International Health Data: How HIPAA Interacts with the EU GDPR

Kelly Koeninger, Robinson Bradshaw & Hinson PA, and John Conley,
University of North Carolina-Chapel Hill and Robinson Bradshaw & Hinson PA

In the United States, health researchers, facilities serving as research sites, and providers of research data have long had to comply with the research-related privacy provisions of the Health Insurance Portability and Accountability Act (HIPAA). For research involving data collected in the European Union (EU), the EU's new privacy law, the General Data Protection Regulation (GDPR), has added a further level of complexity. This article outlines the research-related provisions of both HIPAA and the GDPR and then explains how they relate to each other, focusing on their similarities and differences, and concludes with some practical steps for compliance when both apply.

HIPAA

General Provisions of HIPAA

HIPAA governs the use and disclosure of protected health information (PHI) in the United States. HIPAA defines PHI to include information that relates to the mental or physical health of an individual, the provision of health care to an individual, or the payment for the provision of health care to an individual that also identifies the individual or could reasonably be used to identify the individual.[1] HIPAA only applies to a subset of entities—health plans, health care clearinghouses, and health care providers and their subcontractors who use PHI (i.e., business associates).[2]

HIPAA requires covered entities and their business associates to maintain the privacy and security of PHI. Generally, unless an exception applies, covered entities and business associates are not permitted to disclose or use PHI without an explicit authorization from a patient.[3] HIPAA does provide for fairly broad exceptions to this general rule, particularly for disclosure related to treatment, payment, and health care operations of covered entities.[4] There are also exceptions related to public safety, public health activities, and judicial and administrative proceedings, among others.[5] Data that has been "de-identified" (i.e., stripped of all identifying information) is also not subject to protection under HIPAA.[6]

Specific HIPAA Provisions Related to Research

HIPAA also governs when and how covered entities may use or disclose PHI for research purposes. HIPAA defines research as "a systematic investigation, including research, development, testing, and evaluation, designed to develop or contribute to generalizable knowledge."[7] Researchers are permitted to obtain, create, use or disclose PHI in the course of their research, but generally speaking, covered entities (e.g., teaching hospitals, physicians, etc.) have the underlying data required by researchers. For the covered entities to disclose that information to the researchers, the covered entities either must have the authorization of the patient to disclose such information for research purposes or have documented institutional review board (IRB) or privacy board approval to disclose the information without patient authorization.[8]

Since IRB approval of a waiver of a patient authorization can be a complicated process, many researchers instead choose to simply obtain patient authorization when the patient consents to participate in the study. In addition, covered entities are always permitted to provide de-identified information to researchers.

The EU GDPR

On May 26, 2018, the long-discussed GDPR[9] took effect in all EU countries, replacing the previous regime of country-by-country laws under the 1995 Data Protection Directive (DPD).[10] Whereas an EU Directive requires implementation by individual EU member states, the GDPR is a Regulation (much like a federal law in this country) that immediately became the law throughout the EU.[11] This unification of EU law affects the

collection, transmission, and use of all personal data, including health data. It is likely to have both costs and benefits for health care providers and health researchers who handle health-related data from people who reside in the EU.

General Provisions of the GDPR

The GDPR builds on and expands the privacy protections formerly provided by the DPD. The GDPR defines "personal data" to include any information from which a natural person can be identified—a "data subject."[12] It potentially applies to all "controllers" and "processors" of the personal data, regardless of their location. A processor is anyone who collects, manipulates, uses, or stores personal data; a controller is a party who directs or controls processing.[13] Controllers and processors outside the EU are subject to jurisdiction if they offer goods or services to "data subjects who are in the Union" or monitor their behavior.[14] Accordingly, the GDPR does not cover data collected from an EU citizen who is in the United States, but it may cover data collected from a U.S. citizen who is working in the EU. The legal obligations of controllers and processors are similar, but aggrieved data subjects have primary legal recourse against the controller.

Personal data must be processed lawfully, fairly, and transparently and can be collected only for "specified, explicit and legitimate purposes," and can be processed only in ways that are compatible with those purposes.[15] To meet the threshold requirement of lawfulness, processing must satisfy at least one of several criteria, including: the data subject has given specific, informed, and unambiguous affirmative consent (merely providing an opt-out right is insufficient); the processing is necessary to perform a contract with the data subject or for the controller to comply with a legal obligation; the processing is necessary to protect the vital interests of the data subject or someone else; or the "processing is necessary for the performance of a task carried out in the public interest" or "for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject."[16]

Where the processing relies on consent, subjects must be able to withdraw consent at any time and it must be as easy to withdraw consent as it is to give it, and controllers bear the legal burden of being able to demonstrate consent.[17] Parental consent is usually required for subjects under age 16.[18]

Data subjects are given several important rights, including:

- The right to be informed about data collection;[19]
- The right to access one's data;[20]
- The right to data portability;[21]
- The right to object to processing;[22]
- The right to rectify inaccurate data;[23] and
- The highly controversial (especially in free speech contexts) right to erasure, or "the right to be forgotten," when there is no longer a purpose for maintaining the data.[24]

For research involving data collected in the European Union (EU), the EU's new privacy law, the General Data Protection Regulation (GDPR), has added a further level of complexity.

EU Data Protection Authorities can fine violators up to 4% of gross revenues,[25] and data subjects also have private judicial remedies against controllers and processors.[26] Controllers bear ultimate responsibility for all processing operations in most cases.[27]

Exporting Data from the EU to the United States

Sending any kind of personal data from the EU to the United States is a significant problem, as it was under the DPD. Transferring personal data to the United States is presumptively illegal because the EU does not believe that United States data protection laws are adequate. All data transfers are covered—there is no general exception for intra-company transfers. There are four ways to overcome this presumption. Individual consent remains a valid basis for transfer.[28] In research projects, getting consent to transfer could presumably be part of obtaining informed consent to participate in the research. Absent consent, there are three principal options. First, the U.S. data importer can join the U.S. Department of Commerce's Privacy Shield,[29] whereby the U.S. participant self-certifies (annually) that it provides GDPR-level data protection. However, nonprofits cannot participate in the Privacy Shield because the rules are enforced by the Federal Trade Commission and nonprofits are not subject to its jurisdiction.[30] A second option is for the EU data exporter and U.S. importer to sign model contractual clauses promulgated by the EU under which the parties commit to GDPR-level protection.[31] The clauses cannot be modified in any respect. Finally, under the rarely used binding corporate rules option, a U.S. importer can write GDPR-level data protection into its charter.[32]

Specific GDPR Provisions Related to Health Data

The GDPR has a number of provisions relating to health data and scientific research. In general, the collection, use, and transfer of data for health and research purposes has become more uniformly regulated, an improvement over the DPD's patchwork of rules. However, the specific rules are complex and generally more onerous than under the former law.[33]

Health and genetic personal data, which are deemed "sensitive," are subject to special rules.[34] Processing such data is forbidden unless one of several conditions applies. They include:[35]

- The data subject has given "explicit" consent—a term that is not defined;
- To protect a data subject who is incapable of giving consent—as in the case of a medical emergency with an unconscious patient;

The biggest advantage of the GDPR for researchers is that it imposes a single set of rules throughout the EU, replacing the former patchwork of national laws under the DPD.

- The subject has already made the data public;
- As necessary to provide health care, as when one physician treating the subject needs data from another;
- To meet public health needs, such as protecting against cross-border threats to health or ensuring health care safety;
- For a variety of purposes "in the public interest," including, significantly, scientific research and archival or statistical purposes.

In several respects, scientific research receives some relief from the usual restrictions on the collection and processing of data. For example, anonymous data—which is not identifiable to a human subject—is not subject to the GDPR at all,[36] while pseudonymous data—which is not directly identifiable—is covered by the GDPR but enjoys favored status.[37] In addition, obtaining broad informed consent from a research subject at the outset of a project may support more extensive processing than the GDPR would otherwise permit.[38]

The biggest advantage of the GDPR for researchers is that it imposes a single set of rules throughout the EU, replacing the former patchwork of national laws under the DPD. (Individual member states have authority both to create additional research exceptions to the GDPR's general rules and to impose additional requirements,[39] though these should not be materially different from the GDPR's provisions.) In addition, the GDPR is intended to create "one-stop shopping" whereby a foreign controller can create an "establishment," or place of business, in one EU member state and use that as a base for EU-wide compliance, including the appointment of a representative to deal with the local data protection authority.[40] Overall, after some detailed preparation, researchers will probably find it easier to do research in the EU than under the former DPD.

Merging the Requirements of HIPAA and the GDPR

The collection and use of health data solely within the United States, whether for research, health care, or other purposes, continues to be governed by HIPAA (and applicable state laws in some cases) and is unaffected by the GDPR. However, any "processing"—any collection, use, or retention—of personal data that is identifiable to a person who is present in the EU must comply with the GDPR. Similarly, organizations that collect health data from persons located in the EU, for any reason, will have to comply with the strict requirements of the GDPR. Organizations that transfer health-related data from the EU to the United States must now comply with both legal regimes. Moreover, transferring EU data to the United States can only be done with explicit consent or pursuant to one of the approved transfer mechanisms described above.

Despite conceptual similarities, and some specific ones—such as the exclusion of anonymous data from coverage—the requirements of HIPAA and the Common Rule, on the one hand, and the GDPR, on the other, are not the same. Consequently, compliance with one cannot be assumed to ensure compliance with the other. Some of the most important practical differences are:

- Using an informed consent form that has been approved by a U.S. IRB under the revised Common Rule does not guarantee compliance with the GDPR's consent requirements. IRB approvals are done on a case-by-case basis, whereas the GDPR's demanding standards can rarely if ever be waived. If an organization is collecting health data in the EU on the basis of consent, it should begin with the GDPR's requirements and make sure that its U.S. informed consent documents meet that standard.
- The rights of EU data subjects under the GDPR go well beyond what is typically included in a U.S. informed consent document—for example, the GDPR's rights of access, rectification, and erasure. Organizations that will collect or otherwise process EU data must familiarize themselves with these rights at the outset of every project. Here again, U.S. IRB approval and HIPAA compliance may be insufficient.
- The GDPR's one-stop shopping rule is a two-edged sword. It should simplify compliance in almost every case. But it also imposes requirements, including appointing a representative and notifying the data protection authority in the chosen EU country, that cannot be ignored.
- Transferring EU data to the United States is often the most challenging part of the process. It is doable, often by consent, but the rules are precise and usually unyielding, so this is another issue that must be dealt with at the design phase of any international health data project.

A final point concerns the enforcement efforts by the EU and member state data protection authorities during the GDPR's first year. The imposition has been relatively rare so far, but the frequency is increasing. The factors that have triggered the largest penalties include intent, such as when a violator ignored a problem it was aware of or deliberately ignored the GDPR; the scope of the impact; and the sensitivity of the data. Health data, of course, is always deemed to be sensitive. Conversely, inadvertent violations by organizations attempting to follow the law have provoked few significant penalties, even though the GDPR sets a strict liability standard in most instances. The lesson for U.S. organizations that collect or use EU health-related data is that diligence about the GDPR from start to finish of a project, while not a safe harbor, is likely to reduce the extent of any penalties in the event of a violation.

Kelly Koeninger focuses her practice exclusively on health care regulatory and transactional matters. She brings a global approach to health care deals and compliance issues by incorporating an understanding of federal and state fraud and abuse laws (including Stark and the Anti-Kickback Statute), state corporate practice of medicine rules and privacy laws with an extensive background in corporate and commercial transactions. Kelly's transactional experience includes the negotiation of complex joint venture transactions between regulated entities and providers as well as mergers and acquisitions, physician recruitment and employment agreements, physician investments in ambulatory surgical centers, formation of clinically integrated networks and hospital service line co-management agreements. She also regularly counsels clients on HIPAA and data privacy and breach matters.

John M. Conley is William Rand Kenan, Jr. Professor of Law at University of North Carolina-Chapel Hill. He holds an AB from Harvard and a JD and PhD in anthropology from Duke. In law school, he was Editor in Chief of the *Duke Law Journal.* He teaches civil procedure, intellectual property, and the law of biotechnology, and has written several books and numerous articles on genomics and the law, the law of intellectual property as applied to emerging technologies, scientific evidence, and other topics in law and science. His article (with Roberte Makowski), *Back to the Future: Rethinking the Product of Nature Doctrine as a Barrier to Biotechnology Patents,* was cited by both lower courts in the *AMP v. Myriad Genetics* gene patent case. In his most recent research, he focused on the culture and day-to-day practices of genomic medicine. Conley is of counsel to the law firm of Robinson Bradshaw & Hinson of Charlotte and Chapel Hill, NC, where he practices in intellectual property, biotechnology, privacy, and international law. He is also the editor of the blog *The Privacy Report* and speaks regularly on issues of law and science to audiences in the United States and internationally.

AHLA thanks the leaders of the Business Law and Governance Practice Group for contributing this feature article: **Glenn Prives**, McElroy Deutsch Mulvaney & Carpenter LLP, Morristown, NJ (Chair); **John B. Garver**, Robinson Bradshaw & Hinson PA, Charlotte, NC (Vice Chair—Educational Programming); **Judy W. Mayer**, Inspira Health Network, Woodbury, NJ (Vice Chair—Member Engagement); **M. Daria Niewenhous**, Mintz Levin Cohn Ferris Glovsky & Popeo PC, Boston, MA (Vice Chair—Publishing); **David A. Weil**, Quorum Health Corporation, Brentwood, TN (Vice Chair—Publishing); and **Susan F. Zinder**, Law Office of Susan F. Zinder, New York, NY (Vice Chair—Educational Programming).

Endnotes

1 45 C.F.R. § 160.103.
2 *Id.*
3 45 C.F.R. § 164.502.
4 45 C.F.R. § 164.506.
5 45 C.F.R. § 164.512.
6 45 C.F.R. § 165.502(d).
7 45 C.F.R. § 164.501.
8 45 C.F.R. § 164.508 and 45 C.F.R. § 164.512(i).
9 Regulation 2016/679, 2016 O.J. (L 119) (EU).
10 Council Directive 95/46/EC, 1995 O.J. (L 281) 31.
11 *Regulations, Directives and Other Acts*, Eur. Union, https://europa.eu/european-union/eu-law/legal-acts_en.
12 Regulation 2016/679, at art. 4(1).
13 *Id.* at art. 4(2), (7)-(8).
14 *Id.* at arts. 2-3.
15 *Id.* at art. 5.
16 *Id.* at arts. 6-7.
17 *Id.* at art. 7.
18 *Id.* at art. 18.
19 *Id.* at arts. 13-14.
20 *Id.* at art. 15.
21 *Id.* at art. 20.
22 *Id.* at art. 21.
23 *Id.* at art. 16.
24 *Id.* at art. 17.
25 *Id.* at art. 83(5).
26 *Id.* at art. 79.
27 *Id.* at art. 24.
28 *Id.* at art. 49(1).
29 *See Privacy Shield Program Overview,* Privacy Shield Framework, https://www.privacyshield.gov/Program-Overview.
30 *See generally* Privacy Shield Framework, https://www.commerce.gov/page/how-join-privacy-shield-guide-self-certification (last visited Mar. 7, 2018).
31 GDPR, at arts. 46(2)(c)-(d), 93(2).
32 *Id.* at art. 47.
33 *See id.* at recitals 159-62, arts. 5(b), 5(e), 9.
34 *Id.* at art. 9.
35 *Id.* at art. 9(2).
36 *Id.* at recital 26.
37 *Id.* at recitals 26-29, arts. 4(e), 25(1), 32(1)(a), 89(1).
38 *See id.* at recital 33.
39 *Id.* at art. 89.
40 *Id.* at arts. 27, 60.