64 STAN. L. REV. ONLINE 75
February 8, 2012

SYMPOSIUM ISSUE†

PAVING THE REGULATORY ROAD TO THE "LEARNING HEALTH CARE SYSTEM"

Deven McGraw*

The poor quality and high cost of health care in the U.S. is well documented. The widespread adoption of electronic medical records—for purposes of improving quality and reducing costs—is key to reversing these trends.[1] But federal privacy regulations do not set clear and consistent rules for access to health information to improve health care quality. Consequently, the regulations serve as a disincentive to robust analysis of information in medical records and may interfere with efforts to accelerate quality improvements. This Essay further explains this disincentive and suggests a potential regulatory path forward.

The U.S. has dedicated approximately 47 billion dollars to improve individual and population health through the use of electronic medical records by health care providers and patients.[2] Much of the funding for this initiative, enacted by Congress as part of the Health Information Technology for Economic and Clinical Health Act of 2009, will be used to reimburse physicians and hospitals for the costs of purchasing and implementing electronic medical record systems. The legislation also includes funding to establish infrastructure to enable health care providers to share a patient's personal health information for treatment and care coordination purposes and for reporting to public health authorities.

---

† The Privacy Paradox: Privacy and Its Conflicting Values.

* Director of the Health Privacy Project at the Center for Democracy & Technology.

1. *See* Melinda Beeuwkes Buntin et. al., *Health Information Technology: Laying the Infrastructure for National Health Reform*, 29 HEALTH AFFAIRS 1214-19 (June 2010).

2. KAISER COMM'N ON MEDICAID AND THE UNINSURED, FED. SUPPORT FOR HEALTH INFO. TECH. IN MEDICAID: KEY PROVISIONS IN THE AM. RECOVERY AND REINVESTMENT ACT (2009), *available at* www.kff.org/medicaid/upload/7955.pdf.

Federal policymakers also intend for electronic medical records to be actively used as tools of health system reform. The legislation directs the U.S. Department of Health and Human Services 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.[3] The 2011-2015 Federal Health Information Technology Strategic Plan identifies improving population health, reduction of health care costs, and "achiev[ing] rapid learning" as key goals of federal health information technology initiatives.[4] The vision is to create a health care system that leverages clinical information in electronic medical records to improve the knowledge base about effective prevention and treatment strategies, and to disseminate that knowledge more rapidly to clinicians and patients to improve the quality and efficiency of health care. In other words, the vision is to create a health care system that "learns" more quickly from both its successes and failures.

Achieving this learning health care system will require more robust access to clinical data contained in electronic medical records initially collected for individual treatment purposes. However, access to data for purposes beyond individual treatment (often referred to as "secondary" uses) raises health privacy concerns. Federal and state health privacy laws govern how entities within the health care system may collect, access, and disclose identifiable health information. These rules vary based on the purpose for which the information is being accessed or disclosed. For example, under the Health Insurance Portability and Accountability Act (HIPAA) privacy regulations (the Privacy Rule), the rules governing whether health care entities may access and disclose identifiable health information in order to treat an individual patient are fairly permissive.[5] By comparison, the ability to access this information to facilitate payment for care is more limited. For instance, providers may disclose only the "minimum necessary" amount of information needed to facilitate payment; this requirement does not apply to access and disclosure for individual treatment purposes.[6]

The Privacy Rule authorizes health care entities to access identifiable health information for secondary "learning" purposes in two main categories: health care operations and research. "Health care operations" is a broad category of largely administrative activities that includes "conducting quality assessment and improvement activities, including outcomes evaluation and de-

3. The Health Information Technology for Economic and Clinical Health Act of 2009, 42 U.S.C.A. § 300jj-11.

4. OFFICE OF THE NAT'L COORDINATOR FOR HEALTH INFO. TECH., FEDERAL HEALTH INFORMATION TECHNOLOGY STRATEGIC PLAN 2011-2015, *available at* http://healthit.hhs.gov/portal/server.pt?open=512&objID=1211&parentname=CommunityPage&parentid=2&mode=2.

5. *See, e.g.*, 45 C.F.R. § 164.502(a)(1) (2010).

6. 45 C.F.R. § 164.502(b) (2010).

velopment of clinical guidelines," as long as obtaining "generalizable knowledge" is not the "primary purpose" of any studies resulting from these activities.[7] In contrast, "research" covers activities "designed to develop or contribute to generalizable knowledge."[8] Thus, a key distinction between these categories is whether or not a primary purpose of the activity is to contribute to generalizable knowledge. Overall, 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 for the benefit of others to be "research."

There are fairly significant differences in the regulatory requirements for use of data for operations versus research, so whether a quality assessment and improvement activity is or is not intended to contribute to generalizable knowledge is a critical question. In general, research using identifiable health information requires specific authorization from the individual who is the subject of the information. There are some narrow exceptions to this requirement, and the requirement can be waived in certain circumstances by an entity's Privacy or Institutional Review Board.[9] (This Board is an internal committee tasked with reviewing, monitoring, and approving research on human subjects, including research on information gleaned from medical records.)[10] But the Privacy Rule allows entities to use health data for operations purposes without the need to obtain a patient's consent at the outset or to have the data use vetted, either externally or through internal entity governance.[11]

The federal Common Rule, which governs most research using identifiable health information that is supported by federal funding, also relies on this distinction. The Common Rule defines research as activity contributing to generalizable knowledge;[12] consequently, activity not contributing to generalizable knowledge is not regulated by the Common Rule. The Common Rule currently requires research on identifiable health information culled from electronic medical records to be approved by at least one member of an entity's Institutional Review Board (referred to as "expedited review"); the individual's specific consent also must be obtained, unless the Board waives that requirement.[13]

---

7. 45 C.F.R. § 164.501 (2010).

8. *Id*.

9. *See generally* 45 C.F.R. § 164.512 (2010).

10. *See generally* 45 C.F.R. §§ 46.102, 46.107-109 (2010).

11. 45 C.F.R. § 164.502(a)(1)(ii) (2010); 45 C.F.R. § 164.501 (2010); 45 C.F.R. § 164.512(i) (2010).

12. 45 C.F.R. § 46.102 (2010).

13. 45 C.F.R. § 46.110, 116 (2010). *See also* OFFICE FOR HUMAN RESEARCH PROTECTIONS, CATEGORIES OF RESEARCH THAT MAY BE REVIEWED BY THE INSTITUTIONAL REVIEW BOARD (IRB) THROUGH AN EXPEDITED REVIEW PROCEDURE, *available at* http://www.hhs.gov/ohrp/policy/expedited98.html, for categories of research eligible for expedited review.

In summary, when a secondary evaluation of treatment data from an electronic medical record qualifies as "research," with the results intended to be shared with others, the Privacy Rule and the Common Rule subject that evaluation to more regulatory requirements than one intended only for internal purposes. Researchers have identified the federal research regulations as a significant obstacle to accessing health information for secondary learning purposes.[14] If we want information in electronic medical records to be vigorously and meaningfully leveraged to create a learning health care system, imposing greater regulatory burdens in cases where the results will be shared with others could significantly undermine this goal.

The U.S. Department of Health and Human Services recently took preliminary steps to ease the Common Rule's research requirements, including those applying to research using information in electronic medical records. Earlier this year, the Department sought public comment on a proposal to eliminate the requirement that entities have at least one member of their Institutional Review Board formally vet and approve research using treatment data from electronic medical records. The Department proposed instead to require researchers to file a one-to-two page description of the research with that Board.[15] It also proposed to continue to require patient consent in circumstances where identifiable data from electronic medical records is accessed for research (the opportunity for waiver would still apply), but to streamline the consent process by allowing patients to provide a general, oral consent to having their information used for research.[16]

But will these proposed changes be sufficient to clear the path to greater—yet still responsible—use of data in electronic medical records to create a learning health care system? In comments submitted to the Administration, the Center for Democracy & Technology (CDT) promoted a different approach: consider secondary uses of electronic medical data to be "healthcare operations" whenever the following two criteria are met:

1. The uses involve assessing the quality and/or cost of care already provided to an individual or group of individuals (i.e., retrospective review of care delivered in the ordinary course of business); and
2. The uses are conducted under the stewardship and control of the data holder (the entity legally responsible for stewardship of the records).

Most importantly, these secondary uses should be treated as "health care operations" regardless of whether the entity intends (either from the outset or subsequently) to share the results with peers or the public, and regardless of whether the entity intends to produce "generalizable knowledge."

---

14. *See generally* SHARYL J. NASS ET AL., BEYOND THE HIPAA PRIVACY RULE: ENHANCING PRIVACY, IMPROVING HEALTH THROUGH RESEARCH, (Inst. of Med. 2009).

15. 76 Fed. Reg. 44512, 44517 (July 26, 2011).

16. *Id*. at 44519-20.

The idea is that health care entities should be expected to routinely access information in electronic medical records to analyze whether patients were treated effectively and efficiently, and then share any relevant learning from this analysis. Consequently, such activity should be regulated just like other routine health data uses.[17]

However, treating such uses of electronic medical records as "routine" does not obviate the need for providers to implement sound privacy and security policies and practices to govern these uses. Entities should be required to adopt a full complement of fair information practices (FIPs) (for example, specifying the purpose for which information is collected from electronic medical records and limiting the collection and use to the information strictly necessary to fulfill that purpose), and there should be a system of accountability (ideally better than what currently exists under HIPAA) to ensure this occurs. Although CDT recommends eliminating the requirement that entities use Institutional Review Boards to vet quality studies done using electronic medical record data, an entity could still decide to use this Board as a mechanism of internal accountability. In addition, any sharing of the results of quality reviews must be done in a way that protects individual privacy, such as through reporting only aggregate results and guarding against potential re-identification risks.

In implementing this approach, the following concerns may need to be further discussed and resolved:

- Greater reliance on health care entities to be responsible stewards of health information could backfire. The public may not be prepared to trust all health care entities to responsibly manage this regulatory flexibility. Mishandling of the public's trust by one health care entity could jeopardize the public's willingness to have sensitive medical information accessed by any entity for this purpose. Developing and implementing more reliable mechanisms for holding entities accountable for compliance with the law and implementing FIPs for all data uses and disclosures are critical.
- Individual consent is only one element of the FIPs and frequently provides weak privacy protection in practice, particularly when policies rely on consent without adequately implementing other FIPs. However, the moment where consent for research is sought from an individual often provides a valuable opportunity for transparency and education about secondary uses of their health information, an opportunity

17. This approach was also supported by the Health IT Policy Committee, a federal advisory body created by Congress in the 2009 legislation. *See* Letter from Deven McGraw, Chair, Health IT Policy Comm. 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. The author was appointed to the Health IT Policy Committee by Health and Human Services' Secretary Kathleen Sebelius in 2009, and chairs the Committee's privacy and security subcommittee (commonly referred to as the "Tiger Team").

that would be lost if the requirement to obtain consent is eliminated altogether. (Although if consent is frequently waived in circumstances where electronic health record (EHR) data are accessed for secondary purposes, this teachable moment is largely theoretical.) At a minimum, policymakers should devote much more attention to considering how entities can be more transparent with individuals about secondary uses of health information in EHRs. The case for deeming quality reviews of EHR data to be "routine" is bolstered when such reviews are generally expected and supported by the public. Perhaps such secondary uses should be treated as routine operations only when the results are going to be shared with the public, or at least with the community served by the particular health care entity.

- The requirement to obtain consent also provides individuals with the opportunity to exercise some control over their health information and prevent uses and disclosures they might find objectionable. But requiring consent for routine uses of data is generally not recommended as a matter of privacy policy.[18]
- The Privacy Rule's requirements for research using health information that has been stripped of common identifiers are considerably more relaxed. For example, research using a limited dataset (from which sixteen categories of potential identifiers have been removed) can take place without the need to obtain an individual's authorization, as long as the data recipient executes an agreement that, at a minimum, includes a commitment not to re-identify the data.[19] The Privacy Rule does not regulate research on fully de-identified data.[20] The relaxed treatment of "anonymized" information creates strong incentives to use data in less identifiable forms, which significantly reduce the privacy risks. If all quality evaluations using EHR data are considered to be "operations," there are no incentives to use data in less identifiable forms, as operations may be conducted using fully identifiable health information without individual consent. Such concern may be mitigated by holding entities more accountable to using the "minimum necessary" amount of information for operations purposes (and of course, interpreting the Privacy Rule's existing minimum necessary standard to apply to the degree of identifiability of the information).

---

18. *See* FED. TRADE COMM'N, PRELIMINARY FEDERAL TRADE COMMISSION (FTC) STAFF REPORT: PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: A PROPOSED FRAMEWORK FOR BUSINESSES AND POLICYMAKERS 53-57 (Dec. 2010), *available at* http://www.ftc.gov/opa/2010/12/privacyreport.shtm.

19. 45 C.F.R. § 164.514(e) (2010).

20. 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).

The approach described above will need further discussion and refinement before it can be turned into viable policy. But the discussion could start with support for the concept that conducting quality assessments of electronic medical record data, and sharing the results in a privacy-protected way with others, should become a routine activity for all health care entities.