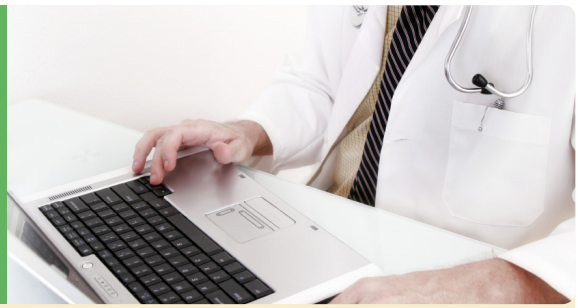
AcademyHealth

Legal and Policy Challenges to Secondary Uses of Information from Electronic Clinical Health Records



The Health IT for Actionable Knowledge project examines the experiences of six large health care systems that have used data from electronic health records and other information technology to conduct research and analysis related to health care delivery. This document is one of five reporting the results of this AcademyHealth initiative. Each report draws on examples from these early-adopting health systems to explore a range of issues relevant to the conduct of health services and other research using electronic clinical data. The six health system partners in this effort are Denver Health, Geisinger Health System, Kaiser Permanente, the New York City Department of Health and Mental Hygiene's Primary Care Information Project, the Palo Alto Medical Foundation Research Institute, and the Veterans Health Administration. AcademyHealth gratefully acknowledges the generous support of the California HealthCare Foundation in funding this project, and the U.S. Agency for Healthcare Research and Quality (AHRQ) for providing seed funding.

Summary

In order to achieve a learning health care system in which quality and effectiveness of health care are improved as costs are lowered, leveraging electronic health record data for purposes beyond treatment and payment will need to become easier and more widespread. This paper explores the current legal and policy challenges associated with secondary use of electronic clinical data, including those inherently relying on Institutional Review Board (IRB) review, and discusses a number of strategies that early health IT-adopters have employed to address them. The paper closes by noting potential changes to federal research rules that could ease restrictions on research in the future and by raising one additional policy challenge – support for health services research infrastructure – that, if unresolved, could create obstacles to further progress.

Introduction

Over the next five years, the federal government will invest an estimated $47 billion to promote the adoption and use of electronic medical records by health care providers.[1] The bulk of this investment is in Medicare and Medicaid incentives for certain health care professionals and health care institutions to adopt and use certified electronic health record (EHR) technology. However, both federal and state tax dollars are also funding the development of infrastructure to support the electronic exchange of health information.

The initial phase of these investments is focused largely on the use of EHRs for individual treatment purposes and for reporting to public health agencies. However, policymakers have also identified the goal of creating a learning health care system and more robustly using information initially collected in EHRs for treatment purposes to improve health care quality and effectiveness and reduce—or at least rationalize—costs. For example, in the Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH), the legislation authorizing the EHR-related investments, Congress directed the Office of the National Coordinator for Health Information Technology (ONC) to develop a "nationwide health information technology (health IT) infrastructure" that "improves quality, reduces medical errors, reduces health disparities, and advances the delivery of patient-centered medical care…reduces health care costs," and "facilitates health and clinical research and health

care quality."[2] In its health IT strategic plan, ONC identifies a key goal as "achieving rapid learning and technological advancement."[3] Consequently, there is an expectation that information in EHRs will be accessed also for secondary learning purposes.

Though the numbers of providers investing in EHRs is expanding rapidly due to these federal investments, several early health IT-adopting health systems have already discovered many challenges (and some promising practices) associated with leveraging electronic clinical data for purposes beyond treatment and payment. Among the challenges are legal and policy issues related to the access, use, and disclosure of EHR data for purposes of improving health care quality, safety, effectiveness and efficiency. In fact, all partner organizations participating in the Health IT for Actionable Knowledge project made reference to these challenges during the course of site visits and other meetings. Not surprisingly, similar challenges also have been raised by the Institute of Medicine (IOM)[4] and most recently by the federal Department of Health and Human Services (HHS) and the Office of Science and Technology Policy.[5]

In brief, the main legal and policy challenges include, though are not limited to:

- Lack of clarity regarding which federal laws govern secondary uses of EHR data;
- Reliance on IRBs, each of which adopts its own internal policies, especially in cases of multi-site research studies;
- Maintaining some organizational control or stewardship over data while at the same time making it available for secondary purposes; and
- Differences in state health information laws.

The paper provides examples of how some of the Health IT for Actionable Knowledge partners and their IRBs have addressed these challenges, and also notes some potential changes to laws and policies regarding research that may be on the horizon. In closing, the paper raises a potential additional policy challenge: support for health services research infrastructure that, if unresolved, could create obstacles to further progress.

Current Legal Framework

HIPAA and the Common Rule

When it comes to uses of health information, the two most relevant federal laws are the Health Insurance Portability and Accountability Act (HIPAA) and the Common Rule. The HIPAA Privacy Rule permits "covered entities," which includes most health care providers and health care institutions, to access, use, and disclose identifiable personal health information, or "protected health information," for treatment, payment, and health care operations without the need to first obtain a patient's consent.[6] Included in the category of health care operations is the performance of quality assessment and improvement activities, as long as the primary purpose of such activity does not to contribute to "generalizable knowledge."[7] The intent to contribute to generalizable knowledge, not the specific methods or tests applied to the data, is the true test of whether an activity is research.

The Common Rule covers only research conducted with the support of federal funding from certain agencies including, among others, HHS, the Department of Veterans Affairs and the Department of Energy.[8] The Privacy Rule and the Common Rule each define research as "systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge."[9]

Application of Current Rules Governing Research on Identifiable Data

When an activity is considered "research," a number of specific legal provisions likely apply. 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 the exceptions or requirement for authorization is waived by an IRB or Privacy Board. The nature of secondary uses of EHR data makes it difficult or often infeasible to obtain prior consent or authorization of such use by the patients. Thus, the challenge is to determine when authorization is required, and if so, whether the need for individual patient authorization can be waived. (In general, the term "consent" is used to refer to the agreement of a subject to be in a research study, and "authorization" is used to refer to the agreement of a patient to allow the use of his or her protected health information under HIPAA).

The following types of research using identifiable health information do not require prior patient authorization:

- Review of information in order to prepare for research, such as generating a research question or hypothesis, as long as the information does not leave the covered entity;
- Research on persons no longer living;[10] and
- Research using a "limited data set."[11] (As explained in more detail below, a limited data set is information stripped of specific categories of identifiers).

In addition, an IRB or Privacy Board can waive the requirement for authorization where (1) the research raises minimal risk to privacy, (2) the research could not practicably be done without a waiver, and (3) the research could not practicably be conducted without the identifiable health information.[12] Research raises "minimal risk" to privacy when (1) an adequate plan is in place

to protect the information from improper use or disclosure, (2) there is an adequate plan in place to destroy identifiers, and (3) written assurance is provided that the identifiable information will not be disclosed further than identified in the waiver.[13]

Generally, when authorization is required (i.e., it does not meet an exemption or is not eligible for a waiver), it must be in writing and include the following information:

- 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 use and/or disclosure of the information.[14]

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 is not part of a research protocol.[15] However, HHS recently proposed allowing more general consent for use of identifiable information for all research purposes and allowing compound authorizations in some circumstances.[16]

Under the Common Rule, research using identifiable data originally collected for other, non-research purposes (such as treatment) is subject to similar regulations. 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 IRB chairperson or by one or more experienced reviewers designated by the chairperson from among members of the IRB.[17] The patient's consent is also required if the researcher is receiving identifiable information.[18]

Such consent can be waived by the IRB in circumstances somewhat similar to those for a waiver of authorization under HIPAA: (1) the research involves no more than minimal risk, (2) the waiver will not adversely affect the rights and welfare of the patients, (3) the research could not practicably be carried out without the waiver, and (4) when appropriate, the subjects are provided with additional pertinent information after participation.[19] As discussed in more detail below, HHS recently announced some potential changes to the Common Rule; such changes would potentially make all research on identifiable EHR data collected for non-research purposes exempt, even if identifiers are provided to the researcher, but patient consent would still be required for such studies.[20] HHS is also considering making such consent more "flexible" and easier to obtain.[21]

Although the Common Rule does not require full IRB approval of research using treatment data, many institutions require such review as a matter of practice (see discussion of particular responses from a number of Health IT for Actionable Knowledge partners below).

Rules Governing Research 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 less regulatory oversight. HIPAA has two categories of datasets that can be used for research purposes and are subject to less – or no – regulation.

- A limited data set may be used by covered entities or contractors (business associates) acting on their behalf, for health care operations, research, and public health purposes.[22] To qualify as a limited data set, the information must be stripped of 16 categories of identifiers, including name and specific address. (Dates such as birth date and dates of health care services may be included).[23] Uses of a limited data set do not require the patient's consent; however, the data provider and the data recipient (often the researcher) must enter into a data use agreement describing the permitted uses of the data and prohibiting the data from being re-identified.[24]
- Data that qualifies as "de-identified" under the HIPAA Privacy rule is not subject to further regulation, and can be accessed, used, or disclosed for any purpose.[25] The Privacy Rule sets forth two methodologies for achieving the legal standard for de-identification, which is "no reasonable basis to believe that the information can be used to identify an individual."[26] Under the Safe Harbor method, 18 specific categories of identifiers must be removed, including elements of dates (other than year),[27] which often makes this methodology difficult for researchers to use, as dates are often critical for health services research. Those seeking to de-identify data can also use the statistical methodology, which requires that a qualified statistician attest that the data has been sufficiently "anonymized," meaning that it raises very small risk of re-identification.[28] This is often the methodology used to de-identify data for research purposes, since dates are not per se required to be removed. Instead, various statistical and masking techniques are used to enable dates to be represented in the dataset while still achieving the standard of very small risk of re-identification.

When identifiable information is used with authorization or a waiver of authorization, 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; this standard applies to uses of information for operations and research purposes.[29] Although little guidance

has been issued on compliance with the minimum necessary standard by the HHS Office for Civil Rights, which has oversight over HIPAA regulations, some have suggested that the standard should apply to the identifiability of the data.[30]

As noted above, the Common Rule only applies to research using identifiable information.[31] Under the Common Rule, information is not identifiable "if the identity of the subject is not or may not be readily ascertained" by the researcher.[32] However, HHS is now considering adopting HIPAA Privacy Rule standards of identifiability.[33] Because information that is de-identified or less identifiable is subject to less regulation under HIPAA and the Common Rule, researchers often strive to access data that qualifies for more favorable treatment.

Issues and Concerns

Variable Interpretation of Federal Laws Governing Secondary Uses

As discussed above, the primary federal provisions governing use of data for secondary purposes 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, such as through publication, and information evaluation activities that are intended for internal use.

Not only is this distinction often difficult to make, but the laws leave a fair degree of room for interpretation on how to comply. This can pose a challenge for entities that have little experience in accessing their clinical data (or making it available for others to access) for secondary purposes and for those who may not yet perceive the value of making data available for secondary purposes. In an overabundance of caution, such organizations may choose not to make clinical data accessible for secondary purposes outside of their own internal quality improvement uses. However, many Health IT for Actionable Knowledge partners – having both more experience in making these determinations and in recognizing the value proposition – tend to err on the side of treating nearly all secondary uses of clinical information as research. As a result, it is the IRBs that tend to set determinative policy when it comes to the treatment of data for secondary purposes.

The trend toward treating all such secondary uses as research is magnified by the publication policies of academic journals, most of which require some evidence of IRB approval before results can be considered for publication.[34] As a result, even if institutions are conducting quality improvement (QI) activities that would not by law require IRB approval, or if investigators' projects involve entirely de-identified data thus not needing a waiver of authorization, the institution will itself require an IRB review as a matter of internal policy and to pave the way for publication.

Challenges Related to IRB Review…and Potential Solutions

Although new mechanisms for and approaches to data sharing may well be necessary now or in the near future, the current tendency for organizations to rely heavily on IRB review can often prove challenging. For example, when consent and/or authorization is required for research purposes, this could introduce the potential for selection bias in the research, as persons who agree to have their information used for research purposes often differ from those who do not.[35] In multi-site research studies, it is possible that consent could be required for use of information from one institution but not required in another due to differential interpretations of legal requirements and institutional policy.

Further, many institutions, such as Denver Health, have experienced frustrations with an IRB that focuses more on clinical versus health services research, given that the latter makes obtaining consent implausible. In other cases, researchers seeking to conduct research at multiple institutions have noted the difficulty of achieving approval from multiple IRBs, each of which has its own procedures, timelines, and standards of review.[36]

These IRB-related concerns, however, can be addressed successfully. Another project partner, the Palo Alto Medical Foundation Research Institute (PAMFRI), has developed a three-part framework to handle secondary data use: (1) send all proposed uses by its investigators through an IRB to protect its researchers' ability to respond to requests by journals; (2) create a limited data set that can be routinely accessed by information analysts without specific privacy officer approvals to generate de-identified project-specific research files eligible for an expedited exempt determination by the IRB; and (3) keep all data and analysis on servers behind a firewall or encrypted computers to address any concerns a loss or theft might entail a HIPAA breach. PAMFRI has devoted significant time and attention to establishing processes that enhance privacy and regulatory compliance in a way that minimizes research barriers. This organization and others are working to leverage their IRBs most effectively, working with them to make the process as easy and transparent as possible for all involved.

The issues stemming from multiple IRB reviews also can be addressed in part by creating a multi-institution, centralized IRB. For example:

- The Department of Veteran's Affairs (VA), which conducts a number of multi-site research projects, recently implemented a Central IRB to review such studies.
- In Colorado, information specific to health services research is reviewed by the Colorado Multiple Institution IRB (COIRB), which serves Denver Health, the Denver VA, the Colorado Prevention Center, the Children's Hospital, and the University of Colorado Hospital and Health Sciences Medical Center.

- The Kaiser Foundation Research Institute at the program (i.e., interregional) level within Kaiser Permanente provides legal and governance support for privacy, IRBs, intellectual property, and related issues to all regions as well as for inter-institutional research.

Organizational Models for Research

When considering whether or not to make data available for secondary purposes, data holders often express concern about losing control of information over which they have both legal and ethical obligations. Some organizations are more comfortable with research arrangements where the raw data can only be accessed internally, or behind institutional firewalls, with aggregate results shared externally. The organizations can maintain better control of uses of information, be more assured of compliance with applicable law, and decrease the probability that any sort of security or privacy breach will result in high-profile news stories. In such a case, the data holder must analyze the laws that apply to its use of identifiable health information, but typically the disclosure of the results takes place only via de-identified data, which triggers fewer regulatory hurdles, as noted above. Sending identifiable data to a centralized research database requires participants to comply with any rules (federal or state) that govern the disclosure of identifiable data for research purposes.

Some Health IT for Actionable Knowledge partners have employed distributed data models for research. For example, the New York Primary Care Information Project (PCIP) maintains all raw patient EHR data at the practices' offices and has no centralized data repository. Researchers have access to de-identified, aggregated "count" data, and only for a subset of priority data elements through queries of the individual practices.

Other partners have employed other techniques for managing data access. For example, in the VA Informatics and Computing Infrastructure (VINCI) firewalls are created for access to each separate database from a participating site, and data can only be accessed by certain users and for certain purposes. VINCI provides a robust, virtualized computing environment and serves most VA clinical data back to 2000 in a rationalized database. The computing power and databases available in VINCI create incentives for researchers to keep data in a central repository—a practice designed to minimize data loss. VINCI manages authorizations for data access through the Data Access Request Tool (DART), which was developed in collaboration with VA Information Resource Center (VIReC) and coordinates the processing of requests through various VA offices. Through directory permissions based on the DART authorization database, VINCI controls access to data, so only authorized users can access data for specific research projects under an active IRB protocol. This practice is designed to prevent researchers from accessing data for one project and then reusing data for multiple other projects without IRB approval. Finally, VINCI caches and randomly audits outbound data transfers to verify that patient data are not inappropriately transferred out of VINCI.

Other Health IT for Actionable Knowledge partners use a centralized data warehouse with a diversity of controls depending on the position and role of the end user. For example, at the Geisinger Health System, administrators, business analysts, and researchers can be granted differential levels of access through a common enterprise data warehouse, the Clinical Decision Intelligence System (CDIS). CDIS receives real-time data feeds from multiple sources, including the EHR. Data used for operations, improvement, and other business needs are managed behind a firewall. De-identified, analytic databases are created from CDIS as needed for research and used outside of the firewall.

Another way of handling certain data requests is to employ a so-called "honest broker" system, whereby an intermediary who has no direct interest or stake in the data creates linkages between data in separate databases and shares the de-identified results for analytic purposes. Geisinger has employed this method to link data between its health plan and clinical operations and between biobank samples and EHR information.

Dealing with Potential Variability in State Laws

We have already discussed the federal laws governing the use of health information, but providers are also responsible for complying with the state laws that govern their use of health information. Most states have health information privacy laws and laws that provide even greater protections for health information than the HIPAA rules are valid.[37] Some of these laws cover all health information; most state laws apply to certain sensitive categories of data, such as genetic information or HIV test results. In most cases, the laws apply only to identifiable information. For example, state laws that govern certain types of sensitive data may also be implicated – and consent required – when the research is using identifiable data in one of these sensitive categories.

When research is conducted at a single institution, or at institutions in one state, the institutions are aware of – and required to abide by – a consistent set of rules regarding uses of health information. However, when the research takes place across multiple sites, some institutions could face greater legal obligations with respect to research uses of data than others participating in the same study.

In distributed research networks, providers are expected to abide by their own state laws with respect to their access to data for research purposes. Typically, the identifiable data is analyzed behind the firewall, and only aggregate results are shared. In

such a situation, the fact that other research participants may be governed by different state laws is less of a problem. Participants are not required to comply with the laws of other states. However, in circumstances where separate institutions across states are pooling or centralizing identifiable data for secondary uses, the laws of any state where a participating institution is located may be implicated; thus, the activity may be governed by multiple state laws. The use of distributed networks, or research arrangements, where identifiable (or potentially identifiable data) remains behind institutional firewalls and only non- or less-identifiable data is shared may help ameliorate this challenge, particularly where state laws apply only to fully identifiable data.

Paths Forward

Is Help on the Way? The HHS Research ANPRM

HHS in July 2011, released an "Advanced Notice of Proposed Rulemaking" (ANPRM) on *Human Subjects Protections: Enhancing Protections for Research Subjects and Reducing Burden, Delay and Ambiguity for Investigators,*[38] intended to get early public feedback on some potential changes to key federal privacy regulations. The ANPRM indicates a desire on the part of regulators to respond to a changing health information environment and suggests ways to address a number of the challenges and ambiguities identified above. Specifically, the ANPRM proposes to: (1) expand the generic obligations for the secure handling of protected health information by research organizations, which allows for the elimination of project-specific IRB review of research on data collected in EHRs for treatment purposes; (2) replace IRB review with a simple 1-2 page registration requirement; (3) require patient consent or authorization in circumstances where identifiable data is accessed for research but streamline the consent process by allowing patients to provide a "general" consent to research; and (4) make clear that research involving de-identified data or a limited dataset may be done without IRB review or registration and without the need to obtain a patient's consent or reauthorization (as long as recipients of the data contractually agree not to re-identify).[39]

In many ways, the ANPRM recognizes that the success of health care reform will depend upon increased access to clinical information for secondary purposes, in addition to coordination of care across settings and across time, increased exchange of information with patients and caregivers, and computation of standardized measures of clinical quality. However, this emerging electronic exchange environment may create new challenges for balancing reliable access to clinical data with protection of patient privacy and respect for individual patient preferences regarding data use. The ANPRM is not a set of official proposals, but is instead a way for regulatory agencies to gather public input on some initial ideas for regulatory reform. Hence, it is too early to tell whether these recommendations will become official policy, and if so, whether they will have a significant impact in addressing the challenges identified in this paper.

In considering the changes proposed by the ANPRM, the Health IT Policy Committee, a federal advisory committee to the Office of the National Coordinator for Health IT (ONC) created by HITECH, took on the question of the utility of the current legal distinction between secondary data uses for internal quality improvement purposes and uses intended to contribute to generalizable knowledge. In recent recommendations officially submitted as public comments to the ANPRM, the Policy Committee noted that "the creation of a learning healthcare system will depend on more widespread dissemination of the results (in a way that safeguards individual privacy) of treatment interventions and evaluations of the health care system." Thus, "characterizing research as any evaluative activity that contributes to the 'generalizable knowledge' arguably no longer serves the interests of either patients or providers."[40]

Retrospective chart reviews for quality improvement purposes is a classic example of how this "health care operations versus research" question plays out in practice. When a health care organization looks back at patient charts to evaluate the quality of care provided – for example, examining whether the organization has been effective in delivering evidence-based care – the activity is regulated as a health care operation if the organization intends to use the results only for internal purposes. However, if the organization intends to share such results externally, under HIPAA and the Common Rule the activity would be regulated as research. The disparate treatment under the law of such reviews, which are or should be fairly routine, can become a fairly significant obstacle to developing a learning health care system. Whether the Policy Committee's recommendations to eliminate this disparity will achieve more support over time and result in further changes in policy is unclear.[41]

Question of Data "Ownership" and Support for Research Infrastructure

In discussions of barriers to secondary uses of health information, some have suggested that resolving the question of "who owns the data" in EHRs would help resolve the challenges associated with accessing health information for research or other secondary purposes. However, this isn't a particularly relevant question, as the issue of who owns health data in medical records is not a matter of federal law and is often not covered by state law.[42] Even in the few parts of the country where state law establishes who owns health data in medical records, ownership over data does not necessarily translate into an absolute right to grant or bar access to data.[43]

There is, however, a useful distinction to be made between the question of who owns data about a patient and who owns or controls the rights to a collection, especially a processed collection, of such data. Unless an entity is able to charge for the use of analytic files, it may underinvest in their production, which would undermine numerous health reform initiatives to systematically track, analyze and improve upon clinical outcomes. Significant effort – and arguably some intellectual property – is involved in making data available and useful for research purposes, and resources are necessary to support this effort. If the costs of developing and implementing a health services research infrastructure are not supported or able to be recouped, an entity may be less likely to invest the resources necessary to provide access to its electronic clinical data for valuable secondary purposes.

A full exploration of the challenge of ensuring financial support for health services research infrastructure is beyond the scope of this paper. However, one potential new obstacle is worth noting. A provision enacted by Congress in HITECH prohibits the unauthorized sale of protected health information by entities covered under HIPAA.[44] This restriction could become an obstacle to financial support for research infrastructure if it is not properly interpreted. The restriction does include an exception that allows some data holders (including health care providers and academic medical centers) to sell identifiable health information to researchers "if the price charged reflects the costs of preparation and transmittal of the data."[45] To ensure financial support for health services research using clinical information in electronic medical records, it is critical that support for infrastructure not be interpreted as a "sale" of data.[46]

Conclusion

The legal and policy challenges associated with conducting research using data from EHRs coupled with the challenges of dealing with IRBs can seem daunting, and often require effort to resolve. Health IT for Actionable Knowledge partners are currently demonstrating the approaches to successfully conducting research using EHR data while still remaining compliant with the law and effectively managing their legal risks.

The potential for changes in both HIPAA and the Common Rule governing research uses of EHR data provide some hope that simplification and clarification of research rules and processes may be on the horizon, which likely would reduce necessary reliance on IRBs. In the meantime, sharing of best practices and model institutional policies and approaches can help researchers and data holders navigate this sometimes tricky environment.

About the Authors:

Deven McGraw, J.D., M.P.H., L.L.M. is the Director of the Health Privacy Project at the Center for Democracy & Technology.
Alice Leiter, J.D., is the Director of Health IT Policy at the National Partnership for Women & Families.

Acknowledgements

AcademyHealth gratefully acknowledges the time and expertise provided to AcademyHealth in the preparation of this report by the researchers, clinicians, IT professionals, executives at the health systems participating in AcademyHealth's HIT for Actionable Knowledge project – Denver Health, Geisinger Health System, Kaiser Permanente, the New York City Department of Health's Primary Care Information Project, the Palo Alto Medical Foundation Research Institute, and the Veterans Health Administration. Any errors are AcademyHealth's.

Endnotes

1. "Federal Support for Health Information Technology in Medicaid: Key Provisions in the American Recovery and Reinvestment Act," Kaiser Family Foundation. Web. August 2009. Retrieved from http://www.kff.org/medicaid/upload/7955.pdf. Accessed on January 3, 2012.
2. Health Information Technology for Economic and Clinical Health Act of 2009, Pub. L. No. 111-5. 123 Stat. 227. (Feb. 17, 2005). Retrieved from: http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/hitechact.pdf.
3. The office of the National Coordinator for Health Information Technology. (2011, Nov. 4). The Federal Health IT Strategic Plan. Retrieved from http://healthit.hhs.gov/strategicplan
4. Nass, S., et al., 2009. Beyond the HIPAA Privacy Rule: Enhancing Privacy, Improving Health Through Research. Washington, D.C.: The National Academies Press. (Hereinafter "IOM Report").
5. Human Subjects Research Protections: Enhancing Protections for Research Subjects and Reducing Burden, Delay, and Ambiguity for Investigators. 76 Fed. Reg. 44512, 44513-14 (July 26, 2011).
6. Uses and disclosures of protected health information: general rules. 45 C.F.R. Sect. 164.502 (2010).
7. Definitions. 45 C.F.R. Sect. 164.501 (2010).
8. 45 CFR Sect. 46.101 (2010). We 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 Lee, B. (March 10, 2009). Science and Research: Comparison of FDA and HHS Human Subject Protection Regulations. Retrieved from http://www.fda.gov/ScienceResearch/SpecialTopics/RunningClinicalTrials/EducationalMaterials/ucm112910.htm, accessed on January 30, 2012.
9. Definitions. 45 C.F.R. Sect. 164.501 (2010), and Basic HHS Policy for Protection of Human Research Subjects. 45 C.F.R. Sect. 46, Subpart A (2010).
10. Uses and disclosures for which an authorization or opportunity to agree or object is not required. 45 C.F.R. Sect. 164.512(i)(1)(ii)&(iiii) (2010).
11. Other requirements relating to uses and disclosures of protected health information. 45 C.F.R. Sect. 164.514(e) (2010).
12. Uses and disclosures for which an authorization or opportunity to agree or object is not required. 45 C.F.R. Sect. 164.512(i)(2)(ii) (2010).
13. Ibid., Sect. 164.512(i)(2)(ii)(A) (2010).
14. Ibid., Sect. 164.508(c) (2010).
15. Ibid., Sect. 164.508 (b)(3) (2010).
16. Modifications to the HIPAA Privacy, Security, and Enforcement Rules Under the Health Information Technology for Economic and Clinical Health Act. 75 Fed. Reg. 40867, 40895 (Jul. 14, 2010).
17. Expedited review procedures for certain kinds of research involving no more than minimal risk, and for minor changes in approved research. 45 C.F.R. Sect. 46.110 (2010). See http://www.hhs.gov/ohrp/policy/expedited98.html for categories of research eligible for expedited review.
18. General requirements for informed consent. 45 C.F.R. Sect. 46.116 (2010).
19. Ibid., Sect. 46.116 (c-d) (2010). Consent can also be waived for certain research evaluating public benefit services or programs.
20. Human Subjects Research Protections: Enhancing Protections for Research Subjects and Reducing Burden, Delay, and Ambiguity for Investigators. 76 Fed. Reg. 44512, 44512-19 (July 26, 2011).
21. Ibid, 44519-20.

22. Other requirements relating to uses and disclosures of protected health information. 45 C.F.R. Sect. 164.514(e)(3) (2010).
23. Ibid., Sect. 164.514(e)(2) (2010).
24. Ibid., Sect. 164.514(e)(4) (2010).
25. Ibid., Sect. 164.514(a) (2010).
26. Ibid.
27. Ibid., Sect. 164.514(b)(2)(i) (2010).
28. Ibid., Sect. 164.514(b)(1) (2010).
29. Uses and disclosures of protected health information: General rules. 45 C.F.R. Sect. 164.502(b) (2010); Other requirements relating to uses and disclosures of protected health information. 45 C.F.R. Sect. 164.514(d) (2010).
30. Center for Democracy and Technology. (September 13, 2010). Letter to Georgina Verdugo. P.p. 21-22. Retrieved from http://cdt.org/comments/cdt-comments-hhs-proposed-rule, accessed January 30, 2012.
31. Definitions. 45 C.F.R. Sect. 46.102(f) (2010).
32. Human Subjects Research Protections: Enhancing Protections for Research Subjects and Reducing Burden, Delay, and Ambiguity for Investigators. 76 Fed. Reg. 44525 (July 26, 2011).
33. Ibid.
34. See, e.g., http://www.research.northwestern.edu/oprs/irb/faqs/index.html and http://www.unh.edu/research/human-subjects-faqs, accessed on January 30, 2012.
35. See IOM Report, p.p. 209-14.
36. Ibid., p.p. 224-27.
37. Congress dictated that HIPAA would preempt (or nullify) any conflicting or less protective laws. Public Law 104-191. U.S. Department of Health & Human Services (2006, Dec. 11). See, e.g., Does the HIPAA Privacy Rule preempt State laws? Retrieved from http://www.hhs.gov/hipaafaq/state/399.html, accessed on January 5, 2012.
38. Human Subjects Research Protections: Enhancing Protections for Research Subjects and Reducing Burden, Delay, and Ambiguity for Investigators. 76 Fed. Reg. 44512, 44512-53 (July 26, 2011).
39. Ibid. at 44527.
40. McGraw, D. (2011). Letter to Farzad Mostashari. Retrieved from http://healthit.hhs.gov/portal/server.pt/gateway/PTARGS_0_16869_955995_0_0_18/HITPC_Privacy_and_Security_Transmittal_Letter_10_18_11.pdf, accessed on January 30, 2012.
41. See, e.g., McGraw, D., "Paving the Regulatory Road to the 'Learning Healthcare System,'" Stanford Law Review Online, Vol. 64, February 2012, pp. 75-81. Retrieved from www.stanfordlawreview.org/online/privacy-paradox/learning-health-care-system, accessed on February 24, 2012.
42. Evans, Barbara J. "Much Ado About Data Ownership," Harvard Journal of Law and Technology, Vol. 25, Fall 2011. The ability to access data from patient-controlled sources, such as personal health records, or from patient-contributed sources, may be more directly affected by ownership laws. That dimension of this issue, however, is outside the scope of this paper.
43. Ibid.
44. Restrictions on certain disclosures and sales of health information; accounting of certain protected health information disclosures; access to certain information in electronic format42 U.S.C. § 17935 (d) (2009).
45. Ibid. 17935(d)(2)(B).
46. See Evans, Barbara J. "Waiving Your Privacy Goodbye: Privacy Waivers and the HITECH Act's Regulated Price for Sale of Health Data to Researchers," Univ. of Houston Public Law and Legal Theory Working Paper No. 2010-A-22, August 23, 2010. Retrieved from: http://ssrn.com/abstract=1660582, accessed on January 30, 2012.