12 Hous. J. Health L. & Policy 137

Houston Journal of Health Law & Policy
ISSN 1534-7907

A POLICY AND TECHNOLOGY FRAMEWORK FOR USING CLINICAL DATA TO IMPROVE QUALITY

Deven McGraw* and Alice Leiter**

I. INTRODUCTION

Despite the undeniable advancements in medicine over the last several decades, the U.S. has been unable to match this progress with respect to health outcomes, due at least in part to the failure to effectively manage and use health data. There is a high price to be paid for this lack of advancement, both with respect to quality and cost of care.

Although Americans are living longer, they are often sicker, with multiple complex health conditions.[1] As a result, the U.S. notoriously spends more on health care than any other country, yet its health system ranks 37th worldwide.[2] Studies show that patients in America only get the right care—at the right time and for the right

* Director, Health Privacy Project, Center for Democracy & Technology, Washington, DC.

** Policy Counsel, Health Privacy Project, Center for Democracy & Technology, Washington, DC.

1 CAMPAIGN FOR BETTER CARE, NAT'L P'SHIP FOR WOMEN & FAMILIES, FACT SHEET: THE CASE FOR BETTER CARE (Jan. 12, 2011), http://www.communitycatalyst.org/doc_store/publications/CBC%20Fact%20Sheet%203_Cost%20to%20Families%20and%20Caregivers.pdf.2009).

2 Christopher Murray & Julio Frenk, *Ranking 37th — Measuring the Performance of the U.S. Health Care System*, 362 NEW ENG. J. MED. 98, 98–99 (2010), *available at* http://www.nejm.org/doi/pdf/10.1056/NEJMp0910064 (citing World Health Organization, The World Health Report 2000 152-55 (2000), http://www.who.int/whr/2000/en/).

reason—about half the time;[3] and, there are pronounced disparities in access to, and quality of, care.[4]

Health information technology (health IT) alone will neither solve these quality problems nor the skyrocketing costs of care, but its effective implementation and widespread use are seen as key to reversing these trends. It can help establish better access to and use of information, both of which are significant milestones on the path to reform. Health IT has the potential to improve individual health through better communication and coordination of care, as well as reduced medical errors and increased efficiency of time and resources. Population health stands to benefit as well, through reduction of disparities in care, improved quality reporting, strengthened and connected public health initiatives, and more rapid and targeted research.

The unprecedented resources made available by Congress in the stimulus legislation of 2009 and in the health reform law of 2010 represent a historic opportunity to transform care so that it is noticeably improved from the eyes of consumers—the taxpayers who finance these initiatives and who have the most to lose if they do not succeed. The U.S. has embarked on an approximately 47 billion-dollar initiative, broadly referred to as "Meaningful Use," to improve individual and population health through the use of electronic medical records by health care providers and patients.[5] The funding to support this initiative, enacted as part of the Health Information

---

[3] *See*, *e.g.*, Rita Mandione-Smith, et al., *The Quality of Ambulatory Care Delivered to Children in the United States*, 357 NEW ENG. J. MED. 1515, 1515, 1521–1523 (2007), http://www.nejm.org/doi/pdf/10.1056/NEJMsa064637.

[4] For example, African Americans have higher rates of mortality from heart disease, cancer, HIV/AIDS and cerebrovascular disease than any other racial or ethnic group in the U.S. *See* COMM. ON UNDERSTANDING AND ELIMINATING RACIAL AND ETHNIC DISPARITIES IN HEALTH CARE, INST.BRIAN SMEDLY ET AL., INST. OF MED., UNEQUAL TREATMENT: CONFRONTING RACIAL AND ETHNIC DISPARITIES IN HEALTH CARE 5 (Brian SMEDLY et al. eds., (2003), *available at* http://books.nap.edu/openbook.php?record_id=10260.

[5] *See Overview: The Official Web Site for the Medicare and Medicaid Electronic Health Records (EHR) Incentive Programs*, *See Programs*, CTRS. FOR MEDICARE & MEDICAID SERVS., http://www.cms.gov/ehrincentiveprograms/ (last visited Mar. 29, 2012); *see also* Terri Shaw, CHILDREN'S P'SHIP & THE KAISAR COMM'N ON MEDICAID AND THE UNINSURED, *Federal Support for Health Information Technology in Medicaid: Key Provisions in the American Recovery and Reinvestment Act*, CHILDREN'S P'SHIP & THE KAISER COMM'N ON MEDICAID AND THE UNINSURED (Aug. 2009), http://www.kff.org/medicaid/upload/7955.pdf.

Technology for Economic and Clinical Health Act of 2009 (HITECH), is a combination of incentive payments for health care providers (chiefly physicians and hospitals)-to purchase electronic health record (EHR) systems that meet certain minimum criteria-and grants to states and other entities-to create EHR infrastructure and further support use of health IT.[6] In the initial phases of the incentive program, which began in 2011, the emphasis is on capturing relevant demographic and clinical data in EHRs and using that data to improve treatment and care coordination for individual patients, with some focus on reporting to public health agencies; in later stages of the program, the expectation is that the focus will expand to population health initiatives.[7]

HITECH further directs the Department of Health and Human Services (HHS) (specifically, the HHS Office of the National Coordinator for Health IT (ONC)) to develop a "nationwide health information technology infrastructure" that improves health care quality, reduces medical errors and disparities, and reduces health care costs from inappropriate or duplicative care.[8] This will be complemented by the federal focus on using health IT more broadly as a tool of health reform. The 2011-2015 Federal Health Information Technology Strategic Plan issued by ONC identifies improving population health, reduction of health care costs, and achieving rapid learning as key goals of federal health IT initiatives.[9] The vision is to create a "learning" health care system that leverages clinical

---

[6] The Health Information Technology for Economic and Clinical Health Act (HITECH) Act), Pub. L. No. 111-5, tit. XIII, Div. B, tit. IV, 123 Stat. 115, 276–79; 467–96 (2009).

[7] Press Release, CTRS. FOR MEDICARE & MEDICAID SERVS., CMS FINALIZES DEFINITION OF MEANINGFUL USE OF CERTIFIED ELECTRONIC HEALTH RECORDS (EHR) TECHNOLOGY (July 16, 2010), http://www.cms.gov/apps/media/fact_sheets.asp (search "CMS Finalizes Definition").

[8] HITECH Act, § 3001(b).

[9] OFFICE OF THE NAT'L COORDINATOR, DEP'T HEALTH & HUM. SERVS., FEDERAL HEALTH IT STRATEGIC PLAN 2011-2015, http://healthit.hhs.gov/portal/server.pt/gateway/PTARGS_0_0_4318_1211_15583_43/http%3B/wci-pubcontent/publish/onc/public_communities/f_j/onc_website___home/fed_health_strategic_plan/fed_health_it_strategic_plan_home_portlet/files/final_federal_health_it_strategic_plan_0911.pdf (last visited Mar. 30, 2012). 4-5, http://healthit.hhs.gov/portal/server.pt/community/federal_health_it_strategic_plan_-_overview/1211. THE FEDERAL HEALTH IT STRATEGIC PLAN 2011-2015, (follow "Read the Federal Health IT Strategic Plan [PDF - 1 MB]" hyperlink).

information in EHRs to improve the knowledge base about effective prevention and treatment strategies, and to disseminate that knowledge more quickly and efficiently to clinicians and patients to improve the quality and efficiency of health care.[10]

Achieving this learning health care system will not be possible without easier and more robust access to clinical data in EHRs initially collected for treatment purposes. More broadly, enabling expanded secondary use of treatment data for health quality improvement purposes will require a policy framework to support it, as access to data for purposes secondary to treatment raises health privacy concerns. As explained in more detail below, current federal privacy and data-governance policies regarding use of EHR data for quality improvement purposes are based on outdated schools of thought on how best to protect privacy–largely through an overreliance on patient consent. Current policies also do not address critical questions of data architecture (e.g., how data can be accessed across multiple institutions for quality purposes).

This article explores some key problems with current policies governing uses of EHR data for quality analytics and calls for the development and implementation of a comprehensive policy and technology framework to govern the use of clinical EHR data for these purposes that is based on the full complement of Fair Information Practice Principles (FIPPs). Initial steps to develop this framework should include:

- Reducing reliance on consent to govern such secondary uses and bolstering policies that strengthen accountability for strong data stewardship among holders and users of EHR data;
- Eliminating current disincentives to conduct health quality analytics with EHR data with the intent of sharing the results (in privacy-protected ways) for purposes of improving the health care system; and
- Utilizing distributed network approaches, when possible, to conduct multi-site quality analytics.

---

[10] *See id*. at 5.

II. CURRENT LAW

Federal and state health privacy laws govern how entities within the health care system may collect, access and disclose identifiable health information. These rules typically vary based not only on who is handling the information, but also on the purpose for which the information is being accessed or disclosed. Below, this article briefly summarizes how federal health privacy laws govern the use of treatment information in EHRs for secondary purposes.

A. Laws Governing Secondary Use of Identifiable Data in EHRs

The primary federal laws governing secondary use of EHR data are (1) the Health Insurance Portability and Accountability Act (HIPAA),[11] (2) privacy regulations (the Privacy Rule),[12] and (3) the Common Rule.[13] Other federal and state laws also place some limits on access, use, and disclosure of identifiable health information.

1. The HIPAA Privacy Rule

The HIPAA Privacy Rule permits "covered entities" (most health care providers and health care institutions) to access, use and disclose identifiable personal health information ("protected health information") for treatment, payment and health care operations without the need to first obtain a patient's consent.[14] The Rule further authorizes health care entities to access identifiable health information for "learning" purposes, or those beyond treatment and payment, in two main categories: health care operations and research.[15] "Health care operations" is a broad category of largely administrative activities that includes "conducting quality assessment and improvement activities, including outcomes evaluation and development of clinical guidelines," as long as obtaining "generalizable knowledge" is not the "primary purpose" of

---

[11] Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (1996).

[12] 45 C.F.R. Parts 160, and 164 (Subparts 2003 Subparts A and E).

[13] Federal Policy for the Protection of Human Subjects, 45 C.F.R. pt. 46.

[14] 45 C.F.R. § 164.502(a)(1) (2010).

[15] *Id.*; *see also* § 164.512(i) (2010).

any studies resulting from these activities.[16]

In contrast, "research" covers activities "designed to develop or contribute to generalizable knowledge."[17] Thus, a key distinction between these categories is whether or not a primary purpose of the activity is to contribute to generalizable knowledge. In general, health care entities interpret this distinction by considering quality improvement activities intended solely for *internal* use to be "operations" and activities whose results may be shared and disseminated outside the organization for the benefit of others to be "research."[18]

2. The Common Rule

The federal Common Rule governs most research using identifiable health information that is supported by federal funding from certain agencies (including, among others, HHS, the Department of Veterans Affairs and the Department of Energy).[19] The Common Rule also perpetuates the distinction between uses for operations and research by defining "research" as activity contributing to generalizable knowledge.[20] As a result, activity *not* contributing to generalizable knowledge is not regulated by the Common Rule.

3. Other Federal and State Laws

There are a number of other federal laws that protect particular types of data, and a whole host of state-specific laws governing

---

[16] 45 C.F.R. § 164.501 (2010).

[17] *Id*.

[18] *See* Deven McGraw & Alice Leiter, *Legal and Policy Challenges to Secondary Uses of Information from Electronic Clinical Health Records*, ACADEMY HEALTH, http://www.academyhealth.org/files/publications/HIT4AKLegalandPolicy.pdf.ACADEMY HEALTH, 2012), http://www.academyhealth.org/files/publications/HIT4AKLegalandPolicy.pdf (last visited Mar. 30, 2012).).

[19] *See generally* 45 C.F.R. pt. 46 (2010). Note that FDA regulations conform to the Common Rule to the extent permitted by statute, but the FDA has its own rules governing human subjects research that include a different definition of "research." *See* Bonnie M. Lee, *Comparison of FDA & HHS Human Subject Protection Regulations*, U.S. FOOD & DRUG ADMIN. (Mar. 10, 2009), http://www.fda.gov/ScienceResearch/SpecialTopics/RunningClinicalTrials/EducationalMaterials/ucm112910.htm , (last visited Mar. 29, 2012).

[20] 45 C.F.R. § 46.102(d)10 (2010).

various types of health information and their exchange. For example, Part 2 of the Code of Federal Regulations[21] provides protection for the confidentiality of information related to drug and alcohol treatment, and the Family Educational Rights and Privacy Act (FERPA)[22] protects identifiable health information held in education records of federally-funded educational institutions.

In addition to navigating federal laws, those looking to access health data must comply with applicable state laws governing health information, and all state laws that provide greater protections for health information than the HIPAA rules are valid.[23] Some of these laws cover all health information; most state laws apply only to identifiable information, and specifically information in certain sensitive categories, such as genetic or mental health information, or HIV test results.[24] This means that state laws that govern certain types of sensitive data may be implicated when research is using identifiable data in one of these categories.

A full discussion of federal and state privacy laws is beyond the scope of this paper, which will focus on HIPAA and the Common Rule.

---

[21] *See generally* 42 C.F.R. pt. 2 (2002).

[22] *See generally* Family Educational Rights & Privacy Act, 20 U.S.C. § 1232g (2006).

[23] *See generally* Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1987 (codified as amended at 42 U.S.C. § 300gg-62 (2010)); *see also* U.S. DEP'T OF HEALTH & HUMAN SERVS., *Does the HIPAA Privacy Rule Preempt State Laws?*, http://www.hhs.gov/hipaafaq/state/399.html (last updated Dec. 11, 2006) (Congress dictated that HIPAA would preempt (or nullify) any conflicting or less protective laws, and leave intact any state law more restrictive than HIPAA) HHS.GOV, (last visited Mar. 29, 2012).

[24] *See generally* OFFICE OF NAT'L COORDINATOR FOR HEALTH INFO. TECH., HARMONIZING STATE PRIVACY LAW COLLABORATIVE, HEALTH INFORMATION SECURITY AND PRIVACY COLLABORATION*: Harmonizing State Privacy Law Collaborative Final Report*, U.S. DEP'T OF HUMAN & HEALTH SERVS. (Mar. 31, 2009), http://healthit.hhs.gov/portal/server.pt?open=512&objID=1280&PageID=16053&mode=2&cached=true (click "Final Report"), *See also* http://healthit.hhs.gov/portal/server.pt?open=512&objID=1280&PageID=16053&mode=2&cached=true (last visited Mar. 30, 2012) (Report on State Privacy and Security Laws Related to Electronic Health Records and Electronic Health Information Exchange); s*ee also* JOY PRITTS ET AL., *The State of Health Privacy:* SECOND EDITION, *A Survey of State Health Privacy Statutes*, 2 INST. FOR HEALTH CARE RES. & POL'Y GEO. U. i, ii (2nd ed.) (2002), http://ihcrp.georgetown.edu/privacy/pdfs/statereport1.pdf.

B. Rules Applying to Use of "Anonymized" Data

Under both HIPAA and the Common Rule, research using information that is not identifiable (or raises less risk of identification) can be conducted with fewer restrictions. In general, this is wise policy, as information in less identifiable form raises less privacy risk.

There are two classes of data stripped of identifiers that are either exempted from, or treated differently under, the HIPAA Privacy Rule. The first, referred to as "de-identified" data, has been so stripped of common identifiers that there is no "reasonable basis" to believe it can be linked to a particular individual.[25] Data that qualify as "de-identified" under the Privacy Rule are not regulated at all, and there are no restrictions on who can acquire it or the purposes for which it can be accessed, used or disclosed.[26]

Of note, the Common Rule only applies to identifiable data. Research that involves information recorded "in such a manner that subjects cannot be identified, directly or through identifiers linked to the subjects" is outside the scope of the Rule.[27] Further, "human subject" is defined as a "living individual about whom [a researcher obtains] . . . [i]dentifiable private information" and, additionally, the "information must be individually identifiable . . . in order for obtaining the information to constitute research involving human subjects."[28]

The second class of less identifiable data under the Privacy Rule, known as a "limited data set," is stripped of many categories of identifying information but retains information often needed for public health and research, such as birth dates, dates of treatment,

---

[25] 45 C.F.R. § 164.514(a) (2002).

[26] *Id.*; *see also Stronger Protections for, and Encouraging the Use of, De-Identified (and "Anonymized") Health Data*, CTR. FOR DEMOCRACY & TECH., (June 26, 2009), https://www.cdt.org/policy/stronger-protections-and-encouraging-use-de-identified-and-anonymized-health-data.

[27] 45 C.F.R. § 46.101(b)(4) (2005).

[28] 45 C.F.R. § 46.102(f) (2011); *see also* Human Subjects Research Protections: Enhancing Protection for Research Subjects and Reducing Burden, Delay, and Ambiguity for Investigators, 76 Fed. Reg. 44512, 44525 (Proposed July 26, 2011) (to be codified at 45 C.F.R. pt. 46, 160, 164 and 21 C.F.R. pt. 50, 56) (of note, HHS is considering changing the Common Rule to adopt the standards for de-identification in the HIPAA Privacy Rule).

and some geographic data.[29] Entities covered by HIPAA may share a limited data set for research, public health and health care operations purposes permitted by the Privacy Rule, so long as all recipients are bound by a data use agreement with the originator of the data.[30] This agreement must detail the permitted uses and disclosures of the covered data, establish who is permitted to use and disclose the data, and prohibit the data from being re-identified.[31]

Even when identifiable information is used, the Privacy Rule's minimum necessary standard requires providers to use the least amount of data necessary to accomplish a particular purpose for which information is accessed or disclosed, and this standard applies to uses of information for operations and research purposes.[32] Although little guidance has been issued by the HHS Office for Civil Rights (which has oversight over HIPAA regulations) on compliance with the minimum necessary standard, some have suggested that the standard should apply to the identifiability of the data particularly with respect to non-treatment uses.[33]

C. The Role of Institutional Review Boards in Reviewing Research

In regulating research using identifiable data, both HIPAA and the Common Rule rely heavily on review of research by Institutional Review Boards. Institutional Review Boards (IRBs) are committees designated to approve and review research involving human subjects. The Food and Drug Administration and the Office for Human Research Protections within HHS issue regulations that

---

[29] 45 C.F.R. § 164.514(e)(2) (2010).

[30] 45 C.F.R. § 164.514(e)(4) (2010); *Id.*; *see also Stronger Protections for, and Encouraging the Use of, De-Identified (and "Anonymized") Health Data*, CTR. FOR DEMOCRACY & TECH., (June 26, 2009), https://www.cdt.org/policy/stronger-protections-and-encouraging-use-de-identified-and-anonymized-health-data.

[31] 45 C.F.R. § 164.514(e)(4) (2010).

[32] 45 C.F.R. §§ 164.502(b), 164.514(d) (2010).

[33] *See, e.g.*, Ctr. for Democracy & Tech. et al., comments to the Health & Human Svcs.,HHS *Notice of Proposed Rulemaking: Modifications to the HIPAA Privacy, Security, and Enforcement Rules under the Health Information Technology for Economic and Clinical Health Act* (2010), https://www.cdt.org/files/pdfs/CDT_Comments_to_HHS_Proposed_Rulemaking_09-13-10.pdf.

govern these bodies, which are responsible for conducting scientific, ethical and regulatory oversight functions.[34]

For example, under the HIPAA Privacy Rule, internal use or disclosure of identifiable health information for research purposes usually requires specific authorization from the individual, unless the research meets one of a few, narrow exceptions,[35] or the requirement for authorization is waived by an IRB or Privacy Board.[36] Under the Privacy Rule, such authorizations must be in writing and include: who can use or disclose identifiable health information; to whom the information may be disclosed; what information may be used or disclosed; and the purposes for the use and/or disclosure of the information.[37] Research authorizations must be specific to a particular research project and cannot be combined with other consents that may be required (such as for treatment, as long as the treatment not part of a research protocol),[38] although HHS has recently proposed allowing more general consent for the use of identifiable information for all research purposes and allowing compound authorizations in some circumstances.[39]

Under the Common Rule, research using identifiable data originally collected for purposes other than research, such as treatment, is subject to similar regulations.[40] IRB approval is required, but such research is eligible for expedited review——a procedure through which certain kinds of research may be reviewed and approved without convening the entire IRB, but rather by the

---

[34] *See generally*, *Institutional Review Boards Frequently Asked Questions - Information Sheet*, U.S. FOOD & DRUG ADMIN. (Aug. 9, 2011),FDA.GOV, http://www.fda.gov/RegulatoryInformation/Guidances/ucm126420.htm; *see generally* 21 C.F.R. § 56.111 (2011) (last visited Mar. 29, 2012).

[35] *See generally* 45 C.F.R. § 164.512(i) (2010). Exceptions include review of protected health information as necessary to prepare for research, as long as the information does not leave the covered entity, research on decedents' information, and research on a limited data set.

[36] 45 C.F.R. § 164.512 (i)(1)(i) (2010). A Privacy Board is a review body that may be established to act upon requests for a waiver or an alteration of the authorization requirement under the Privacy Rule for uses and disclosures of personal health information for a particular research study.

[37] 45 C.F.R. § 164.508(c) (2002).

[38] 45 C.F.R. § 164.508(b)(3) (2002) (noting limited exceptions).

[39] 75 Fed. Reg. 40867, 40892-95 (Jul. 14, 2010); *see also* 76 Fed. Reg. 44512, 44523 (July 26, 2011).

[40] *See generally* 45 C.F.R. § 46.101 (2011).

"IRB chairperson or by one or more experienced reviewers designated by the chairperson from among members of the IRB."[41] The patient's consent is also required if the researcher is receiving identifiable information.[42]

Such consent can be waived by the IRB in circumstances somewhat similar to those for a waiver of authorization under HIPAA.[43] HHS recently announced some possible changes to the Common Rule that would potentially make all research on identifiable EHR data collected for non-research purposes exempt, even if identifiers are provided to the researcher; patient consent, however, would still be required for such studies.[44] HHS is also considering making such consent more flexible and easier to obtain.[45]

However, because the nature of secondary uses of EHR data makes it difficult or often infeasible to obtain the patient's prior consent or authorization, researchers often have two choices: obtain a waiver of consent or use information that is less identifiable and that is subject to less regulation under both the Privacy Rule and the Common Rule.

III. SHORTCOMINGS OF CURRENT LAW

The current legal framework for secondary uses of EHR data has been criticized by many as creating obstacles to such uses of data, while providing few meaningful protections for an individual's

---

[41] 45 C.F.R. § 46.110 (2010); *see also Categories of Research That May Be Reviewed by the Institutional Review Board (IRB) Through an Expedited Review Procedure*, OFF. FOR HUM. RES. PROTECTIONS (Nov. 9, 1998),(*see* http://www.hhs.gov/ohrp/policy/expedited98.html (listing categories of research eligible for expedited review)).

[42] 45 C.F.R. § 46.116 (2010).

[43] The requirement for consent can be waived if: "(1) [t]he research involves no more than minimal risk . . .; (2) [t]he waiver will not adversely affect the rights and welfare of the [patients]; (3) [t]he research could not practicably be carried out without the waiver . . .; and (4) [when] appropriate, the subjects [are] provided with additional pertinent information after participation." (45 C.F.R. 46.116(d) (2010)). Consent can also be waived for certain research evaluating public benefit services or programs. (45 C.F.R. 46.116(c) (2010)).

[44] Human Subjects Research Protections: Enhancing Protections for Research Subjects and Reducing Burden, Delay, and Ambiguity for Investigators, 76 Fed. Reg. 44512, 44519 (July 26, 2011).

[45] *Id*.

personal health information.[46] This article focuses on three particular criticisms:

1. Overreliance on patient consent–in both HIPAA and the Common Rule–to protect individual privacy and confidentiality when research is done using identifiable information initially collected for treatment purposes in EHRs;
2. Preferential regulatory treatment under HIPAA of quality improvement analyses that will be used only internally, which may create a disincentive to share internally gathered knowledge with peers in order to contribute to a "learning" health care system; and
3. Lack of policy regarding appropriate technical architectures for analyzing EHR data.

The inadequacies of the current framework will be exacerbated by increasing pressures to use EHR data for secondary purposes, as well as by an increase in the availability of such data due to the HITECH incentives and health reform imperatives. Private sector initiatives that are focused on getting health care costs under control will further amplify the need for more robust analysis of EHR data to gather the most effective, including the most cost-effective, information.

In the section below, this article discusses these criticisms in more detail. The article then calls for a more comprehensive policy framework, based on the full complement of FIPPs, to govern secondary uses of EHR data, particularly with respect to quality analytics. The article further recommends that analysis of EHR data take place using a distributed network architecture, where potentially sensitive health information remains under the stewardship of the source of the information but is still made available for a robust

---

[46] *See, e.g.*, COMM. ON HEALTH RESEARCH & THE PRIVACY OF HEALTH INFO., BEYOND THE HIPAA PRIVACY RULE: ENHANCING PRIVACY, IMPROVING HEALTH THROUGH RESEARCH 250, (Sharyl J. Nass et al...,. eds., 2009), *available at* http://books.nap.edu/openbook.php?record_id=12458; Fred H. Cate, *Protecting Privacy in Health Research: The Limits of Individual Choice*, 98 CAL. L. REV. 1765, 1769; Charles Safran et al., *Toward a National Framework for the Secondary Use of Health Data: An American Medical Informatics Association White Paper*, 14 J. AM. MED. INFORMATICS. ASS'N 1, 1-3(2007); Meryl Bloomrosen & Don Detmer, *Advancing the Framework: Use of Health Data—A Report of a Working Conference of the American Medical Informatics Association*, 15 J. AM. MED. INFORMATICS ASS'N 715, 715 (2008).

analysis for quality and cost purposes.

A. Overreliance on Consent

As mentioned above, both HIPAA and the Common Rule have traditionally placed a major focus on when an individual's authorization or consent is or is not required for secondary uses of identifiable clinical data. Related laws—even HHS' recently-released "Advanced Notice of Proposed Rulemaking" (ANPRM) on *Human Subjects Research Protections: Enhancing Protections for Research Subjects and Reducing Burden, Delay and Ambiguity for Investigators*[47]—perpetuate this historic emphasis.[48]

The reliance on notice and consent to protect privacy is not limited to health regulators. In 1998 the U.S. Federal Trade Commission (FTC) released a report regarding what it believed privacy policies should contain.[49] According to the FTC, "[t]he most fundamental principle is notice . . . [because] [w]ithout notice, a consumer cannot make an informed decision as to whether and to what extent to disclose personal information."[50] The FTC added that "[t]he second widely-accepted core principle of fair information practice is consumer choice or consent . . . [over] how any personal information collected from them may be used."[51]

Notice and consent may play some role in making patients more aware of the potential for use and disclosure of their information beyond treatment or payment purposes,[52] but these procedures do very little on their own to protect an individuals' privacy. In isolation, without other legal limits, mandating consent is more likely

---

[47] 76 Fed. Reg. 44512, 44519.

[48] *See, e.g.*, 45 C.F.R. § 46.102(f) (2009).

[49] Martha K. Landesberg, et al., *Privacy Online: A Report to Congress*, FED. TRADE COMM'N (June 1998), http://www.ftc.gov/reports/privacy3/priv-23a.pdf. [hereinafter "FTC Report"]; Cate, *supra* note 46, at 1768.

[50] FTC Report, *supra* note 49, at 7.

[51] *Id*. at 8.

[52] A number of critics of reliance on consent to protect privacy are doubtful that notice and consent plays much of an effective role in educating individuals about uses of their information. *See, e.g.*, Cate, *supra* note 46, at 1773; *see also,* Solon Barocas & Helen Nissenbaum, *On Notice: The Trouble with Notice and Consent*, N.Y.U. (Oct. 2009), http://www.nyu.edu/projects/nissenbaum/papers/ED_SII_On_Notice.pdf.

to lead to over-broad information sharing than to the protection of patient privacy. In the words of one pointed critic, "[a]ll of the available evidence suggests that notices are widely ignored by individuals and are written in overly broad or overly detailed language."[53]

Too often, privacy notices are widely ignored by the very people they purport to protect.[54] For example, patients may be asked for their consent to use their information to improve the quality of their health care and reduce costs, which will sound appealing and acceptable to most, but conveys little meaningful information on how the information is going to be used. "As a result, individuals are not aware of—or do not understand—the choices available to them, or those choices are so broad or so frequent as to be meaningless."[55] Essentially, consent often leaves decisions about whether a particular use of data will contribute to quality improvement or cost reduction in the hands of the person or entity accessing the data for this purpose.

Further, "[o]ver-reliance on consent can confer disproportionate bargaining power on providers and others seeking approval for disclosure," especially in circumstances under which patients are unlikely to withhold consent, such as when they are seeking health care or insurance coverage.[56] It also inappropriately shifts the burden for protecting privacy onto patients, rather than making the entity holding the health data responsible for adopting comprehensive privacy protections.[57] "Yet few individuals have the time, knowledge, or interest to make all of those choices about data collection and use."[58] For example, "[c]hoice can be a disservice to the individual. . .when the individual injures his or her own interests through an uninformed or unwise choice. And there are many

---

[53] Cate, *supra* note 46, at 1769.

[54] *Id.* at 1769, 1773.

[55] *Id* at 1769.

[56] CENTER FOR DEMOCRACY & TECH., RETHINKING THE ROLE OF CONSENT IN PROTECTING HEALTH INFORMATION PRIVACY (January 2009) at 8, http://www.cdt.org/files/pdfs/20090126Consent.pdf.

[57] See *id*.

[58] Cate, *supra* note 46, at 1776.

situations in which individual choice is outweighed by other interests of the individual or society."[59] This is particularly true when consent is sought in a general or "blanket" way (such as consent for all "research" uses of EHR data).[60]

Under HIPAA, research requires individual "authorization," which must contain a number of core elements, including: a description of the information to be used or disclosed; the name of the person or persons authorized to make the requested use or disclosure; the name of the person or persons to whom the covered entity may make the requested use or disclosure; a description of each purpose of the requested use or disclosure; an expiration date; and the signature of the individual.[61] Such an authorization, because of its level of detail, is designed to be more protective of privacy than mere general consent. However, whether the individual will understand and read a detailed explanation, and feel empowered to make a choice not to share, is another matter. In addition, HHS has recently proposed some revisions to this and related requirements that would make them somewhat more flexible.[62]

Moreover, the HIPAA Privacy Rule's imposition of authorization requirements in the research context has been shown to introduce the potential for selection bias.[63] Individuals who agree to have their information used for research purposes often differ from those who do not.[64] Some have argued that those "who refuse to consent—or to make a decision of any form—exhibit distinct demographic and health characteristics that are statistically capable of skewing the research base."[65]

As discussed in more detail below, this article does not propose eliminating requirements to obtain individual consent or authorization for *any* secondary use of identifiable EHR data.

---

[59] *Id*. at 1769.

[60] *See* CENTER FOR DEMOCRACY & TECH., *supra* note 56, at 8.

[61] 45 C.F.R. § 164.508(c).

[62] *See* 76 Fed. Reg. 44512, 44523.

[63] *See* Cate, *supra* note 46, at 1791.

[64] *Id*.

[65] *Id*.

Notwithstanding the weaknesses of consent in protecting privacy, individuals consistently express the desire to have some choices regarding whether their information is used for research purposes.[66] Ethical principles have long supported an individual's right to consent to research uses of information about them, and the rules on research set forth in the Privacy Rule and the Common Rule are consistent with these principles.[67] However, given the urgent need to leverage clinical EHR data to improve health care quality and get costs under control, secondary uses that advance that objective arguably should be governed by different—yet still privacy protective—set of rules.

B. Disincentive to Share Results of Internal Quality Reviews

As discussed above, the primary federal rules governing use of EHR data for quality analytics attempt to draw the line between information collection, use or disclosure that is intended to contribute to the knowledge base of the health care community and activities that are intended for internal use. In practice, where there are significantly fewer hurdles, such uses of data for internal quality improvement purposes may contribute to reluctance by health care organizations to engage in quality improvement efforts that involve sharing information across enterprise boundaries.

In fact, researchers have identified federal research regulations as a significant obstacle to accessing health information for secondary learning purposes.[68] The distinction between quality review that

---

[66] *See* Sid J. Schneider et al., *Consumer Engagement in Developing Electronic Health Information Systems: Final Report*, AGENCY FOR HEALTHCARE RES. & QUALITY, 36 (July 2009), http://healthit.ahrq.gov/portal/server.pt/document/888520/09%%-0081-ef_%pdf.

[67] *See* Julia A. Pedroni, & Kenneth D. Pimple, *A Brief Introduction to Informed Consent in Research with Human Subjects*, POYNTER CTR. FOR THE STUDY OF ETHICS & AM. INSTS. (June 2001), http://poynter.indiana.edu/sas/res/ic.pdf; *see also International Ethical Guidelines for Biomedical Research Involving Human Subjects*, COUNCIL FOR INT'L ORGS. OF MED. SCIS. (2002), http://www.cioms.ch/publications/guidelines/guidelines_nov_2002_blurb.htm.

[68] See, e.g., INST. OF MED. OF THE NAT'L ACADS., BEYOND THE PRIVACY RULE: ENHANCING PRIVACY, IMPROVING HEALTH THROUGH RESEARCH 249 (Sharyl J. Nass et al. eds., 2009), http://books.nap.edu/openbook.php?record_id=12458; Deven McGraw, *Paving the Regulatory Road to the "Learning Health Care System"*, 64 Stan. L. Rev. Online 75, 78 (2012), *available at* http://www.stanfordlawreview.org/sites/default/files/online/privacytopics/64-SLRO-75_0.pdf.

qualifies as "operations" and quality reviews that contribute to "generalizable knowledge" may be difficult to make, particularly for entities that have little experience in using information in their records for quality analytics, or who do not yet fully appreciate the value their clinical data hold for purposes beyond treatment.[69] Other institutions default to considering all quality analytics to be "research."[70] This trend is bolstered by the publication policies of peer-reviewed academic journals, most of which require some evidence of IRB approval before results can be considered for publication.[71]

The goals of health care reform, and the overarching health IT strategy of HHS, will require data in EHRs to be "vigorously and meaningfully leveraged to create a learning health care system."[72] Consequently, imposing greater regulatory burdens only for quality research "where the results will be shared with others could significantly undermine this goal."[73] There is a strong argument to be made that the current distinction between operations and research does not serve the purposes either of patients or providers and may be a disincentive too robust and beneficial secondary uses of EHR data for quality analytics.[74]

C. Failure to Address Technical Architecture Issues

Moving the needle on health care quality through retrospective reviews of clinical data in EHRs will almost certainly require access to such records across numerous health care providers and institutions.[75] However, current federal rules neither dictate nor provide guidance on the appropriate technical architecture to facilitate research across multiple institutions. A commonly used

---

[69] McGraw, *supra* note 68, at 77.

[70] *See* McGraw & Leiter, *supra* note 18, at 4.

[71] *See, e.g.*, *IRB FAQs*, NW. U. FOR RES., http://www.research.northwestern.edu/oprs/irb/faqs/index.html (last visited Mar. 30, 2012); *Human Subjects FAQs*, U. OF N.H. RES. OFF., http://www.unh.edu/research/human-subjects-faqs (last visited Mar. 30, 2012).

[72] *See* McGraw, *supra* note 68.

[73] *Id*.

[74] *See* McGraw & Leiter, *supra* note 18, at 6.

[75] *See generally* McGraw & Leiter, *supra* note 18.

path is to create centralized databases of copies of EHR data that can be used to address one or more research questions.

The information essential to addressing quality questions already exists in databases held by health care providers and health plans. Creating multiple copies of this data to address these questions triggers a number of privacy risks.[76]

- Data breaches: Maintaining copies of sensitive information in various locations for long periods of time sharply worsens the risk and severity of data breaches, which are a growing and extremely costly problem for patients, health care companies, and government agencies.[77]
- Public trust: Public trust in the privacy of electronic health records and the clinical information they contain is fundamental to the evolution to a modern, information-driven health care system.[78] Studies regularly show that patients who do not trust the confidentiality of their data are much less likely to share important information with their providers, information necessary for good treatment and care.[79]

---

[76] *Decentralizing the Analysis of Health Data,* (June 26, 2009), https://www.cdt.org/paper/decentralizing-analysis-health-data.

[77] PONEMON INST.,*New Ponemon Institute Study Finds Data Breaches Cost Hospitals $6 Billion; Patient Privacy in Jeopardy: Hospitals Are Not Protecting Patient Data; Healthcare Industry Lagging Behind HITECH* Standards, PONEMON INST. (Nov. 9, 2010), http://www2.idexpertscorp.com/press/healthcare-news/new-ponemon-institute-study-finds-data-breaches-cost-hospitals-6-billion.

[78] *See* David Blumenthal & Georgina Verdugo, *Building Trust in Health Information Exchange: Statement on Privacy and Security*, OFF. OF THE NAT'L COORDINATOR FOR HEALTH INFO. TECH. (July 8, 2010),http://healthit.hhs.gov/portal/server.pt?CommunityID=2994&spaceID=11&parentname=CommunityEditor&control=SetCommunity&parentid=9&in_hi_userid=11673&PageID=0&space=CommunityPage.

[79] *See* CONNECTING FOR HEALTH COMMON FRAMEWORK, *The Architecture for Privacy in a Networked Health Information Environment*, MARKLE FOUND., 3-4 (Apr. 2006), http://www.markle.org/sites/default/files/P1_CFH_Architecture.pdf. In a recent study, more than a quarter of U.S. patients stated they would withhold information from clinicians and avoid treatment in order to preserve the confidentiality of their health data. NEW LONDON CONSULTING, *UK: How Privacy Considerations Drive Patient Decisions and Impact Patient Care Outcomes: Trust in Confidentiality of Medical Records Influence When, Where, Who, and What Kind of Medical Treatment is Delivered to Patients*, 10-11 (Oct. 6, 2011), http://www.fairwarningaudit.com/documents/2011-whitepaper-uk-patient-survey.pdf.

- Inefficient, costly, and burdensome: Diverse entities often want access to health data for secondary purposes that have similar goals.[80] Not only is it burdensome and costly to set up and secure multiple data feeds to different entities in various locations, but it also may be highly inefficient, especially when the analyses are substantially similar. In addition, establishment and maintenance of centralized databases can be expensive.
- Scope creep: When any entity other than a data source possesses copies of health data, there is a risk that uses of the data will incrementally expand, particularly where limits on additional uses are not set forth and enforced in a data use agreement. This has dire consequences for patient—and public—trust.

As described in more detail below, the more privacy-enhancing path to leveraging clinical data in EHRs for quality improvement purposes will enable access to the data at the source, versus creating copies to address a multitude of valuable research questions.

IV. THE NEED FOR A COMPREHENSIVE PRIVACY AND SECURITY POLICY AND TECHNOLOGY FRAMEWORK FOR USE OF EHR DATA FOR QUALITY ANALYTICS

As mentioned above, the current legal framework governing uses of health information for quality analytics overemphasizes the role of individual consent, provides disincentives to using EHR data to conduct quality reviews with the intent of publicly sharing the results, and does not encourage the use of more privacy-protective

---

[80] For example, both the U.S. Office of Personnel Management's (OPM) Health Claims Data Warehouse and many state All-Payer Claims Databases (APCD) perform cost and quality comparisons across geography and demographics. *See* Privacy Act of 1974: New System of Records, 75 Fed. Reg. 61532 (Oct. 5, 2010); Denise Love et al. *All-Payer Claims Databases: State Initiatives to Improve Health Care Transparency*, 99 COMMONWEALTH FUNDAPCD COUNCIL 1,2, 4-5 (Sept. 2010), http://apcdcouncil.org/sites/apcdcouncil.org/files/All-Payer%20Claims%20Databases%20State%20Initiatives%20to%20Improve%20Health%20Care%20Transparency.pdf.

data architectures. To ensure information in EHRs can be effectively leveraged for quality analytics that will help lead to a higher performing, "learning" health care system, policymakers need to develop and implement a comprehensive policy and technology framework to govern data access and use for this purpose. As described in more detail below, such a framework should emphasize responsible data stewardship by data holders, through the adoption of policies and best practices that implement fair information practice principles, and encourage the use of distributed approaches to multi-site quality initiatives whenever possible.

The American Medical Informatics Association (AMIA) has long promoted the need for policy frameworks governing the secondary use of information, noting some five years ago that a "lack of coherent policies and standard 'good practices' for secondary use of health data impedes efforts to transform the U.S. health care system."[81] AMIA has called for an emphasis on public transparency and discourse, concluding that addressing the challenges inherent in health system reform "ultimately requires a national framework for secondary use of health data, including a robust infrastructure . . ."[82] Further, AMIA has made an effort to not only define the concept of data stewardship, but to promote the model's inclusion in policy approaches.[83] In conjunction with articulating some key principles of the concept, AMIA notes that "[d]ata stewardship has emerged as a means to balance the rights of individuals to have their personal information protected and their desire for improved health, more effective health services, and a strengthened and sustainable health system."[84]

It is the intent of this paper to build upon the foundation put forth by AMIA in its study of the necessary elements of an appropriate policy framework for secondary use of information for

---

[81] Charles Safran et al., *Toward a National Framework for the Secondary Use of Health Data: An American Medical Informatics Association White Paper*, 14 J. AM. MED. INFORMATICS ASS'N 1, 3 (2007).

[82] *Id*. at 3.

[83] *See* Meryl Bloomrosen & Don Detmer, *Advancing the Framework*: *Use of Health Data—A Report of a Working Conference of the American Medical Informatics Association,* 15 J. AM. MED. INFORMATICS ASS'N 715, 717 (2008).

[84] *Id*. at 717.

purposes of quality analytics.

A. Adopt Policies and Best Practices Based on Fair Information Practice Principles

1. FIPPs as the Foundation

Fair Information Practice Principles (FIPPs) are the widely-accepted foundation for most current laws governing the collection, use and disclosure of personal information in the U.S. and internationally.[85] They have been shown to be "both "flexible and comprehensive, making them applicable to a wide range of technologies and data usage contexts."[86] The principles are seen as "essential to ensuring that the collection, use, and dissemination of personal information are conducted fairly and in a manner consistent with consumer privacy interests"[87] and can be applied to health data exchange in a comprehensive and balanced fashion, regardless of business model or technology platform.[88]

Common to all FIPPs codes are five core principles of privacy protection: "(1) Notice/Awareness; (2) Choice/Consent; (3) Access/Participation; (4) Integrity/Security; and (5) Enforcement/Redress."[89] When applied appropriately, they implement a model of strong data stewardship where entities that access, use, disclose or retain personal health information are subject to a set of obligations (imposed through law and the adoption of responsible business practices) that determine when they are permitted to collect, use, disclose and retain such information and the types of security safeguards that must be employed to bolster those policies.

---

[85] *See* FED. TRADE COMM'N, *Fair Information Practice Principles,* http://www.ftc.gov/reports/privacy3/fairinfo.shtm (last visited Mar. 30, 2012).

[86] DEP'T OF COMMERCE INTERNET POLICY TASK FORCE, *COMMERCIAL DATA PRIVACY AND INNOVATION IN THE INTERNET ECONOMY: A DYNAMIC POLICY FRAMEWORK* 25, *available at* http://www.ntia.doc.gov/files/ntia/publications/iptf_privacy_greenpaper_12162010.pdf (last visited Mar.30, 2012).

[87] *See* FTC Report, *supra* note 49, at ii.

[88] *See* Deven McGraw et al., *Privacy as an Enabler, Not an Impediment: Building Trust Into Health Information Exchange*, 28 HEALTH AFFAIRS 416, 417-18 (2009), http://content.healthaffiars.org/content/28/2/416.full.pdf+html.

[89] *See* FTC report, *supra* note 49, at 7.

Within a health care context, these principles together serve to promote transparency about data policies; clearly specify the permitted purposes for collection, use, and disclosure of health information and then place limits on data flows consistent with these purposes; protect the quality, integrity, and security of information collected; and ensure accountability for compliance with data policies.

There are a number of formulations of the FIPPs for health data, all of which have similar characteristics; the following articulation is from the Markle Foundation's Connecting for Health Core Principles:

1. Openness and transparency: Consumers should be able to know what information has been collected about them, the purpose of its use, who can access and use it, and where it resides. They should also be informed about how they may obtain access to information collected about them and how they may control who has access to it.
2. Purpose specification: The purposes for which personal data are collected should be specified at the time of collection, and the subsequent use should be limited to those purposes, or others that are specified on each occasion of change of purpose.
3. Collection limitation and data minimization: Personal health information should only be collected for specified purposes and should be obtained by lawful and fair means. The collection and storage of personal health data should be limited to that information necessary to carry out the specified purpose. Where possible, consumers should have the knowledge of or provide consent for collection of their personal health information.
4. Use limitation: Personal data should not be disclosed, made available, or otherwise used for purposes other than those specified.
5. Individual participation and control: Consumers should be able to control access to their personal information. They should know who is storing what information on them, and how that information is being used. They should also be able to review the way their information is being used or stored.
6. Data quality and integrity: All personal data collected should

be relevant to the purposes for which they are to be used and should be accurate, complete, and up-to-date.

7. Security safeguards and controls: Reasonable safeguards should protect personal data against such risks as loss or unauthorized access, use, destruction, modification, or disclosure.
8. Accountability and oversight: Entities in control of personal health information must be held accountable for implementing these principles.
9. Remedies: Remedies must exist to address security breaches or privacy violations.[90]

HHS' Office of the National Coordinator has also endorsed a similar articulation of the FIPPs in its Nationwide Privacy and Security Framework for Electronic Exchange of Individually Identifiable Health Information.[91] In doing so, it explained that "[a]doption of privacy and security protections is essential to establishing the public trust necessary for effective electronic exchange of individually identifiable health information. A common set of principles that stakeholders accept and support is the first step towards realizing those privacy and security protections and establishing the necessary public trust."[92]

In the above articulation of the FIPPs, and other commonly used iterations, the principle that individuals should have some choices about how their information can be accessed, used and disclosed is nested within just one or two of the FIPPs. In other words, FIPPs envision that individual consent or choice is but one aspect of a framework of privacy protection—not the linchpin for protecting

---

[90] CONNECTING FOR HEALTH: COMMON FRAMEWORK FOR NETWORKED PERSONAL HEALTH OVERVIEW AND PRINCIPLES, MARKLE, 4-5 (June 2008), http://www.markle.org/health/markle-common-framework/connecting-consumers/overview (last visited Mar. 30, 2012).

[91] *See* OFFICE OF THE NAT'L COORDINATOR FOR HEALTH IT, INFO. TECH., U.S. DEPT OF HEALTH & HUMAN SERVS., NATIONWIDE PRIVACY AND SECURITY FRAMEWORK FOR ELECTRONIC EXCHANGE OF INDIVIDUALLY IDENTIFIABLE HEALTH INFORMATION, 1, 3 (Dec. 15, 2008), *available at*: http://healthit.hhs.gov/portal/server.pt/gateway/PTARGS_0_10731_848088_0_0_18/NationwidePS_Framework-5.pdf. ONC acknowledged use of the Markle Common Framework principles (as well as other commonly used articulations of FIPPs) in developing its version. *Id*.

[92] *Id* at 6.

privacy.[93] The FIPPs instead place affirmative obligations on data holders to develop, implement, and be held accountable for specific limitations on the purposes for which information can be accessed, the amount of data that is needed to accomplish that purpose, and how long information can be retained.[94] Thus, the FIPPs place the burden of protecting personal information primarily on the holders of the information, instead of relying chiefly on individuals to understand and make appropriate choices about uses of their information.

2. Using the FIPPs to Adopt Specific Policies

The policy framework for uses of EHR data for quality analytics purposes should rely more extensively on the FIPPs and accountable data stewardship than is currently the case. Specifically, policies set forth in the Privacy Rule and in the Common Rule governing the use of EHR data for quality analytics should rely less on individual consent and instead require researchers to adopt and adhere to strict internal policies regarding data collection, use and retention. In addition, policies to govern use of EHR data for quality analytics should be consistent and eliminate the potential disincentive to sharing internal quality reviews to contribute to more general knowledge about health care quality.

In other words, policymakers should treat use of EHR data for quality analytics purposes as a routine use of information, not subject to specific requirements to obtain consent, as long as robust policies based on FIPPs are adopted and consistently followed. This approach is consistent with the federal Health IT Policy Committee's explicit recommendations that state that such uses should be treated as health care operations under the Privacy Rule,[95] as well as with recommendations from the Federal Trade Commission (FTC), which has proposed that consent not be required for the "commonly

---

[93] *See, e.g.*, *supra* Part IV.A.1.

[94] *Supra* Part IV.A.1.

[95] *See* Letter from Paul Tang, Vice Chair, HIT Policy Committee, U.S. Dep't of Health & Human Servs., to Farzad Mostashari, Nat'l Coordinator for Health Info,. Tech., U.S. Dep't of Health & Human Servs. (Oct. 18, 2011), *available at* http://healthit.hhs.gov/portal/server.pt/community/healthit_hhs_gov__policy_recommendations/1815.

accepted practices" of an entity.[96]

Here are some examples of robust policies based on FIPPs for quality analytics:

- The amount of data accessed for this purpose is only what is necessary to address the particular question, and "minimizing" data access should also apply to the identifiability of the data.[97]
- Access to the data for quality analytics purposes is limited to those participating in the research, and these limits are enforced through security protections like role-based access and authentication of identity.[98]
- Entities conducting quality analytics using EHR data (or making their data available for this purpose) engage in meaningful efforts to be transparent with the community they serve about the fact that they use data, or make it available, for quality analytics purposes.[99]
- Entities develop and implement systems to ensure internal accountability for compliance with these policies, and regulators play a stronger and more consistent oversight role.[100]
- The results of quality analytics are shared with the public only in a privacy protective way, such as through the reporting of aggregate results.[101]

Collectively, these policies and practices have the potential to drive deep and solid public support for use of clinical data in EHRs for quality analytics. Such an approach also leverages the broad trust that individuals place in their providers to protect the privacy and security of their health information;[102] such trust supports greater

---

[96] F.T.C., PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: A PROPOSED FRAMEWORK FOR BUSINESS AND POLICYMAKERS 53-56 (Dec. 2010), *available at* http://www.ftc.gov/os/2010/12/101201privacyreport.pdf.

[97] *See* Tang, *supra* note 93, at 5.

[98] *Id*.

[99] *Id*.

[100] *Id*.

[101] *Id*.

[102] *See generally, e.g.*, NAT'L. P'SHIP FOR WOMEN & FAMILIES, MAKING IT MEANINGFUL: HOW

reliance on a data stewardship approach to making patient data available for quality analytics (at least with respect to information in provider EHRs). Although not all of the FIPPs detailed above may be relevant to some researchers,[103] most can be used in such a way that they will translate into responsible data stewardship, and ultimately more widespread consumer confidence.

3. Potential Concerns to Address

Implementing the above recommendations will likely require policymakers and stakeholders to resolve at least three concerns: (1) eliminating the requirement to obtain consent, notwithstanding its weak privacy protection, may undermine public trust in quality research; (2) vesting trust in entities to adopt robust fair information policies and practices may not result in a consistent environment of responsible use of personal information, especially given the historically weak enforcement of Privacy and Security Rule protections by federal authorities; and (3) eliminating requirements to obtain consent when identifiable information is used for quality analytics may reduce the incentive to use a limited data set or de-identified data for this purpose.

a. Eliminating the Requirement to Obtain Consent

Eliminating the requirement to obtain consent will likely be met with considerable resistance, both by some policymakers and some data holders who are accustomed to thinking of consent as the linchpin of privacy. Longstanding legal precedent requiring consent for research uses of health information has resulted in widespread expectations that individuals will have the right to give consent for research uses of their health information. It will be exceedingly

---

CONSUMERS VALUE AND TRUST HEALTH IT, 29-38 (Feb. 2012), *available at* http://www.nationalpartnership.org/site/DocServer/HIT_Making_IT_Meaningful_National_Partnership_February_2.pdf?docID=9783; *see also* CAL. HEALTHCARE FOUND., CONSUMERS AND HEALTH INFORMATION TECHNOLOGY: A NATIONAL SURVEY, 19-24 (Apr. 2010), *available at* http://www.chcf.org/~/media/MEDIA%20LIBRARY%20Files/PDF/C/PDF%20ConsumersHealthInfoTechnologyNationalSurvey.pdf.

[103] For example, the requirement to provide individuals with access to copies of information about them or to provide a mechanism for correcting data may not be relevant to some researchers.

difficult to reorient public perception of what is seen as a key element of respect for individual autonomy and the right of individuals to have some control over information about them, particularly when that information is sensitive.

Regardless, if decreasing reliance on consent is perceived to be a radical departure from current policy and ethical norms, it may be all the more important to limit the application of this policy (at least initially) only to reviews of EHR data solely for purposes of quality improvement and not for other "research" uses. In addition, it will be critical for regulators to define, or at least provide some guidance on, what constitutes a use of health information for quality improvement purposes, so that this change in policy does not end up paving the way for inappropriate uses of patient data.[104] If additional guidance is provided by HHS on the scope of quality initiatives covered by this new policy, it may dampen criticism that eliminating consent to this research may subject to patient data to objectionable uses.[105]

The change may also be more palatable if it applies only in circumstances where the data holders—the entities typically trusted by the patient—retain control over the information.[106] As noted above, the Health IT Policy Committee, which provides advice on policy matters to the Office of the National Coordinator for Health Information Technology, also recommended that access to EHR data for quality improvement purposes be treated like a routine use – i.e., health care operations – but only in cases where the data holder

---

[104] Limiting the application of this policy also will allow policymakers and stakeholders to assess whether it is possible to extend this treatment to other important secondary uses of EHR data.

[105] Due to the limits of consent in protecting privacy, allowing individuals a choice about whether information about them may or may not be used for a particular quality initiative does not guarantee that an individual will be informed enough to object to a use to which he or she may object. Policymakers will also have to consider whether quality improvement activities, which arguably benefit all patients, are a use of data that patients should have the right to object to.

[106] The focus of control should be on control over decisions with respect to the data, and not necessarily physical custody. For example, a data holder could direct a contractor to perform quality analytics on EHR data. Consistent with the recommendations of this article, such contractor should be bound by FIPPs-based policies and monitored for compliance.

maintains control and stewardship over the data.[107] Further, to provide incentives for entities to contribute to the learning health care system, the regulatory approach recommended in this article should apply only in circumstances where the entity conducting the research shares or publicizes the results in a way that protects individual privacy.

If the requirement to obtain consent is eliminated, it will need to be replaced with vastly improved transparency to the public about how clinical information is used for quality improvement purposes.[108] It is critical that such education not take place solely through the Privacy Rule's Notice of Privacy Practices, as patients often do not read them and, when they do, frequently do not understand them.[109] More work will need to be done to develop and test creative and effective strategies for achieving greater public transparency about appropriate secondary uses of EHR data. It will be difficult to justify treating quality uses of EHR data as "routine" if the public is in the dark about them. As the Health IT Policy Committee has observed, "patients [ideally] should not be surprised" by uses of their health information.[110]

---

[107] *See* Letter from Paul Tang, Vice Chair, Health Info. Tech. Policy Comm., to David Blumenthal, Nat'l Coordinator for Health Info. Tech., Dep't Health & Human Servs. 9-10 (Sept. 1, 2010), *available at* http://healthit.hhs.gov/portal/server.pt/gateway/PTARGS_0_0_6011_1815_17825_43/http%3B/wci-pubcontent/publish/onc/public_communities/_content/files/hitpc_transmittal_p_s_tt_9_1_10.pdf.

[108] Studies show that individuals care a great deal about how their personal health information is collected and used. *See, e.g.*, CAL. HEALTHCARE FOUND., *supra* note 102, at 2-5, 7, 14, 30; *see also* Lucian L. Leape, *Perspective on Health Reform: Transparency & Public Reporting Are Essential for a Safe Health Care System*, THE COMMONWEALTH FUND, 3 (March 2010), http://www.commonwealthfund.org/~/media/Files/Publications/Perspectives%20on%20Health%20Reform%20Brief/2010/Mar/Transparency%20and%20Public%20Reporting/1381_Leape_transparency_public_reporting_Perspectives_brief.pdf. (March 2010).

[109] *See, e.g.*, Nathaniel Good et al., *Stopping Spyware at the Gate: A User Study of Privacy, Notice and Spyware*, 1, 8-9, Symposium on Usable Privacy and Security (SOUPS) (2005), http://cups.cs.cmu.edu/soups/2005/2005proceedings/p43-good.pdf; *see generally*, Priscilla Regan, *The Role of Consent in Information Privacy Protection, in* CONSIDERING CONSUMER PRIVACY: A RESOURCE FOR POLICY MAKERS AND PRACTITIONERS 24, 25 (Paula Bruening, ed., (2003).

[110] Letter from Paul Tang, *supra* note 107, at 4.

b. Trusting Entities to be Good Data Stewards

Relying more heavily on health care entities themselves to be responsible stewards of health information, however, could also have unintended consequences. Greater regulatory flexibility would require the public to trust health care entities to handle their data responsibly and consistently with the FIPPs discussed above, and further assumes that all of them are good actors. This is potentially problematic, as it means that one widely-publicized information breach or misuse could shatter this trust. The development of robust and reliable accountability mechanisms—both for compliance with the law and for implementation of robust FIPPs-based policies and practices—is paramount.

Policymakers could address this concern by limiting this policy's application to only those entities whose policies and practices have been objectively audited and determined to be robust and comprehensive. For example, in Ontario, under the province's Personal Health Information Protection Act (PHIPA)[111], so-called health information custodians (HICs) are "permitted to disclose personal health information *without consent* to 'prescribed persons or entities' that are prescribed by the legislation."[112] Such a designation requires that the person or entity "have in place practices, policies, and procedures to protect the privacy of individuals whose personal health information it receives and to maintain the confidentiality of such information."[113] Importantly, prescribed persons and entities must also make *publicly available* a description of the registry's functions[114] as well as a summary of its practices, policies and procedures. This significant focus on public transparency could mitigate concerns about eliminating consent requirements and is consistent with the above-recommended FIPPs. Other audit or accreditation models similar to this one could be explored as well.

---

[111] Personal Health Information Protection Act, S.O. 2004, c. 3 (Can.); O. Reg. 329/04 (Can.).

[112] Sharyl J. Nass et al., *Beyond the HIPAA Privacy Rule: Enhancing Privacy, Improving Health Through Research*, INSTITUTE OF MEDICINE 262 (2009) (emphasis added).

[113] *Id.*

[114] Such as those compiled or maintained for purposes of facilitating or improving the provision of health care. *See id.*

c. Reduced Incentive to Use Information Scrubbed of Identifiers

As noted above, the HIPAA Privacy Rule does not require consent for research using less identifiable data – specifically, a limited data set[115] or de-identified data.[116] This policy creates a strong incentive for researchers to use data in less identifiable forms, significantly reducing privacy risks. If all quality evaluations using EHR data are considered to be routine "operations," the incentive to use data in less-identifiable forms is largely removed, as operations may be conducted using fully identifiable health information without individual consent. To counter this concern, the FIPPs-based policies governing such secondary uses of EHR data need to emphasize the importance of using the "minimum necessary" amount of information needed to accomplish the desired purpose and interpret the data minimization (or "minimum necessary") requirement to apply to the degree of identifiability of the information.[117] In other words, consistent with current policy, consent is not required only in circumstances where data is used in the least identifiable form that will enable the research question to be addressed; the difference is that this approach is not limiting this treatment only to data that meets the definition of a limited data set or de-identification.

B. Promote Greater use of Decentralized, Distributed Networks

In light of the risks introduced by architectures that rely on copying and centralizing health information, policymakers should promote the use of distributed networks for quality analysis whenever possible. Distributed networks support the coordination of multiple, independent databases to meet a shared objective—such as analyzing database content for research purposes—without requiring the creation of a central data repository.[118] In a distributed

---

[115] 45 C.F.R. § 164.514(e).

[116] 45 C.F.R. § 164.514(a) (2010). Information that meets the HIPAA de-identification standard set forth in this provision is not individually identifiable health information; the Privacy Rule regulates only protected health information, which is individually identifiable health information that also meets other criteria. 45 C.F.R. § 160.202 (2010).

[117] *See* McGraw & Leiter, *supra* note 18, at 3-4.

[118] Jeffrey Brown et al., *Design Specifications for Network Prototype and Cooperative to Conduct Population-Based Studies and Safety Surveillance*, AGENCY FOR HEALTHCARE RESEARCH AND

network, the identifiable information remains under the stewardship of the data holder, and the analysis is executed on the relevant underlying data, either by the data holder, or, in the alternative, the data holder can retain the data but make it virtually accessible, such as through an edge server or a private, secure cloud.[119] This approach is commonly referred to as "bringing questions to the data" instead of bringing the data to the questions.[120]

This technical approach has the advantages of leveraging the trust that patients typically have in their health care providers and continuing to rely on data holders to be responsible stewards of information, common themes of the recommendations in this paper. There are additional, administrative benefits to employing distributed networks for quality analytics. They often require less time and money to establish, as they minimize data transfer and maximize the opportunities created by existing infrastructure.[121] Furthermore, distributed networks also can reduce the risk and severity of data breaches, as they minimize the number of copies of sensitive data sets in circulation.[122]

The FDA's Mini-Sentinel Project is piloting policies to govern the Sentinel Initiative, a national system for ongoing monitoring of drug safety and other medical products already on the market.[123] The project provides a model of a distributed, privacy-protective network for secondary uses.[124] Instead of gathering copies of health data into a central repository for safety analysis, entities participating in Mini-Sentinel maintain control of sensitive, identifiable health

---

QUALITY, July 2009, *available at*: http://www.effectivehealthcare.ahrq.gov/ehc/products/54/150/2009_0728DEcIDE_DesignSpecNetCoopPopSafety.pdf. *See also* Decentralizing the Analysis of Health Data, *supra* note 76, at 9.

119 *See also* Decentralizing the Analysis of Health Data, *supra* note 76, at 12.

120 W. Rishel, "Send the Questions to the Data," GARTNER BLOG NETWORK (July 7, 2011) *available at*: http://blogs.gartner.com/wes_rishel/2011/07/07/send-the-questions-to-the-data/.

121 *See also* Decentralizing the Analysis of Health Data, *supra* note 76, at 9.

122 Richard Platt et al., *The U.S. Food and Drug Administration's Mini-Sentinel Program,* 21 (S1) PHARMACOEPIDEMIOLOGY AND DRUG SAFETY 1, 19 (2012), http://onlinelibrary.wiley.com/doi/10.1002/pds.v21.S1/issuetoc.

123 *Id*. at 10.

124 *Id.* at 3, 7.

information.[125] These entities run safety queries against the health information in their records, and provide only summary or aggregate responses to a contractor working on the FDA's behalf. In addition, the entities themselves are required to comply with FIPPs-based policies governing their access to data for Mini-Sentinel purposes.[126] For example, Mini-Sentinel participating entities commit to limiting who has access to identifiable data and limiting the use of that data for Mini-Sentinel purposes only.[127] In addition, the results of a safety query are submitted to the FDA (and a contractor working on the FDA's behalf) in aggregate or de-identified form only.[128] The FDA also conducted regular outreach to the public on the status of the Sentinel Initiative, and the Mini-Sentinel Pilot, which contributed to greater public transparency.[129] The policies and careful design of the Mini-Sentinel Pilot laid the foundation for public trust in the use of health data for active safety surveillance.

Some researchers have raised concerns that distributed networks will not work for certain types of research.[130] Providers with EHRs may not have the capacity to perform research queries on their EHR data, and may lack the technical expertise or support necessary to enable virtual access. In some circumstances, the scope of the research – and the frequency with which the data may need to be accessed – may necessitate adoption of a model that provides researchers with their own copies of the data. HHS should explore the development of guidance or standards on which types of research are feasible using distributed networks and which are not.

---

[125] *Id.* at 3. The information has been put into a common data model, in order to ensure the research is conducted consistently across multiple sites.

[126] *Id*.

[127] *Id*. at 21.

[128] *Id*.

[129] *See generally* Press Release, FDA, FDA's Sentinel Initiative (Feb. 24, 2012), http://www.fda.gov/Safety/FDAsSentinelInitiative/ucm2007250.htm.

[130] *See* Rishel, *supra* note 120; CDT, supra note 56.

V. CONCLUSION

The imperatives of health care reform, and the desire to improve the health care system through robust quality analytics, require a rethink of current policies governing this particular secondary use of EHR data. Such policies should rely less on individual consent, given its tendency to provide weak privacy protection in practice and to insert hurdles to uses of EHR data for this important purpose, and instead place greater emphasis on strong data stewardship policies and practices and more consistent oversight by regulators. Quality analytics across multiple institutions should also take place using a distributed network technical architecture whenever possible.

The need for improved health care quality is urgent, so policy change regarding use of EHR data for quality purposes needs to occur promptly; yet policy change can take years to accomplish. Given that there will be a need for robust public dialogue about the changes proposed in this article – and other approaches that have been suggested to improve or streamline access to EHR data for quality analytics in privacy protective ways – HHS should consider piloting some of the more promising approaches. Achieving a more effective, high-functioning health care system must begin by learning what works to create and enable it.