The Broad Reach of the GDPR: Europe's New Data Protections and Their Impact on U.S. Health Care Entities

By Jill Raines, University of Oklahoma; Adam Laughton, Seyfarth Shaw LLP; and Ashley Thomas, Baker Donelson

The General Data Protection Regulation (GDPR)[1] was approved and adopted by the European Union (EU) Parliament in April 2016 and became effective in May 2018, with the aim of protecting the processing of data subjects' personal data and ensuring the free movement of such data throughout the international economy. Unlike the Data Protection Directive it replaced (the Directive),[2] GDPR has direct effect and immediate application to European Economic Area (EEA) member states, without the need for transposition into national law of individual member states.[3]

United States (U.S.)-based academic medical centers (AMCs), contract research organizations (CROs), industry sponsors, and other entities involved in the research process interact often with personal data that are subject to GDPR. U.S.-based health care entities arguably are well—or better—positioned to implement GDPR compliance programs given their generally high degree of regulation by the Health Insurance Portability and Accountability Act (HIPAA), Food and Drug Administration (FDA), and other sources. Yet GDPR, with its application across all economic sectors and regulation of broad categories of data and processing activities, is unlike anything many U.S. entities have encountered.

This article provides an overview of GDPR's key concepts and delves into issues of particular relevance to U.S.-based health care entities engaged in research and clinical activities that may invoke GDPR requirements and enforcement.

Key Concepts[4]

Entities must determine whether GDPR applies to their research or clinical activities. If so, they must ensure there is a legal basis for processing personal data and, if personal data are moving from the EEA to a non-EEA jurisdiction that lacks certain protections, a basis to transfer those data.

Jurisdiction

GDPR greatly expands the extraterritorial reach of European privacy law. U.S.-based entities typically had been subject to the Directive if "established in" the EEA by virtue of operating an office, subsidiary, or campus in the EEA (i.e., by having a physical presence in the EEA). While GDPR also applies to processing activities of entities established in the EEA, it includes two additional jurisdictional "hooks" covering entities that (1) offer goods or services to individuals in the EEA, regardless of whether payment is required; or (2) monitor the behavior of individuals in the EEA.[5]

With "Brexit" on the horizon, the United Kingdom (UK) passed the Data Protection Act 2018 (DPA 2018) only days before GDPR's effective date. DPA 2018 largely tracks GDPR, with a few key differences—e.g., certain functions and powers of the UK Information Commissioner's Office (ICO), which acts as the UK's designated "supervisory authority" under GDPR.

Personal Data, Including Special Categories

Personal data are defined broadly compared to the Directive and to U.S. legal regimes. For example, personal data include identifying information of EEA health care providers, such as institutional staff (e.g., principal investigators, study staff) and other individuals who are not study participants or patients.

Personal data include any information relating to an identified or identifiable natural person (i.e., a data subject).[6] An identifiable natural person can be identified, directly or indirectly, by reference to an identifier (e.g., name, identification number, online identifier) or to factor(s) specific to the person's physical, physiological, genetic, mental, economic, cultural, or social identity. "Special categories" of personal data reveal racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and concern processing of genetic data, biometric data used to uniquely identify a person, data concerning health, and data concerning a person's sex life or sexual orientation.

Processing

Processing includes operation(s) performed on personal data or on sets of personal data, whether or not by automated means, including collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure, alignment or combination, restriction, erasure, or destruction.[7]

Controllers and Processors

GDPR applies to controllers—persons or entities that determine the purposes and means of processing personal data—and to processors—persons or entities that process personal data on behalf of controller(s).[8] This distinction is similar to the distinction under HIPAA between covered entities (controllers) and business associates (processors).

Data Subjects

GDPR is agnostic to data subjects' citizenship. For example, EEA citizens employed and residing in the U.S. generally will not be covered by GDPR, yet U.S. citizens working at an EEA branch of a U.S. entity and residing in the EEA generally will be covered by GDPR.

Legal Bases for Processing

Processing is lawful under GPDR only to the extent there is an Article 6 legal basis, including (but not limited to) processing: (a) consented to by the data subject; (b) necessary for the controller's "legitimate interests," unless overridden by the data subject's interests or fundamental rights or freedoms; (c) necessary to comply with legal obligation(s); and (d) necessary to protect a data subject's (or other individual's) "vital interests."[9] Processing special categories of personal data is prohibited unless one of certain Article 9 exceptions is met, including (but not limited to) processing: (1) to which the data subject has provided "explicit consent"; (2) necessary for reasons of public interest in the area of public health (e.g., ensuring high standards of quality and safety of health care and medical products); and (3) necessary for statistical or scientific research purposes.

Legal Bases for Transfer[10]

GDPR places restrictions on transfers of personal data from the EEA to countries outside the EEA, and (with limited exceptions) requires at least one of the following conditions be met:

- The European Commission has deemed the country receiving the data to have an adequate level of protection for data, including so-called "white listed" jurisdictions, such as Switzerland, Israel, and U.S. for-profit entities with EU-US Privacy Shield certification;[11]
- The controller or processor has appropriate safeguards in place, including standard data protection clauses (a.k.a., standard or model contractual clauses), binding corporate rules, or codes of conduct;[12] or
- The transfer of personal data fits within certain derogations for specific situations, including when the data subject has explicitly consented to the transfer after being informed of the possible risks of the transfer due to the absence of an adequacy decision and appropriate safeguards.[13]

Penalties

GDPR provides several penalty options for violations of its terms, including (a) administrative fines; (b) reprimand, if a minor infringement or fine would be a disproportionate burden to an individual; and (c) as may be promulgated by individual member states, criminal penalties for violations of GDPR or of national rules adopted pursuant to GDPR.[14] Significantly and

GDPR greatly expands the extraterritorial reach of European privacy law.

unlike HIPAA, GDPR provides data subjects with a private right of action, including the right to bring a class action suit.[15] GDPR administrative fines may be assessed against controllers or processors and, depending on the violation, have an upper limit of the greater of (1) 10 million Euros or 2% of global annual turnover (e.g., for failure to notify data subjects of data breach) or (2) 20 million Euros or 4% of global annual turnover (e.g., for failure to honor data subjects' rights of access and rectification).

Given these significant penalties, the apportionment of responsibilities and risk between contracting entities becomes all the more important, as discussed below.

Entities that are accustomed to receiving key-coded data that may be considered de-identified according to HIPAA standards (and thus outside the scope of HIPAA) must separately consider whether the data they receive are anonymized according to GDPR standards (and thus outside the scope of GDPR).

GDPR and Research

Examples

The following scenarios illustrate GDPR's application to the clinical trial activities of U.S.-based entities:

- A research sponsor or vendor is collecting personal data from individuals within the EEA. GDPR applies regardless of where the sponsor and vendors are established and regardless of where processing is performed. For example, a U.S.-based AMC monitors the behavior of individuals in the EEA through a mobile application that collects research data from those individuals.
- A U.S.-based CRO actively recruits individuals from around the world (including the EEA) to participate in its clinical trials, and one of those clinical trials is carried out in France. GDPR applies because the CRO actively is advertising to data subjects in the EEA, thus offering its goods or services, and because it is collecting personal data from EEA-based data subjects, thus monitoring their behavior. In contrast, a U.S.-based CRO that recruits, advertises, and collects information only from individuals located in the U.S. and carries out the research study in the U.S. would not be subject to GDPR, even if an EEA citizen, living in the U.S., were to participate in the study. In the latter scenario, the U.S.-based organization is not established in the EEA; has not actively offered, recruited, or advertised to individuals in the EEA; and is not monitoring the behavior of individuals in the EEA. However, the outcome of this scenario could change if the individual returns to the EEA and the U.S.-based CRO continues to monitor the individual's activities as part of the study.
- A U.S.-based AMC (controller) uses an EU-based cloud storage vendor (processor), with subjects' data transferred from the U.S. to the EU-based storage site. Because the vendor is established in the EEA, its processing activities are subject to GDPR. Also, while no basis for transfer would be required in moving data from the U.S. to the EU (e.g., standard contractual clauses), the transfer of data from the EU-based vendor to the U.S.-based AMC would require a basis for transfer given that it is moving from the EEA to the U.S., arguably even if data are not altered by the vendor.

Using Personal Data for Research Purposes

Anonymized and Pseudonymized Data. GDPR does not apply to data that have been anonymized, just as HIPAA does not apply to data that have been de-identified. Unlike HIPAA, however, GDPR includes no "safe harbor" for anonymization—i.e., there is no defined set of variables that, if removed from a dataset, render the data anonymized. Rather, GDPR utilizes a facts-and-circumstances test to determine whether data are no longer identifiable, taking into account "all the means reasonably likely to be used . . . [e]ither by the controller *or by another person* to identify the natural person directly or indirectly."[16] GDPR also defines pseudonymized data, which are data that "can no longer be attributed to a specific data subject without the use of additional information, as long as such additional information is kept separately and subject to technical and organizational measures to ensure non-attribution to an identified or identifiable individual"[17] (e.g., key-coded data).

Entities that are accustomed to receiving key-coded data that may be considered de-identified according to HIPAA standards (and thus outside the scope of HIPAA) must separately consider whether the data they receive are anonymized according to GDPR standards (and thus outside the scope of GDPR). However, pseudonymized data generally remain subject to GDPR because "another person," somewhere in the world, would be able to identify the data subject, such that it is not anonymized under the above facts-and-circumstances test.

Consent as Basis for Processing Personal Data. As described at Section I, GDPR Article 6 requires a specific basis for processing personal data and, to the extent such processing involves special categories of personal data (e.g., health data), GDPR Article 9 requires a specific exception to processing. Explicit consent of the data subject meets both of these requirements. Consent must be freely given, specific, and informed, and must be provided via an unambiguous indication of the data subjects' wishes (e.g., consent cannot be inferred from silence, pre-ticked boxes, or inactivity).[18] Explicit consent indicates that the quality of consent is more than a statement or clear affirmative action, and may require that consent be in writing or documented in some type of permanent record.

Historically, the research community has relied upon consent to meet its obligations under applicable privacy law. Yet under GDPR, entities should consider the pros and cons of continued reliance, as well as the ambiguities around consent, as a basis for processing—including as discussed in guidance promulgated by the Article 29 Data Protection Working Party (Working Party)[19] and guidance trickling in from various supervisory authorities in the UK, France, Germany, and other EEA jurisdictions.

To begin, it will be important for entities relying on consent as a basis for processing to keep abreast of the opinions of the supervisory authorities relevant to such entities' operations. For example, to date, certain regulatory authorities have signaled disapproval or disfavor of consent as a basis for processing in the research context (e.g., UK), while others have signaled strong preference for consent (e.g., Germany). Such disparate views could necessitate that entities operating in multiple EEA jurisdictions rely on different bases for research-related processing depending on supervisory authorities' views in those jurisdictions.

Also, in April 2018, the Working Party issued final guidelines on consent under GDPR, containing potentially problematic interpretations for the research community. GDPR Recital 33 recognizes that "it is often not possible to fully identify the purpose of personal data processing for scientific research purposes at the time of data collection."[20] However, the Working Party guidelines assert that "Recital 33 does not disapply the obligations with regard to the requirement of specific consent," such that consent must include a "well-described purpose" of the processing to be conducted, and that Recital 33 will be subject to a "stricter interpretation" when special categories of data are processed on the basis of explicit consent.[21] Furthermore, to the extent research purposes cannot be fully specified at the start of the research project (often as is the case of future research), researchers "must seek other ways to ensure the essence of the consent requirements are served best," such as consenting subjects at multiple points in the research as details of the research become known, or providing data subjects with a research plan specifying the research questions and methods envisaged.[22] Such statements, however, suggest a lack of understanding among regulators regarding typical research practices and how investigators, study sites, sponsors, and other players in the research process actually interact with participants. As interpreted by the Working Party, GDPR appears to take a more restrictive approach to consent for future research purposes than does HIPAA or the Common Rule.[23]

Finally, consent as the processing basis raises another potential problem for researchers—withdrawal. The Working Party recognizes that a data subject's withdrawal of consent could "undermine" research that requires data that can be linked to data subjects, yet states that a controller "must in principle delete the personal straight away" after receiving a data subject's withdrawal request.[24] Nonetheless, there is a possible reconciliation within GDPR itself, which permits continued processing after withdrawal to the extent there is another purpose justifying continued retention, that such purpose has its own separate legal basis for processing, and that data subjects were informed (at the outset) of such separate purpose and processing basis. For example, a research consent may tell subjects that, if they withdraw their consent to processing for purposes of the study, researchers will continue to process their data to meet adverse event monitoring requirements and for trial integrity purposes as necessary for reasons of "public interest in the area of public health, such as . . . ensuring high standards of quality and safety of health care."[25]

Data Subjects' Rights. GDPR gives individuals certain rights, including to make specific requests to controllers regarding personal data. Data subjects have the right to access their personal data that are being processed by the controller, including metadata, from a clinical trial.[26] (This contrasts with HIPAA, which permits the suspension of individuals' rights to access their health information while the clinical trial is in progress.)

In addition to the right of access, GDPR creates a new right for data subjects known as the "right to erasure" or "right to be forgotten," which permits an individual to request that the controller delete personal data the controller has about the individual under specific circumstances (e.g., when the individual withdraws consent or objects to processing).[27] The controller should grant the request for erasure without undue delay, meaning that the request for erasure should be granted within one month of the receipt of the request, subject to certain exceptions.[28]

Granting an individual's request for erasure of certain personal data could negatively affect the progress of a clinical trial, by preventing use of such data and otherwise jeopardizing a study's integrity. GDPR addresses this concern by providing an exemption for scientific research if the erasure of information is likely to "render impossible or seriously impair the achievement of the objectives of that processing."[29] Clinical trial researchers are permitted to deny participants' erasure requests to the extent researchers can demonstrate that granting the request would defeat or impair the clinical trial.

To the extent consent is used to provide notice requirements under GDPR Articles 13 or 14, such consent must describe subjects' rights and, as a practical matter, should inform subjects that these rights may be subject to certain exceptions (as described above), e.g., to ensure the reliability and accuracy of the research.

AMCs, research sponsors, CROs and other entities engaged in research must carefully manage their risk under GDPR (e.g., data breach obligations and penalties) via the negotiation of indemnification, limitation of liability, and insurance provisions.

Data Breach. GDPR imposes data breach reporting obligations on both controllers and processors, similar to breach notification requirements for covered entities and business associates under HIPAA. A personal data breach is a breach of security that leads to accidental or unlawful destruction, loss, alteration, unauthorized or disclosure of or access to personal data that are transmitted, stored, or otherwise processed.[30]

Data subjects must be notified of a breach without undue delay to the extent such breach is likely to result in a high risk to an individual's rights and freedoms (with limited exceptions). Organizations also must notify the appropriate supervisory authority without undue delay, where feasible, but no later than 72 hours after discovering the breach,[31] which is a much shorter timeframe than that required under HIPAA and most U.S. state data breach laws.

Compliance via Contracting

Selecting and Contracting with CROs. Many research sponsors and institutions utilize CROs to manage logistical and administrative tasks associated with clinical trials.[32] Depending on the trial structure and site, the CROs, trial sponsors, and host institutions may be subject to different responsibilities and obligations under GDPR.

GDPR Article 28 specifies that controllers may only engage processors that provide "sufficient guarantees" that they have the appropriate resources and expertise to comply with GDPR and ensure the protection of data subjects' rights. With CROs typically acting as processors, trial sponsors and institutions contracting with CROs (particularly those not based in the EEA) should determine whether such CROs have experience with trials in the EEA and have tested their GDPR compliance. For example, a trial sponsor evaluating a potential CRO may want to review the CRO's policies and procedures for pseudonymization procedures, to determine if they will reduce risk of data subject identification under GDPR standards, and to include a representation in applicable contracts that the CRO has policies and procedures that do so.

Assigning GDPR Responsibilities and Apportioning Risks. All research contracts should delineate clearly all GDPR roles and responsibilities, including that parties are acting as controller and, as applicable, how roles and responsibilities will be apportioned between joint controllers. Controllers are expected to set limits and parameters regarding processors' use of personal data and to monitor processor adherence to those limits and parameters. In the case of joint controllers, the contract should (among other things) clearly discuss how the joint controllers will handle data subjects' exercise of various rights and how they will satisfy data subject notification requirements under GDPR Articles 13 and 14.[33] Also, controllers must ensure that processors have agreed to contractual terms that meet certain requirements, which require processors to (among other things) act only on instruction of the controller, commit themselves to confidentiality, and assist the controller in complying with its GDPR obligations.[34]

As a general matter, most sponsors and, arguably, study sites will act as controllers of personal data. Sponsors may delegate certain responsibilities to CROs as part of their role in research administration and management, but generally such CROs still would be acting under the direction of such sponsors, even if carrying out certain delegated obligations. One exception may be, for example, if a CRO carries out a Phase 1 study at its own facilities, thus acting like a study site.

To the extent that a study sponsor is not established in the EEA and determines that it must have an EEA representative, it may ask the CRO to act as the sponsor's EEA representative, to the extent such CRO is established in one of the member states in which data subjects whose data are processed are located.[35] Also, to the extent data will be moving from the EEA to a non-EEA jurisdiction, the parties should ensure that they have arranged for a proper legal basis for such transfer (e.g., standard contractual clauses).

AMCs, research sponsors, CROs, and other entities engaged in research must carefully manage their risk under GDPR (e.g., data breach obligations and penalties) via the negotiation of indemnification, limitation of liability, and insurance provisions. Particular attention should be paid to the obligations of each party to indemnify the other, including when both parties may be at fault, and to evaluate carefully whether to accept any limitations on indemnification generally or specifically as to GDPR non-compliance.

Counsel should recommend review of current insurance policies to determine what coverage exists for GDPR-related losses, including for harm caused to data subjects, with insurance limits evaluated in light of potentially hefty GDPR penalties.[36] Entities involved in research activities that invoke GDPR requirements should consider whether to obtain specialized data breach insurance, particularly as more traditional general or professional liability insurers exclude or deny coverage for losses related to data breaches.

Conclusion

AMCs, CROs, and other entities involved in research and clinical activities should be especially vigilant as to the application of GDPR to their activities and its effect on their core functions, including performing research and soliciting participants. Reliance on existing HIPAA or other business practices likely will be insufficient for GDPR compliance. Because the consequences of failing to comply with GDPR can be great, these entities should work with counsel to ensure their compliance programs address GDPR requirements and build-in ongoing monitoring activities around such compliance.

Reliance on existing HIPAA or other business practices likely will be insufficient for GDPR compliance.

Thanks go out to the leaders of Academic Medical Centers and Teaching Hospitals Practice Group (AMCTHPG) for contributing this feature article: **Leah A. Voigt**, Spectrum Health System, Grand Rapids, MI (Chair); **Jessica M. Baker**, The State University of New York Buffalo, Buffalo, NY (Vice Chair—Membership); **Amy Bolian**, McLean, VA (Vice Chair—Publications); **Michael B. Lampert**, Ropes & Gray LLP, Boston, MA (Vice Chair—Research & Website); **Ted Lotchin**, WakeMed, Raleigh, NC (Vice Chair—Strategic Planning and Special Projects); **Gelvina Rodriguez Stevenson**, The Children's Hospital of Philadelphia, Philadelphia, PA (Vice Chair—Educational Programs); **David J. Vernon**, Hooper Lundy & Bookman PC, Washington, DC (Social Media Coordinator).

Authors

Jill Bush Raines serves as the Assistant General Counsel and University Privacy Official at the University of Oklahoma, where she directs and is responsible for the HIPAA compliance program for the University's three campuses. Within the Office of Legal Counsel, Jill's responsibilities include advising on regulatory matters and serving as assigned counsel to various campus areas including the Office of Compliance and the Office of Research Administration.

Adam Laughton is a Senior Associate in the Corporate department of Seyfarth Shaw LLP's Houston office. His practice focuses on providers and entrepreneurs in the health care industry.

Ashley Thomas is an Associate in the Washington, DC office of Baker Donelson. Ashley provides counsel to a broad range of health care industry clients on a wide variety of regulatory compliance matters. She currently serves as the Vice-Chair of Research and Website for AHLA's Public Health System Affinity Group.

Editor

Leslie Thornton, PhD, JD is a Senior Associate at Ropes & Gray LLP practicing in the health care group. Leslie advises clients on a broad range of compliance, regulatory, and transactional issues, with a primary focus on research matters, including pre-clinical and clinical trials, federal grants and contracts, research misconduct, government enforcement, and privacy (HIPAA, GDPR). She works with academic medical centers, universities, research institutes, pharmaceutical and medical device manufacturers, health-focused startups, and other health care organizations, and has completed secondments within the in-house research and development legal divisions of two manufacturers.

Endnotes

1 Regulation (EU) 2016/679 of European Parliament and of Council of 27 April 2016 on the protection of natural persons with regard to processing personal data and on the free movement of such data, and repealing Directive 95/46/EC.
2 Directive 95/46/EC of European Parliament and of Council of 24 October 1995 on the protection of individuals with regard to processing person data and on the free movement of such data.
3 The EEA is comprised of the 28 member states of the European Union (EU), Iceland, Liechtenstein, and Norway.
4 GDPR Article 4 (Definitions) and, as to Sensitive Data, GDPR Article 9.
5 GDPR Article 3 (Territorial Scope).
6 GDPR Article 4(1).
7 GDPR Article 4(2).
8 GDPR Article 4(7) & 4(8).
9 GDPR Article 6.
10 *See generally* GDPR Chapter V (Transfers of personal data to third countries or international organisations).
11 GDPR Article 45 (Transfers on the basis of an adequacy decision). *See also* Adequacy of the protection of personal data in non-EU countries, https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en.
12 GDPR Article 46 (Transfer subject to appropriate safeguards).
13 GDPR Article 49 (Derogations for specific situations).
14 GDPR Recitals 148–149 and 152, and Articles 83–84.
15 GDPR Articles 80 and 82.
16 GDPR Recital 26 (emphasis added).
17 GDPR, Article 4.
18 GDPR, Article 4(11).
19 The Working Party is an advisory body comprised of representatives from various EU data protection authorities, including the European Commission.
20 GDPR, Recital 33.
21 Working Party Guidelines on Consent under Regulation 2016/679 (last revised and adopted Apr. 10, 2018) at 28.
22 Working Party Guidelines at 29.
23 HIPAA authorizations may permit future research, provided the future research is described adequately in the authorization so that an individual reasonably could expect that PHI could be used or disclosed for the future research. *See* 78 Fed. Reg. 5566, 5611–13 (Jan. 25, 2013). Similarly, the 2017 revisions to the Common Rule formalize the concept of "broad consent" through which research subjects can provide consent to future research described in such a fashion that a reasonable person giving the consent for future research would have expected the broad consent to permit the types of research conducted. *See* 82 Fed. Reg. 7149, 7219–7223 (Jan. 19, 2017).
24 Working Party Guidelines at 29–30.
25 GDPR Article 9(2)(i).
26 GDPR Article 15.
27 GDPR Article 17
28 GDPR Article 12(3)–(4).
29 GDPR Article 17(3).
30 GDPR Article 4(12).
31 GDPR Articles 33, 34.
32 As of 2017, one survey stated that clinical trial sponsors utilized CROs in about 45% of trials, and overall 64% of clinical development services were outsourced to CROs. Mathini Ilancheran, *Analyzing the Top Clinical Trial Outsourcing Trends of 2017*, Clinical Leader (Dec. 28, 2017), https://www.clinicalleader.com/doc/analyzing-the-top-clinical-trial-outsourcing-trends-of-0001.
33 GDPR Article 21.
34 GDPR Article 22.
35 GDPR Article 27.
36 *See* GDPR Article 83.