SPECIAL ARTICLE | Genetics inMedicine

Impact of HIPAA's minimum necessary standard on genomic data sharing

Barbara J. Evans, PhD, JD[1] and Gail P. Jarvik, MD, PhD[2,3]

This article provides a brief introduction to the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule's minimum necessary standard, which applies to sharing of genomic data, particularly clinical data, following 2013 Privacy Rule revisions. This research used the Thomson Reuters Westlaw database and law library resources in its legal analysis of the HIPAA privacy tiers and the impact of the minimum necessary standard on genomic data sharing. We considered relevant example cases of genomic data-sharing needs. In a climate of stepped-up HIPAA enforcement, this standard is of concern to laboratories that generate, use, and share genomic information. How data-sharing activities are characterized—whether for research, public health, or clinical interpretation and medical practice support—affects how the minimum necessary standard applies and its overall impact on data access and use. There is no clear regulatory guidance on how to apply HIPAA's minimum necessary standard when considering the sharing of information in the data-rich environment of genomic testing. Laboratories that perform genomic testing should engage with policy makers to foster sound, well-informed policies and appropriate characterization of data-sharing activities to minimize adverse impacts on day-to-day workflows.

Genet Med advance online publication 14 September 2017

Key Words: genomic data sharing; HIPAA Privacy Rule; minimum necessary standard; research; treatment uses

INTRODUCTION

What is the minimal amount of private health data a genomic researcher needs to answer a specific research question? This is not an idle philosophical inquiry, but a question many investigators (and health-care providers that supply data to them) are legally required to ask under the Health Insurance Portability and Accountability Act of 1996 (HIPAA)[1] Privacy Rule,[2] a major US medical privacy regulation in effect since 2003. Amendments to the Privacy Rule in 2013[3] confirmed that genetic information is protected health information (PHI) and is subject to the same protections that apply to other medical data, including HIPAA's minimum necessary standard.[4]

The minimum necessary standard requires HIPAA-regulated entities to use, disclose, and request PHI parsimoniously, so that their activities implicate the smallest amount of PHI that is "reasonably necessary" to achieve the data user's intended purpose.[5] Requesting, using, or supplying too much information—more than one actually needs for the task at hand—can violate the Privacy Rule. In this respect, HIPAA mirrors protections seen internationally. For example, the European Union's 1995 Data Protection Directive[6] and the General Data Protection Regulation[7] that will supersede it in 2018 call for data access not to be "excessive" and to be "limited to what is necessary" in relation to the purposes for which data are collected and further processed.

Minimum necessary violations are one of the top five causes of patient complaints investigated by the US Department of Health and Human Services Office for Civil Rights, which administers HIPAA.[8] People care not only *whether* their health information is shared, but *how much* and *which* information is shared *with whom* and for *what purpose*, and they want their data not to be shared needlessly. In traditional health data environments, minimum necessary violations often are fairly prosaic: for example, a receptionist leaves a voice message confirming a patient's appointment and divulges information about the patient's medical condition; only the appointment time needed to be disclosed.

Genomic testing generates large data files that present questions under the minimum necessary standard. To date, the Office for Civil Rights has not issued regulatory guidance to help genomic testing laboratories understand their obligations: When is it lawful to access or share a patient's entire binary alignment map, FASTQ, or variant call format file, as opposed to just specific variants? The Privacy Rule does allow large data sets, such as a patient's whole medical record or whole genome, to be used and shared, but only when "specifically justified."[9] There is a need for practical regulatory guidance explaining which purposes, in the regulator's view, justify the sharing of entire data files and what procedures laboratories should follow when reviewing such requests. There are also larger policy concerns, such as

[1]Law Center and Department of Electrical and Computer Engineering, University of Houston, Houston, Texas, USA; [2]Department of Medicine/Medical Genetics, University of Washington, Seattle, Washington, USA; [3]Department of Genome Sciences, University of Washington, Seattle, Washington, USA. Correspondence: Barbara J. Evans (bjevans@central.uh.edu)

Submitted 9 February 2017; accepted 11 July 2017; advance online publication 14 September 2017. doi:10.1038/gim.2017.141

whether the labor and time to extract selected parts of files to comply with the minimum necessary standard may make data holders even more reluctant than they already are to share data for research.

In November 2016, the National Committee on Vital and Health Statistics, which advises the Secretary of Health and Human Services on HIPAA-related issues, flagged the field of genomics as raising "potential future issues" with respect to minimum necessary compliance.[10] We live in an age of stepped-up HIPAA enforcement with ever-larger fines for violations.[11] Investigators and medical geneticists need to understand how the minimum necessary standard applies to their work. This article provides a basic introduction.

MINIMUM NECESSARY STANDARD 101

HIPAA's minimum necessary standard holds the dubious distinction of being one of the least-understood provisions of one of America's most-despised regulations. The National Committee on Vital and Health Statistics notes that the standard "remains poorly understood and inconsistently implemented by covered entities and their business associates."[10] This confusion is unfortunate, because the minimum necessary standard can be summarized in three simple points.

Who is subject to the standard? Only HIPAA-covered entities—organizations and individuals regulated by the Privacy Rule—must comply with the minimum necessary standard. Covered entities generally include health-care providers and payers/insurers. Some research laboratories are not HIPAA-covered. Research laboratories can, however, fall under the Privacy Rule if they (even once) use electronic communications to verify a research subject's insurance coverage or to bill an insurer for a test, or if they are subsidiaries of larger HIPAA-covered academic medical centers. When unsure, laboraticians should contact the HIPAA Privacy Officer at their institution to clarify their status.

Laboratories that are not HIPAA-covered can use and request data without having to worry about the minimum necessary standard. Even so, the standard may affect them indirectly if they obtain data—such as clinical information about research subjects—from health-care providers that do have to comply with the standard. The standard can limit access to data for use in research, even when a laboratory is not HIPAA-regulated.

To which data does it apply? HIPAA's minimum necessary standard only applies to uses, requests for, and disclosures of *existing* PHI—data previously created and on file somewhere. The standard does not apply to clinicians when they generate health data in the course of clinical care, for example, by ordering tests or examining patients. If a clinician orders whole-genome sequencing when a variant-specific test would suffice, the patient's insurer may object, but HIPAA does not care: this is not a minimum necessary violation. HIPAA sets no limits on how much information health-care providers can generate, obtain, use, or store for treatment purposes.

How does the standard work? HIPAA's application of the minimum necessary standard has an artful simplicity—although admittedly its simplicity is revealed only after many hours spent mindfully meditating the Privacy Rule's internal twists and turns. To summarize, the Privacy Rule sorts all conceivable data uses into four separate groups. For each group, the Privacy Rule establishes a different way that the minimum necessary standard interacts with the Privacy Rule's individual authorization requirement (which is HIPAA's name for consent to the use of one's data). The result is four distinct tiers of privacy protection, which vary depending on the planned data use. For different uses of their data, individuals receive different levels of privacy protection, as summarized in **Table 1**.[10]

The Privacy Rule's baseline protection, shown as tier 1 in **Table 1**, lets individuals control access to their data either by signing an individual authorization[12] or by exercising their own right of access to their data.[13] When individuals control uses and disclosures of their data, HIPAA's minimum necessary standard is irrelevant. Individuals are free to grant access to as much or as little information about themselves as they feel comfortable revealing. Researchers using data under valid HIPAA authorizations are not subject to the minimum necessary standard.

The three remaining tiers recognize that certain data uses offer social benefits that are so important that individuals should not be allowed to block them. Individual authorization is not required in tiers 2–4, but different standards govern how much data can be disclosed.

In tier 2, individual authorization is not required, but the minimum necessary standard applies. There are about 10 tier 2 data uses, depending on how one counts.[14] Several are important in genomics: research uses of data under a waiver approved by an institutional review board or privacy board,[15] public health uses of data,[16] and data uses to facilitate quality improvement activities and health-care payments.[17]

Example. An investigator seeks access to stored genomic and clinical data for 100,000 patients to search for clinically relevant associations between a specific group of genetic variants and a particular disease. The data are stored at HIPAA-covered hospitals and laboratories, and it is not practicable to locate all 100,000 patients to obtain signed HIPAA authorizations to use their data in the study. Access is still possible under a waiver if an institutional review board determines that HIPAA's waiver conditions at 45 C.F.R. Sec. 164.512(i) are met: i.e., the study presents no more than minimal privacy risks and could not practicably go forward if signed authorizations were required, and the research cannot practicably be conducted without access to the data in question. However, HIPAA's minimum necessary standard will apply. A HIPAA-covered data holder would violate the Privacy Rule if it shared clinical information not relevant to the disease being studied or if it shared entire genomic data files when variant-specific information would suffice to test the investigator's hypothesis.

When requesting data for a tier 2 use, HIPAA-regulated researchers must plan ahead and limit their requests to what is reasonably necessary to accomplish the purpose for which the

Table 1 HIPAA's four tiers of privacy protection

Tier	Data uses that fall in each tier	How HIPAA protects individuals' privacy
1	Any data use that an individual has authorized, for example, a research study in which people gave their permission to share their data with researchers.	Individuals control the use and disclosure of their data. The individual, rather than the minimum necessary standard, decides how much data can be used or disclosed.
	Individuals' access to and use of their own data under HIPAA's individual access right.	
2	Ten enumerated data uses,[14] including three that are important in genomics:	Individuals do not control access to their data (i.e., individual authorization is not required). The minimum necessary standard applies and limits how much data can be requested, used, or disclosed.
	Research uses of data under HIPAA's waiver provision at 45 C.F.R. Sec. 164.512(i), which allows data to be used in research without the individual's authorization under certain circumstances	
	Public health uses of data	
	Health-care billing and operations, including quality improvement activities	
3	Three types of legally required data uses:	Individuals do not control access to their data (i.e., individual authorization is not required). The minimum necessary standard also does not apply, but HIPAA sets other limits on how much data can be requested, used, or disclosed.
	Reporting of abuse, neglect, and domestic violence	
	Data required for judicial and regulatory proceedings	
	Data requested by law enforcement agencies	
4	Disclosures of existing data to health-care providers for use in treating patients.	Individuals do not control access to their data, and HIPAA sets no limits on how much data can be requested, used, or disclosed. Neither the minimum necessary standard nor an alternative standard applies.
	Uses of PHI by covered entities and HHS to ensure compliance with the Privacy Rule.	

HHS, US Department of Health and Human Services; HIPAA, Health Insurance Portability and Accountability Act of 1996; PHI, protected health information.

request is made, and they should be prepared to explain why they need the data to accomplish their purpose.[4] Congress clarified in 2009[18] that it is the data holder—the entity being asked to supply data—that is ultimately responsible for deciding how much data is the minimum necessary. Note, though, that this is judged relative to the *data user's* intended purpose.[19] This implies that data holders must ask questions about a requester's proposed use, before responding to a data request. To summarize, a HIPAA-covered researcher that requests too much information would, in theory, violate the Privacy Rule, but the HIPAA-covered data holder supplying the data bears ultimate responsibility to block an excessive data request.

Tier 3 includes legally required data disclosures, such as data requests from courts and law enforcement agencies.[20] HIPAA-covered data holders could be liable for obstructing justice if they applied the minimum necessary standard in a way that blocks these data flows. To avoid putting data holders in this position, HIPAA applies alternative protections (such as having courts subpoena the data) instead of asking covered entities to apply the minimum necessary standard.

In tier 4, a person's existing data can be shared without his or her authorization and with no minimum necessary limit on how much data can be shared. Not surprisingly, this approach applies only in narrow circumstances. Tier 4 permits unrestricted use and disclosure of data only for an institution's own HIPAA compliance activities, for Department of Health and Human Services regulatory oversight activities,[21] and for treatment purposes.[22] The first two—HIPAA compliance and oversight activities—place a burden on individual privacy to help maintain strong HIPAA privacy protections that presumably benefit the same individuals. For medical geneticists and researchers, a key question is how the data sharing for treatment purposes works. Can a geneticist share a patient's diagnosis or known molecular etiology only to help treat that same patient, or does HIPAA allow the data to be shared with a physician treating a relative of the patient or even with a physician treating a genetically similar individual with no familial relationship to the patient?

SHARING DATA FOR TREATMENT PURPOSES UNDER HIPAA

HIPAA's minimum necessary treatment exception is quite broad, as clarified in the following Office for Civil Rights guidance:

> The Privacy Rule allows those doctors, nurses, hospitals, laboratory technicians, and other health care providers that

> are covered entities to use or disclose protected health information, such as X-rays, laboratory and pathology reports, diagnoses, and other medical information for treatment purposes without the patient's authorization. This includes sharing the information to consult with other providers, including providers who are not covered entities, *to treat a different patient*, or to refer the patient.[23]

Consider the following examples:

> Your patient has developmental delay. His older cousin reportedly has similar issues. The cousin is currently in foster care, so you cannot simply ask family members. The cousin's geneticist has been unable to obtain his authorization to share data with you. Is it permissible for the cousin's geneticist to tell you the cousin's diagnosis to help confirm the diagnosis in your own patient?
>
> Your patient, who was treated for breast cancer several years ago at age 30, underwent testing that found no genetic cause. This implies that testing healthy family members for breast cancer pathogenic variants is not indicated. Your patient has not authorized data sharing. Does HIPAA permit you to tell her sister's physician that your patient tested negative?
>
> Your patient has a rare variant of uncertain significance. This variant has only been seen in a handful of patients to date. In advising your patient, it would be helpful to obtain information about the phenotypes and health outcomes observed in other people with that same variant. Can laboratories and clinicians share this information with you?

In all three cases, the answer is "yes." Neither individual authorization nor compliance with the minimum necessary standard is required[22] when data are requested for a treatment purpose. Data holders should, of course, check whether state law or their own institutional policies restrict access in this situation, but HIPAA's minimum necessary standard does not do so. This aspect of HIPAA understandably is controversial. It implicitly takes the position that an individual's privacy interests, while very important, should bend if they come into conflict with the physical well-being of another patient whose treatment requires access to information. Not everyone would agree.

The Privacy Rule does not explain its rationale for this broad treatment exception. One possible rationale is utilitarian. Broad data sharing for treatment purposes facilitates a learning health-care system that harnesses data from past treatment encounters to improve the care of future patients. This is especially beneficial in medical genetics, where all patients share an interest in having their care informed by data from genetically similar individuals. Yet HIPAA does not state a utilitarian rationale. The minimum necessary treatment exception ultimately may reflect two pragmatic concerns.

The first concern is that applying the minimum necessary standard in treatment settings could expose data holders to tort liability. A treating physician whose decisions harm a patient has a potential defense to malpractice liability if the patient or another party withheld information that could have led to better decisions. Liability for the injury then shifts to the party that withheld the information. A covered entity that applied the minimum necessary standard in a way that withheld information needed in patient care could face liability for resulting injuries. The treatment exception protects covered entities from liability by letting them err on the side of disclosing data that may be relevant to patient care.

A second concern is that the minimum necessary standard would be somewhat self-defeating in treatment settings. Suppose Jack's doctor needs access to Jane's PHI to inform treatment of Jack. To apply the minimum necessary standard, Jane's provider would need to receive detailed information about Jack's health, to use in determining how much of Jane's PHI is truly "necessary" to inform Jack's care. Protecting Jane's privacy (by applying the minimum necessary standard) would thus erode Jack's privacy (by forcing extensive disclosure of Jack's data to support a minimum necessary determination). The pragmatic solution, reflected in the Privacy Rule, is to allow unrestricted disclosure of Jane's data to Jack's physician who, after all, is already subject to strong state-law duties and, in all likelihood, institutional policies to keep medical records confidential. Transferring data from one HIPAA-protected environment to another one may entail little privacy risk.

The treatment exception has critics and supporters. The National Committee on Vital and Health Statistics recently recommended against changing it,[10] even though some other laws adopt a different approach. For example, the 21st Century Cures Act of December 2016 took a more cautious approach than HIPAA takes to the sharing of data from precision medicine initiative research subjects. The Cures Act allows disclosures that are "necessary for the medical treatment *of the individual to whom the information, document, or biospecimen pertains* and made with the consent of such individual."[24] It thus allows people's data to be used only to treat themselves and, even then, rather oddly requires them to consent for their doctors to use their own data. This provision of the Cures Act only applies to research data from the precision medicine initiative, so it does not affect the sharing of other data under HIPAA. In view of the many patient benefits that flow from broad sharing of genomic data in treatment settings, the genomic testing community should encourage the Office for Civil Rights to maintain HIPAA's policy of broad access to genomic data for treatment purposes.

CONCLUSION

HIPAA's minimum necessary standard applies to genomic data, but precisely how it applies and what it requires are uncertain and further regulatory guidance would be

useful. Researchers and clinicians should engage with policymakers to ensure well-informed policies that minimize deleterious impacts and compliance burdens. Appropriate characterization of data-sharing activities—as research, public health, or treatment-related—is also crucial. As the National Committee on Vital and Health Statistics recently noted, "genomic science is in an early and evolving stage that makes it difficult to assess which, and how much, genetic information will be necessary for specific tasks, such as conducting research into the clinical significance of specific genetic variants… It is difficult to say which genetic variants are the 'minimum necessary' to diagnose or study a disease, when new associations between genes and diseases are being discovered almost weekly."[10] Active engagement of genomic scientists would help regulators develop sound policies that afford individuals the full measure of privacy protection that HIPAA's minimum necessary standard aims to provide, while avoiding unintended impacts on innovation and clinical care.

ACKNOWLEDGMENTS

This work received support from NIH/NHGRI/NCI, UO1HG008657, UO1HG006507, and U01HG007307. B.E. has served on the National Committee for Vital and Health Statistics, but the views expressed here are her own and do not reflect views of the Committee.

DISCLOSURE

The authors declare no conflict of interest.

REFERENCES

1. Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (Aug. 21, 1996).
2. 45 C.F.R. pts. 160, 164.
3. US 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. *Fed Regist* 2013 Jan 25;78(17): 5566–5702.
4. 45 C.F.R. § 164.502(b)(1).
5. Id. at § 164.514(d)(3)(i) and at § 164.514(d)(4)(i).
6. EU Data Protection Directive (95/46/EC), Article 6. (Oct. 24, 1995).
7. General Data Protection Regulation (Regulation (EU) 2016/679), Article 5. (Apr. 27, 2016).
8. US Department of Health and Human Services. Top five issues in investigated cases closed with corrective action, by calendar year. 2017. https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/data/top-five-issues-investigated-cases-closed-corrective-action-calendar-year/index.html.
9. 45 C.F.R. § 164.514(d)(5).
10. National Committee on Vital and Health Statistics. Recommendation on the HIPAA minimum necessary standard. 2016. http://www.ncvhs.hhs.gov/recommendation-on-the-hipaa-minimum-necessary-standard/. pp 22–23.
11. Baker Donelson. The HIPAA police are coming—really. 18 March 2011. http://www.bakerdonelson.com/The-HIPAA-Police-are-Coming–Really-03-18-2011.
12. 45 C.F.R. § 164.508.
13. Id. at § 164.524.
14. Id. at § 164.506 and §§ 164.512 (a), (b), (d), (g), (h), (i), (j), (k), (l).
15. Id. at § 164.512(i).
16. Id. at § 164.512(b).
17. Id. at § 164.506.
18. Health Information Technology for Economic and Clinical Health ("HITECH") Act Div. A, Title XIII, and Div. B, Title IV, of Pub. L. 111-5, American Recovery and Reinvestment Act, 123 Stat. 115, at 226; see privacy provisions at Sec. 13001, codified at 42 U.S.C. § 17921 et seq.
19. 45 C.F.R.§ 164.514(d)(3)(i).
20. Id. at § 164.512(c), (e), and (f).
21. Id. at § 164.502(b)(2)(iv),(vi).
22. Id. at § 164.502(b)(2)(i).
23. US Department of Health and Human Services. FAQ guidance. 2013. http://www.hhs.gov/hipaa/for-professionals/faq/481/does-hipaa-permit-doctors-to-share-patient-information-for-treatment-without-authorization/index.html.
24. 21st Century Cures Act, Pub. L No. 114-255 (Dec. 13, 2016); see § 2012 (C)(ii) [emphasis added].