Bloomberg BNA

Medical Research Law & Policy Report®

Electronic Health Records Data and Secondary Use Research

By Nadine P. Peters Esq.

Introduction

An electronic health record (EHR) captures health data for treatment at the point of care but can also serve an important role for quality reporting, surveillance, and research. EHRs contain rich clinical and administrative health data from both primary and tertiary care health providers. They include data on efficacy, effectiveness, safety, and patient-level data such as dosing patterns and treatment combinations, making EHRs a valuable resource for a myriad of observational research studies.

The term ''secondary use'' is used in the industry to refer to using data for a purpose (i.e., research) other than the purpose for which the data were initially collected (e.g., treatment). Recent developments in health information technology and health information exchange have made it easier for researchers to harness the value of electronically collected and transmitted health data, presenting a unique opportunity. More specifically, with the expected widespread adoption of EHRs, secondary use research has the potential to generate research findings that are more generalizable to a diverse population, as well as improve understanding of disease processes and the impact that social and behavioral factors have on illness. Increased secondary use research will save time and resources, as data sharing will enable researchers to maximize use of an existing data set for multiple studies. This in turn will limit the time and cost of finding and recruiting potential research subjects.

As noted, the benefits of secondary use research are significant, and advances—such as better detection of areas of the country where certain diseases are increasingly prevalent—are within the public interest. However, the individual's privacy must be taken into consideration as well. Secondary use of identifiable health data collected for clinical or administrative purposes raises concerns of patient coercion or data misuse if proper safeguards are not in place. This article explores the current regulations governing the secondary use of data for research; the increasing need for an effective, comprehensive governing framework; and recent regulatory activity. While many issues still persist, there appears to be an emerging consensus on the general principles that should govern the secondary use of EHR data for research.

Nadine P. Peters is a partner with Hogan Lovells US LLP in Washington.

The author would like to thank Katherine M. Abramson for her assistance with the article.

The Legal Landscape of Secondary Use Research

In recent years, stakeholders and experts have sought to make the secondary use of health data a priority for U.S. policymakers with only limited success.[1] As a result, researchers are left to navigate a complex and often inconsistent set of regulatory standards because there are no laws or regulations specific to secondary use. In fact, the legal requirements that apply to a particular research study or project will depend on several factors, including the nature of the entities conducting the research and the source of funding. In many cases, secondary use research is very likely to involve two key sets of regulations—the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy

[1] Charles Safran et al., ''Toward a National Framework for the Secondary Use of Health Data: An American Medical Informatics Association White Paper,'' 14 *Journal of American Informatics Association* 1, 3 (February 2007).

 ISSN 1539-1035

Rule and the protection of human subjects regulations known as the Common Rule. The reason is that the entities conducting the research are themselves often covered entities subject to HIPAA requirements and/or institutions that receive federal funding subject to the Common Rule, or they obtain the data from such entities. Given the different scope of the regulations, there are important differences between the Privacy Rule requirements and the Common Rule requirements.

1. Privacy Rule

The HIPAA Privacy Rule does *not* govern research. Instead, it sets forth requirements for how covered entities may use and disclose protected health information (PHI) and the rights that they must afford to individuals about whom they maintain information.[2] A covered entity is either a (1) a health plan; (2) a health care clearinghouse; or (3) a health care provider who engages in electronic HIPAA standard transactions (e.g. claims for reimbursement, eligibility verification).[3] The vast majority of health care providers, particularly large institutions and academic medical centers, are HIPAA-covered entities.

The term ''protected health information'' is defined broadly as individually identifiable health information transmitted or maintained in any form—including electronically, via paper, or through oral communications—that: (1) relates to the past, present, or future physical or mental health or condition of an individual, providing health care to an individual, or the past, present, or future payment for providing health care to an individual; and (2) identifies the individual or where there is reasonable basis to believe the information could be used to identify the individual.[4] This very broad definition means that any individually identifiable health information about a subject maintained by a HIPAA-covered entity that has not been de-identified in accordance with the legal standard set forth in the HIPAA Privacy Rule qualifies as PHI.[5] For example, the mere presence of subject initials or a single date related to the subject (e.g., date of service) is sufficient to render information PHI.

When PHI is used or disclosed for research purposes, the Privacy Rule requires a valid prior written authorization from the subject.[6] The authorization given by the subject must be study- or protocol-specific. As such, a covered entity may not use or disclose PHI on the basis of a blanket authorization for future unspecified research, which is especially significant in the context of secondary use.[7] Under limited circumstances, the Privacy Rule permits a covered entity to use or disclose PHI for research without an authorization.[8] One such example is when a covered entity obtains proper documentation that an institutional review board (IRB) or Privacy Board has determined that specified criteria for waiver of the authorization requirement have been satisfied. In this case, the IRB or Privacy Board must determine that the following criteria are met: (1) use or disclosure involves no more than ''minimal risk'' to the privacy of individuals due to the presence of specified elements;[9] (2) research could not practicably be conducted without the waiver or alteration; and (3) research could not practicably be conducted without access to and use of PHI.[10]

2. Common Rule

The ''Federal Policy for Protection of Human Subjects,'' known as the Common Rule, applies to research conducted by most federal agencies, as well as federally funded research by nonfederal institutions. In addition, most institutions that accept federal funds sign an agreement (known as a Federal Wide Assurance, or FWA) to adhere to Common Rule restrictions in all research, regardless of funding source.[11]

For any research involving human subjects (which includes research using individually identifiable data) that is subject to the Common Rule, researchers must ''obtain the legally effective informed consent of the subject or the subject's legally authorized representative''[12] unless an IRB determines that specified waiver criteria have been satisfied.[13] Through the informed consent process, researchers must provide research subjects with a description of the study and of its anticipated risks and/or benefits, and a description of how the confidentiality of records will be protected. The Common Rule is designed more to address clinical trials than data research, and thus focuses primarily on protecting human subjects from physical risks, rather than informational risks.

3. The Tension Between the Privacy Rule and Common Rule

The authorization required by HIPAA and the informed consent required by the Common Rule clearly serve different purposes, and the varying requirements can create significant hurdles for covered entities and

[2] See generally 45 C.F.R. Parts 160 and 164.
[3] 45 C.F.R. § 160.103.
[4] Id.
[5] 45 C.F.R. §§ 164.514(b)(1) and (2).
[6] 45 C.F.R. § 164.508(a)(1).
[7] 67 Fed. Reg. 53182, 53226 (Aug. 14, 2002).
[8] Any state law that is more protective of patient privacy is not preempted by HIPAA, so state law may preclude researchers from seeking a waiver of authorization in some cases.

[9] The determination of ''minimal risk'' must be based on a finding that at least the following three elements are present (i) an adequate plan to protect personal identifiers from improper use and disclosure; (ii) an adequate plan to destroy such identifiers at the earliest opportunity consistent with the conduct of the research (unless there is a health or research justification for retaining the identifiers or if retention is otherwise required by law); and (iii) adequate written assurances that the identifiable health information will not be reused or disclosed to any third party except as required by law, for oversight of the research project, or for other research for which the use or disclosure would be permitted by the Privacy Rule. 45 C.F.R. § 164.512(i)(2)(ii).
[10] 45 C.F.R. § 164.512(i).
[11] As a result, research performed at academic medical centers is generally subject to the Common Rule.
[12] 45 C.F.R. § 46.116; 21 C.F.R. § 50.20.
[13] The Common Rule permits an IRB to waive some or all of the elements of informed consent or to waive the requirement to obtain informed consent in certain circumstances, including when the IRB finds and documents that (1) the research involves no more than minimal risk to the subjects; (2) the waiver or alteration will not adversely affect the rights and welfare of the subjects; (3) the research could not practicably be carried out without the waiver or alteration; and (4) whenever appropriate, the subjects will be provided with additional pertinent information after participation. 45 C.F.R. § 46.116(d).

  MRLR ISSN 1539-1035

researchers.[14] Most importantly, an ''authorization'' under the Privacy Rule must be study-specific. In contrast, an ''informed consent'' under the Common Rule may cover use of information for future unspecified research provided that the future research uses are described in sufficient detail to allow an informed consent, as determined by the IRB.[15] In addition, while the HIPAA authorization is a legal instrument that sets forth terms under which a HIPAA covered entity may use and disclose PHI about the subject, U.S. Department of Health and Human Services (HHS) guidance has suggested the Common Rule's informed consent is more of a ''teaching tool'' that educates the patient about the risks and benefits of the research.[16] HHS has recently stated its intention to harmonize these rules, which is discussed further below.

Unprecedented Opportunity

The passage of the Health Information Technology for Economic and Clinical Health (HITECH) Act has made it increasingly important to create an efficient, comprehensive framework governing the secondary use of data for research. The HITECH Act was enacted in February 2009 as part of the American Recovery and Reinvestment Act of 2009 (ARRA).[17] The HITECH Act includes a number of provisions aimed at improving health care quality and efficiency, and one of its main goals is to foster ''meaningful use'' of certified EHR technology.

The HITECH Act established incentive payment programs for eligible physicians and hospitals to encourage greater use of EHRs. Title IV of HITECH provides incentive payments through Medicaid and Medicare to those who adopt and use EHRs and will begin penalizing doctors who do *not* achieve meaningful use of EHRs starting in 2015. The HITECH Act specified three requirements for meaningful use: (1) using certified EHR in a meaningful manner (such as e-prescribing); (2) using certified EHR technology in a manner that provides for electronic exchange of health information to improve the quality of care; and (3) using certified EHR technology to submit clinical quality measures and other measures determined by the HHS Secretary.[18] The Centers for Medicare & Medicaid Services has since put in force regulations that provide more detail as to what eligible professionals and hospitals must do to qualify for meaningful use funds.[19] As more clinicians adopt EHRs through these incentives, there will be a dramatic increase in the breadth and depth of information available for secondary use.[20]

In addition to encouraging greater use of EHRs, the HITECH Act introduced other programs intended to foster the adoption of health information technology and electronic health systems. The Strategic Health IT Advanced Research Projects (SHARP) program is one such HITECH incentive program.[21] One of the stated goals of the SHARP program is to foster the responsible secondary use of health data, and to create a unified EHR framework that will allow for the dynamic exchange of patient information among health care providers, government agencies, insurers, and other stakeholders. It is thus becoming increasingly important that the broader societal value that can be derived from EHR data be maximized through the adoption of sound, transparent governance policies to enable secondary use research. To that end, there have been a number of recent developments of note.

Recent Developments

As a result of the recent focus on the opportunity to improve health care through the advancement of secondary use of EHR data for research, HHS has taken several steps to revisit the regulatory framework created by the Common Rule and the Privacy Rule.

1. *Proposed Modifications to Regulations*

a. HITECH Notice of Proposed Rulemaking

In the July 2010 HITECH Notice of Proposed Rulemaking (the Proposed Rule), HHS indicated that it is considering permitting a HIPAA authorization to cover future unspecified research studies, and thus harmonizing it with the Common Rule.[22] The Privacy Rule was originally drafted to require that authorizations for research be ''study specific'' due to HHS's concern that patients could lack necessary information in the authorization to make an informed decision about the future research.[23] At the time, HHS also noted that uses of PHI for future research need not always require the entity to re-contact the individual (i.e., in cases where the criteria for obtaining an IRB waiver of authorization are satisfied).[24] In its 2010 Proposed Rule, however, HHS noted that it received numerous comments that the restriction on future research encumbers secondary use research and results in individuals being re-contacted multiple times in the future to sign multiple authorization forms.[25] Furthermore, HHS noted that there was widespread concern about the divergence between the Privacy Rule and the Common Rule, and several commenters (including the Institute of Medicine) urged HHS to allow the HIPAA authorization to permit future research use. HHS is now considering whether the Privacy Rule should permit an authorization to disclose PHI for future research purposes and how these authorizations should be scripted. HIPAA authorizations that

[14] The differences were brought to HHS's attention in the context of tissue repositories. ''Tissue Repositories: the Common Rule and the HIPAA Privacy Rule,'' Department of Health and Human Services, July 2008, http://www.hhs.gov/ohrp/sachrp/mtgings/mtg07-08/present/markrothstein.html.

[15] 75 Fed. Reg. 40868, 40894 (July 14, 2010).

[16] E.g., ''Tips on Informed Consent,'' Office for Human Research Protections, March 16, 1993, http://www.hhs.gov/ohrp/policy/ictips.html.

[17] Health Information Technology for Economic and Clinical Health (HITECH) Act, Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009 (ARRA), Pub. L. No. 111-5 (Feb. 17, 2009) (hereinafter HITECH).

[18] ''Medicare and Medicaid: EHR Incentive Program,'' Centers for Medicare & Medicaid Services (2010), https://www.cms.gov/EHRIncentivePrograms/Downloads/MU_Stage1_ReqOverview.pdf.

[19] 42 C.F.R. Part 495.

[20] Safran, supra, note 1, at 2.

[21] ''Strategic Health IT Advanced Research Projects (SHARP) Program,'' Office of the National Coordinator for Health Information Technology, April 27, 2011, http://healthit.hhs.gov/portal/server.pt?open=512&mode=2&objID=3128&PageID=20708.

[22] 75 Fed. Reg. at 40894.

[23] Id. at 40893.

[24] Id.

[25] Id.

allow the use of PHI for future research would foster more efficient and flexible secondary use of EHR data.

b. Human Subjects Research Advanced Notice of Proposed Rulemaking

Another notable development is HHS's effort to update and enhance the Common Rule through its July 2011 Advance Notice of Proposed Rulemaking (ANPRM) titled ''Human Subjects Research Protections: Enhancing Protections for Research Subjects and Reducing Burden, Delay and Ambiguity for Investigators,'' which sets forth a great number of proposals and questions for consideration.[26] To harmonize federal oversight of human subjects research, HHS proposes to extend the Common Rule to research that is not federally funded but which is conducted at a domestic institution that receives some funding for human subjects research from a Common Rule federal agency. In recognition of the fact that IRB review and oversight may not be the best way to address informational risk associated with data research (e.g., unauthorized disclosure of identifiable health information), HHS is considering establishing data security and information protection standards for research involving identifiable or potentially identifiable information.[27] These standards would be modeled on the HIPAA Security Rule and require implementing administrative, technical, and physical safeguards and data breach notification.

To further HHS's stated goal to ensure that the level of review is commensurate with the level of risk to human subjects, the ANPRM outlines a proposal to expand the categories of research exempt from IRB review and create a new category of ''Excused'' research. For example, research that involves the secondary use of data collected for other purposes, even if identifiable, would qualify for the Excused category, provided the individual results from the data analysis are not provided back to the individual subjects.[28] Under the current Common Rule, research involving secondary use of existing data qualifies for the exemption only if the sources of data are publicly available or if the researcher does not retain or record any identifiers.[29] Excused research would not need to undergo IRB review, but the researcher would have to file a brief form with the IRB. The proposed information security standards and new general written consent requirements would also apply. More specifically, HHS proposes that for secondary use research involving data initially collected for *non-research* purposes (e.g., treatment data in an EHR), written consent would be required only if the data are identifiable.[30] In contrast, for secondary use research involving data initially collected for other *research* purposes (e.g., clinical trial data), written consent would be required whether the data are identifiable or not.[31]

HHS suggests that this general written consent could allow for broad future research and could be broad enough to cover all data collected at any time by the institution conducting the research;[32] however, requiring general written consent for research using existing data that have been de-identified is a notable change from existing permitted practice. It is likely to chill the type of secondary use research involving de-identified data that is prevalent today, such as epidemiological studies and comparative effectiveness research.

Taken together, these proposals to allow individuals to consent to future research uses of data under both the Common Rule and the Privacy Rule in theory have the potential to advance the goal of greater secondary use research while protecting the privacy of subjects. However, there is also great potential to further hamper secondary use research because a general consent form, as proposed in the ANPRM, would permit the subject to decline participation in all future research at the outset (e.g., upon the first treatment encounter) even for projects involving strictly de-identified information (in the case of research data). The Institute of Medicine (IOM) reports that the vast majority of Americans believe health research is valuable and are interested in health research findings,[33] but the public may not be fully aware of the need to share their clinical data in order to advance research and medical science. Further, in a study of the HIPAA Privacy Rule and its impact on research, the IOM concluded that a general consent requirement can introduce bias into research and lead to invalid results because of inherent differences in the individuals that do or do not grant consent.[34] For these reasons, among others, the recent regulatory proposals do not resolve many of the issues identified by the research community but they are prompting needed public discussion among stakeholders.

2. *Federal Privacy & Security Tiger Team Recommendations*

For instance, there have already been policy developments in response to these regulatory proposals focusing on harmonization and protecting individual privacy. On Sept. 14, the HIT Policy Committee, Privacy and Security Tiger Team workgroup (''Tiger Team'') presented draft recommendations to the full committee that address the gaps in the ANPRM and further aim to establish a workable framework for the secondary use of EHR data for research purposes. The Tiger Team noted that the ANPRM did not change the definition of ''research,'' and suggested that a revised definition would serve the interests of both patients and providers. The Common Rule and HIPAA similarly define ''research'' as activities designed to develop or contribute to ''generalizable knowledge''[35] and as a result of this broad definition, the use of EHR data by provider entities for evaluative activities requires consent or IRB waiver in many cases if results are publicized.

The Tiger Team advocates that the use of provider entities' EHR data for ''treatment purposes or to evalu-

[26] 76 Fed. Reg. 44512 (July 26, 2011).
[27] Id. at 44514.
[28] Id. at 44519.
[29] 45 C.F.R. § 46.101(b)(4).
[30] 76 Fed. Reg. at 44519.
[31] HHS does not specify why it distinguishes between data initially collected for non-research purposes and data initially collected for research purposes, but, as proposed, the potential burden would be less significant for secondary use of EHR data than it would for secondary use of clinical trial data because the EHR data initially are collected for treatment rather than research purposes.
[32] 76 Fed. Reg. at 44519.
[33] ''Beyond the HIPAA Privacy Rule: Enhancing Privacy, Improving Health Through Research,'' Institute of Medicine, 119-20 (2009).
[34] Id. at 35, 210-212.
[35] 45 C.F.R. § 46.102(d); 45 C.F.R. § 164.501

   ISSN 1539-1035

ate the safety, quality, and effectiveness of prevention and treatment activities''[36] should *not* be considered ''research.'' The Tiger Team emphasizes that a provider is expected to maintain proper oversight and be accountable for the conduct of these types of activities, and accordingly, consent should not be required to access EHR data for these purposes (even if the data are not a limited data set or de-identified). In support of this framework, the Tiger Team provided several examples of activities where, as long as the provider entity retains oversight and control of the data, consent need not be required:

- using EHR data to evaluate the effectiveness of care;
- identifying patterns of adverse events;
- evaluating interventions;
- monitoring individual clinicians and professional staff for adherence to existing standards of care; and
- evaluating outreach efforts (i.e. vaccinations).[37]

To further protect privacy, the Tiger Team advocates that research entities (particularly non-providers) adopt the full complement of fair information practices, including transparency, using the minimum amount of data necessary to accomplish the activity, and implementing security measures compatible with the perceived risk to privacy. While the ANPRM seeks comment on its proposed consent requirement for secondary use research, the Tiger Team advocates for a framework where the accountability of the entity conducting the research lessens the need to focus on consent. Notably, the Tiger Team concluded that ''most patients won't understand the difference between a [HIPAA] 'covered entity' and a 'research entity,' but will expect the same privacy and security standards applied to their data.''[38] As a result, the Tiger Team expressed support for the ANPRM proposal to require researchers to implement security and information protection standards. These recommendations subsequently were adopted by the HIT Policy Committee and released in a comment letter to the National Coordinator for Health Information Technology on Oct. 12, 2011. Additionally, the HIT Policy Committee indicated that it planned to submit the same recommendations to HHS as comments to the ANPRM.

3. *Gaining Further Clarity on De-Identification*

It seems unlikely that the patient consent issue will be settled in the near term, which shifts focus to the potential value of using de-identified EHR data for research. New evidence suggests technology can almost fully reduce the risk of re-identification of health data that have been de-identified in accordance with the safe harbor method under HIPAA,[39] which should alleviate many privacy concerns. A recent study, undertaken for the HHS Office of the National Coordinator for Health Information Technology (ONC),[40] revealed a relatively low chance that any particular record in a HIPAA safe harbor de-identified data set can be correctly re-linked to a person. The study assessed whether de-identified data could be combined with readily available outside data to re-identify patients, and the study found that it was able to accurately re-identify only 0.013 percent of the individuals.[41] Despite this evidence, an opposing line of research suggests that a framework in which patients perceive a lack of control over their health data can have adverse outcomes, such as patients limiting the amount and type of health information they disclose or forgoing treatment.[42] It is also important to note that the HITECH Act required HHS to issue guidance on methods for de-identification of PHI as designated in the Privacy Rule.[43] In response, HHS organized a public, in-person workshop in March 2010 to collect stakeholder views regarding de-identification approaches, best practices for implementing and managing the current de-identification standard, and potential changes to address policy concerns.[44] HHS is expected to synthesize the input and publish the guidance; it is hoped it will enable increased reliance on de-identified data for meaningful research.

Conclusion

Even with a renewed focus by the federal government and stakeholders to address the challenges preventing more prolific secondary use research, many key questions persist, including:

- To what extent would mandating fair information practices (including security safeguards and greater transparency through measures like required breach notification) address patient privacy concerns associated with secondary use of EHR data for research?
- Can there be no consensus among stakeholders without a consent requirement for secondary uses of EHR data?

---

[36] Privacy and Security Tiger Team Recommendations, Health IT Policy Committee, Sept. 14, 2011, http://healthit.hhs.gov/portal/server.pt/community/healthit_hhs_gov__policy_past_meetings/1814.

[37] Id.

[38] Id.

[39] Data may be de-identified for HIPAA purposes by only two methods: (1) the covered entity must remove 18 specified identifiers and have no actual knowledge that the information could be used alone or in combination with other information to identify an individual (''safe harbor method'') or (2) a statistician must certify that the risk is very small that the information could be used alone or in combination with other reasonably available information by an anticipated recipient to identify an individual who is the subject of the information (''statistician method''). See 45 C.F.R. § 164.514(b).

[40] Deborah Lafky, ''The Safe Harbor Method of De-Identification: An Empirical Test,'' Department of Health and Human Services, Oct. 8, 2009, http://www.ehcca.com/presentations/HIPAAWest4/lafky_2.pdf.

[41] The study took 15,000 patient records that had been de-identified in accordance with HIPAA, and attempted to match these records with identifiable records in a commercially available repository, and conducted manual searches through external sources. Id.

[42] ''Privacy and Confidentiality in the Nationwide Health Information Network,'' National Committee on Vital and Health Statistics, June 22, 2006, http://www.ncvhs.hhs.gov/060622lt.htm.

[43] HITECH § 13424(c).

[44] See ''Workshop on the HIPAA Privacy Rule's De-Identification Standard,'' Department of Health and Human Services, March 19, 2010, http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/De-identification/deidentificationworkshop2010.html.

- Is provider entity oversight and accountability sufficient to protect individuals from inappropriate uses of their EHR data?
- How should the term ''research'' be defined?
- Would the imposition of penalties for unauthorized re-identification of data by a researcher lead to greater support of secondary use of de-identified data without obtaining consent?

Sustained engagement by all stakeholders will be essential to moving forward. There is a lot at stake, as there are tremendous advantages to resolving these issues and implementing a workable governing framework. Secondary use of EHR data for research provides insight into the delivery of health care that cannot be addressed through existing static databases. Such research enables better analysis of health outcomes, quality, and safety measures and can expand our understanding of therapies or interventions on disease progression. Also, secondary use research can significantly improve the public health care system by facilitating early detection of emerging epidemics and bioterrorist threats.[45] In summary, a governing framework that enables broad secondary use of EHR data for research while providing for appropriate safeguards, transparency, and accountability has the potential to improve patient care, predict public health trends, and reduce health care costs. Progress toward implementing such a framework should thus be a priority for all stakeholders including government, the research community, and patient groups.

[45] Safran, supra note 1, at 2.

   ISSN 1539-1035