, 2012, <http://www.bbc.co.uk/news/health-17553931> (last visited Nov. 29, 2012).

⁶⁷ Karen J. Maschke, *Biobanks: DNA and Research*, THE HASTINGS CENTER, <http://www.thehastingscenter.org/publications/briefingbook/detail.aspx?id=2154> (last visited Nov. 29, 2012)

lenient regulations for providing access to EHR data for the researchers who are conducting record-based researches.⁶⁸

VII. Conclusion

Individual interests in protecting privacy often conflict with public need for promoting wide access to and usage of the individual health records. The answer for how to balance those two interests when conflicting cannot be drawn simply by defining who owns the individual protected health information. The theoretical discussions so far on who owns and controls the EHR data turned out to be futile. The article proposes the creation of an EHR database available for the record-based research purpose, based on the model of U.K. biobank project to ensure effective balancing between private interest in protecting individual privacy and public interest in promoting the beneficial use for the public. U.K. Biobank has already created and made available an online database of medical and lifestyle records from half a million middle-aged people in Britain. By incorporating some of the positive elements that led the U.K. Biobank project to success, the U.S. EHR database will be able to increase its own success in implementation of the protocol for creating the EHR database for the record-based research use. Many of the controversies – i.e., the scope and contents of the patient records to be made available to the researchers, the extent to which the patient's consent should be obtained, the scope of power of the entities/persons who are managing the database content, etc. – had been discussed and covered in the process of creating the U.K. Biobank. This article proposes that the private and public entities form a partnership to initiate a pilot project that starts with EHR data of a regional population to create a central database for the purpose of record-based research

⁶⁸ See Hoffman and Podgurski at 125.

projects. In the process, the partnership will be able to find a more concrete framework for dealing with practical problems in managing the EHR database for the research purposes. By this proposal, this article is not making an effort to decide whether or not the public benefits use should trump the private privacy interests or vice versa; rather it tries to find a compromising point where the two interests can co-exists harmoniously. With the advent of many EHR database on a local levels made available, we are faced with a great potential for the use of valuable resources for the purpose of advancing medical knowledge for public benefits. As Franklin D. Roosevelt once said, “there are many ways of going forward, but only one way of standing still.” The proposal in this article might not be the best way to proceed to the end of serving the medical research community and the public, but it can surely be the first step to that end.