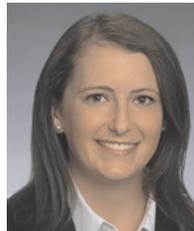


Reproduced with permission from Medical Research Law & Policy Report, 14 MRLR 30, 01/07/2015. Copyright © 2015 by The Bureau of National Affairs, Inc. (800-372-1033) <http://www.bna.com>

Genetic Information Privacy: A Complex Regulatory Framework



BY M. LEEANN HABTE, JENNIFER M. FORDE
AND CLAIRE N. MARBLESTONE

Introduction

Low-cost sequencing of a patient's genome and advances in the interpretation of a patient's genetic information have been key influences in the growth of personalized medicine. It took \$1 billion and

13 years to sequence the first draft of the human genome. Now, a human genome can be sequenced for \$1,000. These scientific advances were paralleled by technological advances in computing power and cloud-based data storage capacity, which (along with new genomic bioinformatics applications) enable the integration of genetic data and electronic health records for use by researchers and by clinicians. However, despite the technological ability to integrate data, the legal framework that governs the use of genetic data remains sector-specific and state-specific, which creates certain challenges with respect to compliance with state and federal privacy laws governing genetic information.

Legal Framework

One of the significant concerns related to genetic information has been the potential for discrimination by employers and insurers. The federal Genetic Information Nondiscrimination Act ("GINA") and state laws prohibit such discrimination. With regards to the protection of genetic information more generally, however, the Health Insurance Portability and Accountability Act ("HIPAA") imposes no special restrictions on the use and disclosure of sensitive information, such as genetic information. All protected health information ("PHI") is subject to essentially the same standards. In contrast,

M. Leeann Habte is senior counsel with Foley & Lardner LLP in Los Angeles. She is a member of the firm's Health Care Industry Team and Privacy, Security, & Information Management Practice.

Jennifer M. Forde is an associate with Foley & Lardner LLP in Washington, where she is a member of the firm's Health Care Industry Team.

Claire N. Marblestone is an associate with Foley & Lardner LLP in Los Angeles, where she is a member of the firm's Health Care Industry Team.

state laws impose a host of special restrictions on the collection, retention, use, disclosure and form of consent for genetic information. Therefore, organizations that collect and use genetic information in multiple states must be aware of these differing compliance obligations.

Federal Law

The HIPAA Privacy Rule applies to “covered entities,” including health plans, health care clearinghouses and any health care provider that electronically transmits health information in connection with a transaction—such as billing a health plan for reimbursement for service—for which there is a HIPAA standard transaction and code set. Covered providers include physicians, genetic testing laboratories, genetic counselors and other organizations.

The HIPAA Privacy Rule was amended in 2013 by the Omnibus Final Rule, which, among other things, incorporated the ban on use and disclosure of genetic information for underwriting purposes by health plans and insurers, including employer-sponsored health plans, as set forth in GINA.¹ The Omnibus Final Rule expressly included genetic information in the definition of PHI and added a definition of “genetic information” that includes not only information about the genetic tests of an individual and any request for genetic services (including genetic testing, counseling, or education) or participation in clinical research, but also information about his or her family members, and the medical history of those family members.² A family member includes any dependent or relation to the fourth degree (e.g., great great-grandparents or grandchildren, children of first cousins) or closer, without reference to the existence of biological ties.³ Under this definition, any use or disclosure of PHI that includes genetic information of family members will require careful scrutiny. Finally, the Omnibus Final Rule modified the definition of PHI to exclude information regarding a person who has been deceased for more than 50 years, so genetic information, like other PHI, is not protected indefinitely.⁴

The HIPAA Privacy Rule provides general limitations on the uses and disclosures of PHI, including genetic information, without individual authorization other than as set forth in the Privacy Rule. However, it permits relatively broad uses and disclosures of PHI for treatment, payment and health care operations (“TPO”).⁵ For example, TPO encompass a broad range of analyses, such as those in support of utilization review, quality assurance and business planning.

State Law

In addition to the general protections afforded to genetic information as PHI under HIPAA, 35 states have laws that impose additional privacy restrictions on genetic tests and/or genetic information. These laws typi-

cally restrict the collection, retention, use or disclosure of genetic information about an individual without written consent, although there are exceptions if the disclosure is in response to a court order or for anonymous medical research. These more stringent laws are not preempted by HIPAA and, in many cases, apply to entities other than covered entities or health care providers.

In 20 of these states, the restrictions on disclosure of genetic information apply generally to any person or entity that obtains or maintains genetic information rather than specific entities, such as insurers or health care providers. For example, in Alaska, a “person” may not collect, retain or disclose a DNA analysis without an individual’s informed and written consent.⁶ As a result, a business that stores genetic information on behalf of individuals, even though not a provider or business associate, would be subject to these state genetic privacy laws.

Moreover, the form of consent is often mandated in state statutes or regulations. Similar to Alaska, New York law requires written *informed consent* to disclose the records, findings and results of any genetic test.⁷ A general authorization is insufficient.

In addition to laws governing the use and disclosure of genetic information, a few states have passed laws that protect genetic data of individuals as property, asserting that an individual is the “owner” of his or her genetic information.⁸ In some states, the laws apply to the results of DNA analysis. In others, the laws that define genetic information as the “unique property” of the individual tested govern insurers.⁹ However, in at least one state, Louisiana, genetic information is broadly defined to include DNA analysis, and “all information about genes, gene products, inherited characteristics, or family history/pedigree that is expressed in common language.”¹⁰ Although there is some precedent regarding the courts’ view on ownership of genetic information,¹¹ these genetic property rights statutes have not been tested in the courts. Nonetheless, from a compliance perspective, these laws suggest that any consent for collection of genetic information from individuals should include a waiver of ownership rights.

Privacy Issues for Research Uses of Data

The Omnibus Final Rule also expanded the use of PHI for research and harmonized HIPAA with the Common Rule¹² by allowing covered entities to obtain individual authorization for the uses and disclosures of PHI for future research purposes. The revised Privacy Rule provides considerable flexibility for creation of research databases, so long as the research authorization adequately describes the future research such that it would be reasonable for the individual to expect that his or her PHI could be used or disclosed for future re-

⁶ Alaska Stat. § 18.13.010(a)(1).

⁷ NY CLS Civ R § 79-1(3)(a).

⁸ See e.g. Alaska Stat. § 18.13.010(a)(2); Fla. Stat. § 760.40(2)(a); O.C.G.A. § 33-54-1(1); C.R.S. § 10-3-1104.7(1)(a); La. R.S. 22:1023(E).

⁹ O.C.G.A. § 33-54-1(1); C.R.S. § 10-3-1104.7(1)(a).

¹⁰ La. R.S. § 22:1023A(8)(a).

¹¹ See e.g. *Moore v. Regents of University of California*, 793 P.2d. 479 (Cal. 1990); *Greenberg v. Miami Children’s Hosp. Research Inst.*, 264 F. Supp. 2d 1064, 1075 (S.D. Fla. 2003).

¹² 45 C.F.R. Part 46.

¹ Department of Health and Human Services, Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules; Final Rule, 78 Fed. Reg. 5,566 (Jan. 25, 2013).

² 45 C.F.R. § 160.103.

³ 45 C.F.R. § 160.103.

⁴ 45 C.F.R. § 160.103.

⁵ 45 C.F.R. § 164.502.

search purposes.¹³ With this additional flexibility, entities can more easily develop research repositories and databases for future research purposes for genetic and genomic research.

In addition, the HIPAA Privacy Rule provides certain limited options for creation of research databases in the absence of individual authorization. Specifically, a covered entity could:

- assuming specified criteria are met, seek approval of an alteration or waiver of an individual authorization by an institutional review board (“IRB”) or privacy board;¹⁴
- obtain certain representations from the researcher that the use or disclosure is sought solely to review PHI as necessary to prepare a research protocol or for similar purposes preparatory to research;¹⁵
- obtain representations from the researcher that the use or disclosure sought is solely for research on PHI of decedents, and the use or disclosure is necessary for research purposes;¹⁶
- enter into a data use agreement with the researcher, pursuant to which the covered entity could disclose a limited data set to the researcher for research, public health, or health care operations;¹⁷ or
- obtain de-identified data. Data are considered de-identified under HIPAA under either the Safe Harbor Method, which requires the removal of identifiers and an absence of actual knowledge that the remaining information could be used to identify the individual, or the Expert Determination Method, which involves a formal determination by a qualified expert.¹⁸

The expert determination method offers significant opportunities for creation of more robust databases that can be used without the restrictions associated with Data Use Agreements or other limitations on use.

State Law Research Issues

Even though under HIPAA, de-identified data are not considered PHI¹⁹ and thus may be freely used and disclosed for research purposes, state law may impose more stringent standards. For instance, Georgia’s law

on genetic testing requires a health care provider that obtains an individual’s clinical individually identifiable health information to notify the individual that the information may be disclosed or retained by the provider for anonymous research or coded research, and allow the individual to opt out of the research.²⁰ An additional consideration is whether genetic data truly can be made anonymous. Some experts have taken the position that it is not possible to make genetic data truly anonymous because an individual’s DNA, by its very nature, has staggeringly high levels of “genetic language” encoded within. Thus, to the extent that state laws apply to anonymous data rather than de-identified data, the threshold for anonymization may prove to be an issue.

Research involving genetic data may be further complicated by the vesting of ownership of genetic data in the individual in certain states. Thus, even if one of the HIPAA research exemptions (e.g., IRB or privacy board approval) was met, state law still may prohibit use or disclosure of the genetic data, absent patient consent. Further, assuming an individual has ownership over the individual’s genetic data pursuant to state law and if the research is governed by the Food and Drug Administration or subject to the Common Rule, waivers of genetic property rights may not be permissible.²¹

Conclusion

While the inherent tension between the new opportunities for genetic and genomic information and the legal framework may ultimately prompt a rethinking of the ways that health information is protected, there are a few key principles for navigating existing law. First, it is important to map the source, type, uses and legal restrictions of data to identify potential barriers to proposed uses of data. Advance planning for any proposed secondary uses of such data is critical, as strategies must be developed to address the authorization/consent, or methods for de-identification of the information. Second, consent, and often informed consent, often will be required for any use or disclosure of genetic information. As a best practice, an entity can consider the more restrictive state laws to which it is subject and implement consent and authorization forms that comply with these more stringent state laws, as well as HIPAA.

¹³ See 78 Fed. Reg. at 5,611-5,615.

¹⁴ 45 C.F.R. § 164.512(i)(1)(i).

¹⁵ 45 C.F.R. § 164.512(i)(1)(ii).

¹⁶ 45 C.F.R. § 164.512(i)(1)(iii).

¹⁷ 45 C.F.R. § 164.514(e).

¹⁸ 45 C.F.R. §§ 164.514(a)-(b).

¹⁹ See 45 C.F.R. § 164.502(d)(2) (de-identification results in health information that is “considered not to be individually identifiable health information”).

²⁰ O.C.G.A. § 33-54-6.

²¹ 21 C.F.R. § 50.20 (Informed consent documents cannot contain exculpatory language that requires subjects to relinquish any of their legal rights.); HHS Office for Human Research Protections, Exculpatory Language in Informed Consent, available at <http://www.hhs.gov/ohrp/policy/exculp.html> (indicating that a statement that the subjects “give up any property rights” in bodily fluids or tissue obtained during research is not acceptable for an informed consent document).