Privacy, Research and the Evolution of Health Care in the 21st Century

By Kirk J. Nahra

For most of the past year, the Energy and Commerce Committee of the U.S. House of Representatives has been developing an important health care initiative called 21st Century Cures. This legislative proposal (still being developed) is intended to “take a comprehensive look at what steps we can take to accelerate the pace of cures in America.” The Committee is “looking at the full arc of this process—from the discovery of clues in basic science, to streamlining the drug and device development process, to unleashing the power of digital medicine and social media at the treatment delivery phase.”

This effort encompasses a variety of issues at the federal level, including several complicated problems involving the regulation of pharmaceuticals. Aside from these drug approval questions and other general health care topics, one of the key issues for the 21st Century Cures effort involves the assessment of how the current privacy and data security rules impact health care research, and whether the rules can be changed to facilitate more effective research without unduly affecting individual privacy. There is significant confusion, even among people in the health-care industry, about how these rules work today, and where there are actual problems with the rules. While the overall legislative package is still evolving, it is important for the Committee to understand how the current rules apply to research, and where reasonable and beneficial changes can be made.

Background

The legal rules surrounding research are driven by two overlapping regulatory packages. First, most health-care research is governed by the “Common Rule,” an ethical mandate governing biomedical and behavioral research involving human subjects. It applies to (essentially) all government-funded research involving human subjects, and also applies in most academic settings, public or private. Driven by certain historical abuses, the Common Rule prescribes an oversight role for Institutional Review Boards, and mandates “informed consent” in connection with human subjects. The core idea of the Common Rule is

1 See http://energycommerce.house.gov/cures.
clear and largely non-debatable—make sure that research projects involving human subjects are appropriate, and that the research participants understand the risks and benefits of the research project before they decide to participate.

The Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule then imposed a new set of requirements, related to patient authorization when research involving “Protected Health Information” was involved. For HIPAA, the primary “risk” involved privacy, rather than specific health risks (e.g., a drug under review causing a new medical problem).

The HIPAA Rules address research in two ways. Primarily, research falls into one of the “public purpose” categories of the HIPAA use and disclosure principles, where research requires a patient authorization unless certain specific criteria are met. For these public purpose categories, HHS—in developing the rules—recognized that there were certain kinds of uses and disclosures of PHI where patient consent was less important or even irrelevant, because of other public goals and policies. Other categories in this area include public health disclosures, oversight investigations and litigation.

For research, the principle is that research disclosures require a patient authorization unless the relevant covered entity “obtains documentation that an alteration to or waiver, in whole or in part, of the individual authorization . . . for use or disclosure of protected health information has been approved by either” an Institutional Review Board or a Privacy Review Board. The Rule sets out specific criteria for this waiver:

■ The use or disclosure of protected health information involves no more than minimal risk to the privacy of individuals, based on, at least, the presence of the following criteria: (1) An adequate plan to protect the identifiers from improper use and disclosure; (2) An adequate plan to destroy the identifiers at the earliest opportunity consistent with conduct of the research, unless there is a health or research justification for retaining the identifiers or such retention is otherwise required by law; and (3) Adequate written assurances that the protected health information will not be reused or disclosed to any other person or entity, except as required by law, for authorized oversight of the research study, or for other research for which the use or disclosure of protected health information would be permitted this subpart.

■ The research could not practicably be conducted without the alteration or waiver.

■ The research could not practicably be conducted without access to and use of the protected health information.

In addition to this section addressing research directly, “research-like” activities also are addressed in connection with the “health care operations” activities permitted by HIPAA. For these “treatment, payment and health care operations” activities, PHI can be used or disclosed by a covered entity without any need for patient consent or authorization. Therefore, where a covered entity needs to use or disclose PHI for treatment or payment purposes, it can do so without any specific patient consent, consistent with the remaining HIPAA principles. This ability to use or disclose information includes “Conducting quality assessment and improvement activities, including outcomes evaluation and development of clinical guidelines, provided that the obtaining of generalizable knowledge is not the primary purpose of any studies resulting from such activities; patient safety activities (as defined in 42 CFR 3.20); population-based activities relating to improving health or reducing health care costs, protocol development, case management and care coordination, contacting of health care providers and patients with information about treatment alternatives; and related functions that do not include treatment” (emphasis added). Because of this restriction on “generalizable knowledge,” many covered entities believe that the HIPAA Rules permit internal data analysis, but prohibit disclosure of the results of these analytics because that would provide “generalizable knowledge” and therefore would not be permitted under this provision of the Rules.

The 21st Century Cures Proposal

One key concept in the overall 21st Century Cures proposal is to review whether these rules can be adjusted or modified to improve the ability of the health-care system to conduct more effective health-care research, for the overall benefit of the health-care system. The Committee—quite appropriately—recognizes the enormous value in health-care research, and is making diligent efforts to determine whether there are appropriate changes that can be made to improve research opportunities without creating undue risks for privacy or otherwise.

The initial proposal addresses a variety of possible approaches. For some of these provisions, the goal of the changes is straightforward, and the provisions are logical and will improve the overall research setting without creating significant new concerns. Other concerns are less focused, or likely will lead to new problems or other unintended consequences. In addition, these proposals attack only a limited range of concerns about how research is conducted. On the whole, the Committee proposal incorporates various “tweaks” to the current system, without identifying broader problems or addressing these issues in a more integrated way.

As the Committee moves forward with its evaluation of this proposed legislation, here are some areas and thoughts for further consideration and/or improvement.

■ Generalizable Knowledge

The current HIPAA rules appear to distinguish between permitted data analysis for internal purposes, and disclosure of research results from this data analysis. By restricting use and disclosure of PHI when a covered entity is “Conducting quality assessment and improvement activities, including outcomes evaluation and development of clinical guidelines” if the “primary purpose” of the activity is “generalizable knowledge,” the current rules—without any real explanation—seem to impede communication of research results. In practice, covered entities have been conservative in their view of this language, even though the rule may give more flexibility than current activities seem to indicate (for example, if internal data analysis leads to results that may be worth publishing, this publication likely was not the “primary purpose” of the initial data analysis).
Congress should consider two aspects of this issue. First, it should consider removing the “generalizable knowledge” restriction. That would make clear that if a covered entity conducted, for example, “quality assessment and improvement” activities, and learned something of general value about this effort, it could disclose the research results through publication or other communication of results. Since the “use” of the patient data would be the same, there should be no additional privacy concerns in this use. Obviously, whether driven by a minimum necessary analysis or otherwise, specific PHI should not be publicly disclosed in publishing any research findings, but this would be normal behavior in any event (and certainly could be included in any regulatory revision if deemed necessary).

Second, Congress should consider whether to instruct HHS to make clear (in guidance) what kinds of disclosures are in fact permitted here—by redefining or explaining when “the primary purpose” of an activity is generalizable knowledge, or clarifying that analysis for other elements of this definition (e.g., population-based activities relating to improving health or reducing health-care costs, protocol development, case management and care coordination) can be conducted even if there is generalizable knowledge at the end.

The current Committee draft addresses this problem in a much broader fashion that likely will create its own issues. It proposes to add the idea of “research” to the definition of health-care operations, which would give a covered entity the ability to use and disclose PHI for research purposes without any additional controls. This concept—while clearly permitting more use and disclosure of data—would seem to eliminate the separate research proposals, and would permit potentially very broad disclosures without meaningful controls. Any step like this should be approached very cautiously.

**Access to Information to Develop Research Protocols**

One element of many research studies involves identifying whose information would be appropriate to include in a study. The current HIPAA rules permit some additional flexibility in this area, where a researcher physically reviews records on the premises of a covered entity. In today’s environment, this provision, while useful, is not as useful as it could be. Therefore, the Committee proposal includes a change to mirror this physical access in an electronic environment. This is a positive development. Moreover, since the risk here is a “security” risk more than a “privacy risk,” the Committee should consider whether it can expand this “preliminary to research” approach to permit more upfront data analysis, as long as appropriate security precautions are in place. Unlike the Committee draft, however, the appropriate security protections need to be on the part of the researcher, who is not generally covered by the HIPAA rules, rather than the covered entity that always has HIPAA security rule requirements.

**Encouraging Use of Limited Data Sets and De-Identified Data**

In connection with research, the HIPAA rules address three categories of data—protected health information, limited data sets and de-identified data. De-identified data is PHI that has been stripped of sufficient individual identifiers (using one of the two methods spelled out in the rules) so that the information is no longer “individually identifiable” and therefore is no longer subject to the HIPAA rules. De-identified data have real value in certain research contexts, and both the Committee and HHS should continue to explore means of enhancing the use and disclosure of de-identified health-care data.

There also are substantial opportunities in connection with limited data sets. Limited data sets is a carefully defined term in the HIPAA rules, meaning information that has been almost de-identified, but by inclusion of certain limited data fields, remains PHI. Under the current rules, covered entities can use and disclose limited data sets for research and certain other purposes, as long as there is an appropriate data use agreement in place. The Committee should explore (or instruct HHS to explore) whether there are additional means (including additional remuneration) of encouraging covered entities to disclose limited data sets for research purposes.

**Expand Use of Data Use Agreements Outside of Limited Data Set Context**

The data use agreement concept also can be expanded. A data use agreement mirrors—in most ways—the terms of a business associate agreement. Most researchers are acting on their own, rather than as a service provider to a covered entity, and therefore are not business associates under the HIPAA rules. Currently, researchers can only receive a limited data set using this data use agreement. The Committee should encourage HHS to implement a broader disclosure rule that permits broader PHI to be disclosed to researchers consistent with the protections of a data use agreement. These protections address both “privacy” concerns (by limiting how the information can be used and disclosed) along with requiring appropriate security protections. This expansion should be explored as a viable means of expanding research opportunities, particularly for “data research,” without raising many of the privacy and security concerns that accompany many other modifications to the HIPAA rules.

**Improved Guidance on Privacy Waivers**

As a general matter, while the HIPAA rules on research have been in place since 2003, there remains significant confusion about them. Most researchers are neither covered entities nor business associates, so they may have little understanding of how these rules work. It is clear that everyone involved—covered entities, researchers, IRBs and Privacy Review Boards—all would benefit from additional guidance from HHS on when a waiver of patient authorization is appropriate. HHS could consider whether there are “safe harbors” where a waiver would be presumed or automatic (e.g., data research only in a controlled and secure environment). Rather than try to define these details, Congress should direct HHS to issue additional guidance and/or clarifications to make this waiver process more efficient and to improve the ability of researchers to obtain and use data (for the benefit of the overall health-care system) where privacy risks are small or otherwise controlled.

**Elimination/Reduction of IRB Role Where Only Data are Involved**

Congress should consider whether there should be an elimination of an IRB role in “data only” research, or
could reduce an IRB’s role if a Privacy Review Board has approved a research project that only involves data (and therefore does not involve the direct health risks that initially led to IRBs).

**Authorization Issues**

HHS (both through OCR and other units) has been reviewing patient authorization requirements in connection with research, to streamline the elements that are required to permit PHI to be used in research. The Committee draft includes an element establishing a “one time” authorization for PHI generally. This idea makes sense, and should move forward in the legislation. This step gives patients more effective control of their data, if they wish to permit use of their data for research activities on a broad basis.

**Remuneration Issues and Concerns**

The Committee draft also raises issues related to how certain kinds of entities involved in research essentially can pay for access to health-care data. As written, this proposal raises substantial concerns. While the intent of the language is not entirely clear, the language appears to permit disclosure of any PHI to pharmaceutical companies, for their research, and would at the same time permit these companies to pay unlimited amounts for these data. If this is the intent of this legislation, it goes way too far (by permitting unrestrained disclosures to pharmaceutical companies without any new controls), and raises enormous red flags by permitting unlimited payments for these amounts (at least under the HIPAA rules—other health-care laws also may come into play). If the proposal were streamlined in important ways—such as by limiting the scope only to limited data sets, with accompanying data use agreements—the proposal might be worth additional consideration.

**Harmonization of HIPAA, the Common Rule and Other Research Principles**

It is clear that one of the key challenges for health-care research in the U.S. (without even considering international opportunities and complications) is that there are multiple rules and approaches that must be addressed and understood for many projects. As with many other areas of privacy law, the mere existence of multiple overlapping, inconsistent and ambiguous regulatory requirements creates its own problems and clearly increases overall transaction costs, to the detriment of both the industry and patients. The current legislative proposal does not address this overall confusion and tension. Moreover, it likely is not an appropriate or feasible legislative step to make legislative changes to an entire series of current regulations to attempt to bring them all together under a single framework. Instead, the Energy and Commerce Committee should consider directing HHS—which oversees many of these frameworks through various different sub-agencies—to study this question of harmonization and provide to Congress a report on how a more integrated and harmonious framework can be developed, to permit research projects to be developed in a more streamlined and efficient manner. Today’s rules create impediments to research based on confusion, without addressing the potential benefits of these projects. HHS should be instructed to evaluate how these confusion-oriented and duplicative impediments can be reduced or eliminated, through development of a more efficient and clearer overall process for developing beneficial research projects.

**Conclusions**

The 21st Century Cures proposal addresses a broad variety of important and useful issues that will advance the debate on providing better health care and improved treatment options. The detail addressed in the bill is extensive, and there clearly are many complicated issues at stake. On the privacy and security front, the current draft represents more of a rough outline, rather than an integrated approach to addressing specific problems without creating more. While there clearly is room for improvement in how the HIPAA (and other) rules address research, we need to make sure that (1) specific problems with the current structure are analyzed and identified; (2) it is clear to most that these problems are with the rules, rather than with how people are acting under the rules; and (3) that any changes to enhance research opportunities are directed at these specific problems while still protecting patient privacy in effective ways.