Risks and Legal Protections in the World of Big-Data

Leslie E. Wolf *

Abstract

The development of large electronic data sets, whether from electronic health records, health registries, or large-scale gene-environment interaction studies, offer an unparalleled, innovative opportunities to learn more about human health and disease. However, because these data may be used in unexpected ways, without the knowledge or consent of individuals whose data are being used, they also raise critical concerns about protections of individuals against risks. Traditional approaches to protecting research participants and patients may not address new or heightened risks in the “big data” era. My research colleagues and I conducted legal research to elucidate the web of legal protections afforded research participants in genomic research, including laws governing human subjects research, privacy, consent, discrimination, and use of research participants’ genetic information. It has revealed substantial regulatory activity and variation across the 50 states that may fill known gaps in federal protections. For example, some states go further than the Genetic Nondiscrimination Act (GINA) by extending genetic antidiscrimination statutes to life and disability insurers or to employers with less than 15 employees. In addition, states explicitly provide remedies, such as statutory damages, attorneys’ fees, and costs that can facilitate enforcement of legal rights not afforded in federal laws. This research has broader implications for data use in other research or in health care settings. In this paper, I suggest how this research can inform approaches to data privacy law in the United States and beyond to provide appropriate protections as health systems and scientists seek to harness the promise of big data while respecting individuals’ interests in their data.

Keywords: Human Subjects, Research Ethics, Genetic Information, Legal Protections, Data Privacy, Health Information Privacy, Confidentiality

* J.D., M.P.H., Director and Professor, Center for Law, Health & Society, Georgia State University College of Law P.O. Box 4037 Atlanta, GA 30302-4037, lwolf@gsu.edu

Acknowledgements: This work is supported, in part, through a grant from the National Human Genome Research Institute at the U.S. National Institutes of Health (NIH R01-HG-007733), Laura M. Beskow, Principal Investigator. I would like to thank my research partners on that project, in particular, Laura Beskow at Vanderbilt University and Erin Fuse Brown at Georgia State University College of Law, for the many discussions that informed my discussion here.
I. Introduction

There is now a surfeit of data available resulting from the move to electronic health records and the proliferation of “smart” technologies—from medical devices to consumer wearables—that can provide a steady stream of information about patients’ measurements, status, and activities. Health systems, insurers, governments, and researchers are all seeking ways to harness these data to improve health care delivery and health outcomes.

In some ways, these efforts are no different from the research, quality improvement, and other efforts to learn from patient experiences in the health system. In the United States, health systems, insurers, governments, and researchers routinely access patients’ medical records to support these types of efforts. Despite ethical and legal norms of patient privacy, confidentiality of medical records, and informed consent, U.S. law permits a much broader use of patient records for quality improvement or research efforts without patients’ knowledge or consent.\(^1\) The rationale has been that such activities pose very low risk to patients, while providing substantial societal benefits from the knowledge gained.\(^2\)

In other ways, however, the sheer magnitude and variety of available data and the unexpected ways they can be combined raise critical concerns about whether the data privacy risks to individuals remain low and whether there are mechanisms available to adequately protect individuals against those risks. Traditional approaches to protecting patients and research participants may not address new or heightened risks in the “big data” era.

My research partners and I conducted legal research to elucidate the “web” of legal

\(^1\) The HIPAA Privacy Rule sets minimum national standards regarding confidentiality of patient medical records, although states may adopt stricter requirements. U.S. Department of Health and Human Services, Summary of the HIPAA Privacy Rule (U.S. Department of Health and Human Services, “Summary of the HIPAA Privacy Rule,” July 26, 2013, https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html). These include requirements for written patient authorization to access medical records. But both the federal and state laws permit access to records without authorization for some activities, including peer review, quality improvement, and research under some conditions (Ibid.). Similarly, federal regulations governing human subjects research typically require consent, but research using medical records may be exempt from the provisions. See 45 C.F.R. 46 § 101(b)(4) § 111.

protects afforded to research participants in genomic research in the United States. Our analysis of the federal and state laws that protect research participants identified several approaches to protecting participants, gaps in the protections, and specific ways individual states have filled those gaps. Drawing on this research, in this paper, I describe the general approaches to data privacy law in the research context in the United States and then consider which types of protections may be necessary as health systems and scientists seek to take full advantage of the promise of big data while respecting individuals’ interests in their data.

II. Types of Risks

Because protections should be responsive to harms, I first considered the potential risks to research participants in big data research. For purposes of this paper, I identified three major potential risks: use of information without consent, inappropriate access to information, and inappropriate use of information. The latter includes the potential re-identification of individuals from de-identified or aggregate data.

The use of genomic and/or medical information without the individuals’ knowledge or consent could be considered a violation of the principle of respect for persons, both by failing to respect individual autonomy and by invading privacy. As such, it would be a wrong in and of itself, even if no harm to the individual arises from the use. In the United States, there have been several instances in which research participants have objected to use of their information without their knowledge or consent. In some of these cases, the participants objected to the research itself, as well as the use without consent. These cases have mainly

3 Because the proposed uses of big data would provide population-based benefit, rather than individual benefit, the potential harms to patients are likely the same as to research participants.


5 Henrietta Lacks’ story is probably the best known, as a result of Rebecca Skloot’s best-selling book The Immortal Life of Henrietta Lacks. Mrs. Lacks, a young African-American woman, underwent surgery for her cervical cancer at Johns Hopkins Hospital in 1951. Tissue samples removed at the time of surgery were used for research without her knowledge or consent and developed into one of the first successful cell lines. Named HeLa, they have since been in use in research worldwide. Her family lived in poverty with limited access to health care, unaware of their mother’s legacy. Although the book and other media focused attention on such unconsented
revolved around use of biospecimens in research without consent; they include secondary research use of biospecimens originally collected with consent for research and research use of biospecimens originally collected for non-research use. Despite widespread media attention to some of these cases, including a recent dramatization of the Henrietta Lacks case starring Oprah Winfrey, the public remains largely ignorant of how much research still may be legally conducted without consent. The controversy over Facebook’s manipulation of users’ news feeds (that Facebook controls by algorithms) without their knowledge or consent to evaluate how the emotional content of those feeds affects users’ posts provides further evidence that the public expects to be asked to consent, even in cases where the regulations do not require it.

Inappropriate access to information by a third party is the second risk I identified. There are many people who may have legitimate access to and uses for genomic or health information. For example, the HIPAA Privacy Rule, the federal health information privacy research, it remains legal (Laura M. Beskow, “Lessons from HeLa Cells: The Ethics and Policy of Biospecimens,” *Annual Review of Genomics and Human Genetics* 17 (2016): 395-417). Another recent case that received media attention is that of the Havasupai, a small Native American tribe who live near the Grand Canyon. They had given blood samples to an Arizona State University study to conduct diabetes research, a condition that affected the tribe. Unbeknownst to them, the samples were also used in research offensive to them, including research on inbreeding, schizophrenia, and migration. The latter conflicted with the Havasupai’s origin story. The Havasupai sued the researchers and ASU for the misuse of their samples and for their return. Although legally permissible, ASU settled the suit, apologized to the Havasupai, and agreed to collaborate with the tribe on health, education, and economic development issues (Michelle M. Mello and Leslie E Wolf, “The Havasupai Indian Tribe Case—Lessons for Research Involving Stored Biological Samples,” *New England Journal of Medicine* 363, no. 3 (2010): 204-207). In another case, parents in Minnesota and Texas sued after learning that their newborns’ blood spots had been used in research. See Adam Doerr, “Newborn Blood Spot Litigation: 70 Days to Destroy 5+ Million Samples,” *Genomics Law Report*, February 2, 2010, https://www.genomicslawreport.com/index.php/2010/02/02/newborn-blood-spot-litigation-70-days-to-destroy-5-million-samples/; Allison M. Whalen, “That’s My Baby: Why the State’s Interest in Promoting Public Health Does Not Justify Residual Newborn Blood Spot Research Without Parental Consent,” *Minnesota Law Review* 98 (2013): 419-453.


law, permits use of health information for treatment and payment purposes without written authorization.⁸ Most individuals want such sharing of information for these purposes. However, they may have concerns about their information being accessed for other purposes. In some cases, the information may be highly personal or stigmatizing, such that disclosure of the information in and of itself may be considered a wrong.⁹ Individuals may want to control to whom they disclose certain information. Federal and state genetic and medical privacy laws limit disclosure of genomic and health information without patient authorization, but there are often numerous exceptions, including for research, quality improvement, and peer review. Patients and research participants may not be fully cognizant of how their information may be shared and used without their consent.

A third risk is inappropriate use of information. This may arise when people have legitimate access to the information, but may use it for other purposes. Genetic and medical privacy laws commonly allow law enforcement to get access to medical records without authorization, although, in some cases, there may be judicial oversight. Individuals may fear that medical information may be used in investigations or prosecutions that could put them in legal jeopardy.¹⁰ Employers and insurers may legitimately have access to information for one purpose, and the concern is that, once in their hands, it may be used for other purposes. For example, an employer may obtain genetic or health information for a claim for worker’s

---

⁸ U.S. Department of Health and Human Services, “Summary of the HIPAA Privacy Rule.”

⁹ For example, information about sexually transmitted diseases, mental health, and substance abuse are generally considered sensitive. Accordingly, this type of information is sometimes afforded special confidentiality protections (Timothy Stoltzfus Jost, “Constraints on Sharing Mental Health and Substance-Use Treatment Information Imposed by Federal and State Medical Records Privacy” in Improving the Quality of Health Care for Mental and Substance-Use Conditions: Quality Chasm Series (United States: Institute of Medicine Committee on Crossing the Quality Chasm, 2006)). Similarly, under the 2013 amendments to HIPAA, patients who pay cash for treatment may restrict their health insurer’s access to that treatment information. The amendment recognized that some individuals may avoid care because of privacy concerns (Jim Pyles, “The Right to Obtain Restrictions under the HIPAA/HITECH Rule: A Return to Ethical Practice of Medicine,” ABA Health 9, no. 9 (2013), https://www.americanbar.org/content/newsletter/publications/aba_health_esource_home/aba_health_law_esource_1305_pyles.html).

compensation and use it against the person in promotion or retention decisions. Similarly, an insurer may use genetic or health information to deny or limit coverage or set premiums.

Re-identification of individual participants is a special subset of inappropriate use of information. Significant research may be conducted without consent when it is considered minimal risk because the researchers do not have identifiers or they have taken steps, like coding, to prevent individuals from being readily identified. However, the proliferation of information that is widely available challenges this basic understanding. Researchers have demonstrated as an academic exercise that it is possible to identify individuals in data that has been stripped of direct identifiers based on limited publicly available information.11 While such re-identification may currently be beyond the skills of ordinary citizens, it is a growing risk as re-identification becomes easier and as more data become available. In addition, as such information increasingly is perceived as valuable, the incentives to seek data and connect it will also grow.12

III. Corresponding Types of Protection

There are three major types of legal protections that correspond to the risks I identified. These are: consent, which affords individuals some level of control over their genetic information; confidentiality obligations, which respond to concerns about inappropriate access; and laws that limit use of information, which respond to concerns about inappropriate use of information. The latter laws often are antidiscrimination laws, but also include a


limited number of laws restricting re-identification of individuals. In addition to these types of protections, states add to these protections by including enforcement mechanisms of their own.

Consent. Consent has been considered an important mechanism for protecting individual autonomy. Consistent with international norms, federal regulations governing human subjects research generally require consent as a prerequisite to research participation. This requirement allows individuals to decide whether to participate in the research after being informed of the research’s purpose and its risks and benefits, among other things. Nevertheless, the federal regulations also permit medical records or biospecimen research to be conducted without consent under certain circumstances, such as when the information lacks identifiers or uses codes in place of identifying information, that minimize risks to participants.

My colleagues and my research indicates that some states have laws that allow individuals to exercise control over their information in a variety of ways that go beyond federal law. For example, in the research context, some states expand federal consent requirements by requiring consent to all research conducted among certain populations or

\[13\] The first provision of the Nuremberg Code, often considered one of the first codes of research ethics, is, “The voluntary consent of the human subject is absolutely essential.” The text of the Nuremberg Code is available at https://history.nih.gov/research/downloads/nuremberg.pdf. It has no exceptions to this requirement.

\[14\] See, e.g., 45 C.F.R. 46.111(a)(4) and 46.116. Some have begun to challenge this conception, suggesting there may be an obligation to participate in some forms of research and, in minimal risk research that allows for learning health care systems, such research can be conducted without consent. See, e.g., Ruth R. Faden, Tom L. Beauchamp, and Nancy E. Kass, “Informed Consent, Comparative Effectiveness, and Learning Health Care,” New England Journal of Medicine 370 (2014): 766-768.

\[15\] See, e.g., 45 C.F.R. 46.116(a) & (b).

\[16\] Such research may be exempt from the regulatory requirements or may be conducted under a waiver of the consent requirement (45 C.F.R. § 46.101(b)(4) and 45 C.F.R. § 46.116(d)). For a discussion of how these regulatory requirements may be applied, see Leslie E. Wolf, “Advancing Research on Stored Biological Materials: Reconciling Law, Ethics, and Practice,” Minnesota Journal of Law, Science & Technology 11, no. 1 (2010): 127-133. The U.S. Department of Health and Human Services has promulgated revised regulations which continue to allow such research to be conducted without consent (U.S. Department of Health and Human Services, “Federal Policy for the Protection of Human Subjects,” 82(12) Fed. Reg. 7149 (2017)). The revisions currently are under review by the Trump administration (Jeanne Baumann, “Trump Administration Seen Unlikely to Change Human Research Rule,” Health Care on Bloomberg Law, May 26, 2017 https://www.bna.com/trump-administration-seen-n73014451606/).
in certain settings, or requiring consent to genetic research under circumstances that the federal exemptions would not require. Consistent with general medical privacy laws, including the federal HIPAA privacy rule, that require patient authorization to disclose their information, some states require consent before disclosure of genetic information. States also impose requirements to obtain consent before conducting genetic testing or before retaining genetic information. Such consent requirements limit the likelihood the individual’s information will be used without their knowledge or consent. However, like the federal research regulations, many of these provisions have exceptions to them, including for research purposes, which undermine individual control.

The exceptions to consent in federal and state law have been justified on the grounds that they present minimal risk to those whose information is used because they are not identified. Moreover, such research provides important information to improve public health. However, as the examples described above illustrate, the public may be ill-informed about these exceptions to the consent requirements and may object when their information and materials are used without their knowledge and consent.

Confidentiality protections. Confidentiality protections respond to concerns that information may be disclosed beyond the needed or authorized use. Confidentiality protections come in a variety of forms. Sometimes the provisions are general—they declare the genetic information to be confidential, but do not specify more. Some states expand on these general obligations, requiring those who work with confidential information to sign

---

17 See, e.g., Ala. Code § 22-56-4 (mental health services); N.Y. Comp. Codes R. & Regs. Tit. 14 § 815.11 (substance abuse programs).


22 Other common exceptions include for law enforcement or public health purposes, as well as with a court order.

a document acknowledging their confidentiality obligations.\textsuperscript{24} While these provisions do not substantively change the confidentiality obligations, they may have a practical effect on employees’ understanding of their duties. Such confidentiality provisions are consistent with the well-recognized confidentiality obligations within the doctor-patient relationship. While the federal HIPAA Privacy Rule does not have a private right of action, its provisions can serve as evidence of a standard of care to provide claim for breach of confidentiality.

In many cases, states provide more specific confidentiality protections than federal law does. The consent provisions that grant patients’ and participants’ control over who has access to their information correspondingly impose obligations on those who hold the data to get appropriate consent before disclosing. Under some laws, these obligations apply only to specific types of individuals (e.g., health care providers), whereas other laws apply to the data itself, regardless of who receives it. Some states further protect confidentiality of genetic information by protecting against compelled disclosure, such as through subpoena, in any legal proceeding.\textsuperscript{25} These laws typically prohibit disclosure of the identity of the individual, although they may permit disclosure of information that is not identifiable, such as aggregate data. Some states go further, in some cases declaring genetic information inadmissible\textsuperscript{26} and not allowing even discovery of it.\textsuperscript{27}

\textit{Limitations on use.} The limits that federal and state laws impose on use of information generally pertain to anticipated potential misuses. Specifically, because the United States does not have guaranteed health insurance, there were concerns that health insurers might deny coverage or charge higher rates based on genetic information. Accordingly, numerous states adopted laws prohibiting health insurers from using genetic information in underwriting decisions, and the federal government later enacted the Genetic Information Non-Discrimination Act (GINA), extending such protection nationwide.\textsuperscript{28} Some states

\textsuperscript{24} See, e.g., R.I. Gen. Laws Ann. § 5-37.3-4; HIPAA requires worker training on confidentiality obligations, citing 45 C.F.R. § 160.103 and 45 C.F.R. § 164.530(b)(Department of Health and Human Services, “Summary of the HIPAA Privacy Rule”).


\textsuperscript{26} See., e.g., Ark. Code Ann. § 20-35-103.

\textsuperscript{27} See., e.g., Ark. Code Ann. § 20-35-103.

go beyond GINA’s limited application to health insurance and prohibit use of genetic information in disability and long-term care insurance,\(^{29}\) and one state prohibits use of genetic information in underwriting any type of insurance, including life insurance.\(^ {30}\) Another concern is that employers might make an adverse employment decisions—such as hiring, firing, or promoting—against individuals based on their genetic information. The federal GINA and similar state laws also prohibit employers’ collection and use of genetic information in employment decisions.\(^ {31} \)

The state confidentiality laws against compelled disclosure also have some role to play in protecting against inappropriate use, as they prevent third parties from gaining access to information that could be used to harm the individual. These protections typically limit disclosure of identifiable information, but often permit the disclosure of information that has been stripped of identifiers. The assumption has been that such information is rendered anonymous, although that assumption has proven faulty; a number of experts have demonstrated that people with technical knowledge, access to multiple sources of data, and an interest in re-identifying de-identified data can do so. Fuller protection requires restrictions on attempts to re-identify individuals whose data have been revealed. At least one state has such a restriction.\(^ {32} \) Such restrictions also have been used in protective orders when

\(^{29}\) See, e.g., Colo. Rev. Stat. Ann. § 10-3-1104.7 (group disability and long-term care insurance).


data have been ordered disclosed in discovery, but such protections are *ad hoc*, requiring litigants to request them and for a judge to grant them.

*Enforcement.* All these protections are further strengthened to the extent that they also provide a mechanism to enforce the requirements. Although federal laws often do not provide a mechanism for individuals to bring claims if they are injured, states more commonly do so. For example, many of the consent provisions also have remedies for failing to get the requisite consent. When states provide a mechanism for bringing a claim, they often also specify that those aggrieved may obtain damages, attorneys’ fees, and costs. Several states include legal minimums for damages per claim or per violation. These legal minimums, coupled with attorneys’ fees and costs, make it more likely that an aggrieved individual could bring an action and enforce the protections afforded by law.

**IV. Lessons for data-driven health care**

Although the analysis my colleagues and I conducted focused on genomic research, the protections we studied often applied more generally to health information. Moreover, the concerns the laws we studied address are also applicable to the use of health data that is used to develop a data-driven health care system. Accordingly, our research, coupled with some of the American experiences evidencing concerns about use of data without individuals’ knowledge, has lessons for other countries seeking to take advantage of the wealth of genomic and health data being generated.

First, whether to require consent to use patient data is an issue that deserves careful consideration. There are strong scientific reasons not to do so, as data will be significantly more representative and complete without requiring consent. Moreover, there are long-standing precedents for using such data without consent. Despite general norms regarding consent, United States research law permits research using medical records and biospecimens

---


without consent under certain circumstances. In addition, despite general norms of patient confidentiality, United States health care laws generally permit use of records for research and a variety of quality improvement activities. Indeed, some have argued that citizens have an obligation to allow their information to be used in support of learning health systems that benefit all. Moreover, individual medical information may be used for numerous, legitimate government functions, such as public health activities, quality oversight, and audits of government spending. Many of the state consent requirements my colleagues and I found pertain to specific contexts—research among specific populations and genetic testing—that may not be generalizable to medical information more generally.

Although such unconsented uses of health and genomic information are common, the public is typically unaware of these uses. For example, public messaging regarding HIPAA’s protections has emphasized how it empowers patients, but not its numerous exceptions. Failing to meet the public’s expectations regarding the use of their health information can lead to negative consequences. Indeed, despite suing the state for using her newborn’s blood taken for genetic screening in research without her knowledge or consent, one parent indicated that she probably would have consented had she been asked. Thus, it is not the research that was objectionable, but the lack of information about the research.

This parent’s comment points to a way forward without seeking individual consent: better communication about how health information is actually used. Had this parent been told at the outset that her child’s blood spot would be used for research, in addition to her child’s screening, she likely would not have objected. Her support for the research likely would have increased had she been told that research conducted with spots like her child’s

---


36 Because of its predictive nature, genetic information has been perceived differently than other medical information. As a result, there is a so-called genetic “exceptionalism” incorporated into these laws, although some have questioned its appropriateness. See, e.g., James P. Evans and Wylie Burke, “Genetic Exceptionalism. Too much of a good thing?” *Genetics in Medicine*, 10 (2008): 500-501.


38 As described above, controversies have arisen when actions have been conflicted with public expectations.

made such public health screening—and treatment, as necessary—possible. Evidence suggests that, when asked about it, Americans are largely supportive of research and willing to have their information used in it. Educating the public about how their health information might be used in research to improve health and health care delivery and how individuals’ interest will be protected would help set more realistic expectations and convey the benefits of population-based research. It is more respectful to be transparent about the uses of individuals’ information. Such education may also provoke public discussion that could inform efforts to ensure the public’s interests are protected. It also makes it possible to permit meaningful opt-out from participation because individuals are aware that there is a choice to be made.

Second, there needs to be consideration of what protections are needed to protect the information in use. Public willingness to have their information used in data-driven health care will undoubtedly depend on the expectation that their information will be protected and the individual risks to them will be minimized. Accordingly, some level of confidentiality protections is necessary. At a minimum, protections for securing and sharing such information should be consistent with protections for medical information generally. However, it is worth considering whether additional protections are warranted because the use will not benefit individuals directly. Given critiques of “genetic exceptionalism,” which treats genetic information differently than other medical information because it is uniquely identifiable, it is worth discussing whether genetic information should receive additional protections, as seen in some of the U.S. laws regarding genetic testing and information.

Third, there needs to be some reflection on the legal and cultural context in which these legal protections have been and will be adopted. The United States emphasizes individual preferences and rights. American laws reflect that orientation, and respect for autonomy and individual consent play a central role within American medical ethics. At the same time, there is a long history of discrimination that has resulted in persistent health disparities and distrust of the medical professional and research among African-Americans particularly. Legal protections can provide a mechanism for realizing collective benefit, while recognizing and protecting individual interests. However, the particular approaches adopted in the United States may not be suited for countries with a more communitarian orientation and where

---

40 U.S. Department of Health and Human Service, “Your Rights under HIPAA.”
there may be more trust in the government.

Similarly, some protections afforded in the United States may not be necessary in other contexts. For example, the concerns that resulted in GINA and similar state genetic privacy/antidiscrimination laws arose, in part, because the United States does not have universal health insurance. People were concerned that health insurance coverage would be denied or made prohibitively expensive because of genetic information that had not manifested as a disease or condition. Although there is little evidence that insurers did so, they certainly made underwriting decisions based on other types of health information, such as pre-existing conditions or family history. Insurers require such information, and failure to provide accurate information can result in rescission of the policy. In countries with universal health insurance, these particular protections may not be necessary. In contrast, the components of GINA and similar state laws that limit use of genetic information in employment decisions likely have broader relevance across countries. Thus, I present these general approaches, as well as the particular federal and state laws that have been adopted in the United States, not as a blueprint for other countries, but rather as concrete examples that can be adopted, adapted, and rejected as appropriate.

Finally, if protections are afforded, there ought to be some mechanism for enforcement. Again, the type of enforcement should be suited to the legal and cultural context. The granting of an individual right to suit that my colleagues and I found in some state laws may reflect the U.S. legal system’s reliance on the adversarial process. However, whatever approach is taken, it should provide meaningful redress to individuals who suffer harms as a result of their information being used for research to the cause of data-driven health care.

In sum, my colleagues and my research has revealed a variety of approaches that the federal and state governments have adopted toward data privacy in the context of genomic research. Some of these provide greater control to individuals over their data and protection against potentially harmful uses of their data. These include allowing individuals to decide whether their information is used through consent requirements, imposing confidentiality obligations with respect to the data, and prohibiting certain uses. In determining how to move forward with a data-driven health system, policymakers should consider what laws and policies are necessary to maintain public trust in such a system. Quality improvement efforts and scientific advances depend on access to some of the most personal information.
Those conducting the work have an ethical responsibility to those individuals whose data is used, especially when that information is used without individuals’ knowledge and consent. Any approaches must be respectful of individual interests, or the erosion of public trust and support for research and quality improvement efforts will leave the benefits of a data-driven health system unrealized.

Received: January 4, 2018
Revised: February 26, 2018
Accepted: March 11, 2018