Ropes & Gray
8 December 2022

Research, Development and Regulatory Roundtable

Impact of International Privacy Laws on Research – Challenges and Solutions

Discussion Paper and Guide[1]

In an increasingly connected world, clinical trials and other research activities are no longer state- or country-specific. Not surprisingly, the globalization of research activities creates any number of legal and compliance challenges for stakeholders involved in the development, authorization, and commercialization of medicinal products, including under data privacy regulations that continue to evolve.

The December 13, 2022 meeting of the Research, Development and Regulatory Roundtable of the Multi-Regional Clinical Trials Center of Brigham and Women's Hospital and Harvard and Ropes & Gray LLP ("MRCT R3") will tackle some of the most pressing of these challenges. For example, we will address issues that go to the heart of the General Data Protection Regulation ("GDPR") of the European Union ("EU"), such as what constitutes a restricted international data transfer,[2] the appropriate lawful basis to legitimize the processing of personal data in the context of clinical trials and secondary research,[3] and the designations of parties participating in research as controllers and processors.[4] We will also discuss potential solutions to problems that continue to challenge the research community, including in relation to the provision of notice or "fair processing" information to data subjects in scenarios in which the controller does not have contact with data subjects. Additionally, we will review how parties may receive, utilize, and share data for secondary research purposes, including in connection with real world evidence ("RWE") projects.

The research community has been awaiting further guidance on the topic of the GDPR and research from the European Data Protection Board ("EDPB") for several years.[5] Initially forecast to issue in 2021, as we reach the end of 2022, such guidance has still not been released. The research community must thus navigate several complex issues in the absence of relevant regulatory guidance. The MRCT R3 hopes to elicit current challenges and practical solutions through a series of panels made up of experts from the life sciences industry, government, and academia to address key challenges faced by the research sector under the GDPR. These panels will address the following topics:

---

[1] This discussion paper was prepared by David Peloquin and Edward Machin of Ropes & Gray LLP.

[2] Principle 14 of the Privacy Shield Framework Principles (the "Principles") states that a transfer from the EU to the U.S. of key-coded or pseudonymized data does *not* constitute a transfer of personal data that is subject to the Principles. By contrast, Recital 26 of the GDPR makes clear that pseudonymous data remain personal data and are thus within the scope of the Regulation, including in respect of transfers of personal data to third countries.

[3] For example, we continue to see organizations — in the EU, the U.S., and further afield — conflate (i) the *requirement* to obtain informed consent from trial participants for the purposes of the International Council for Harmonisation of Technical Requirements for Pharmaceuticals for Human Use's Good Clinical Practice, and (ii) the *option* to obtain the participants' consent for the purposes of legitimizing the processing of personal data (including special categories of personal data) in the context of the clinical trial.

[4] While the GDPR technically applies throughout the European Economic Area ("EEA"), which includes the 27 EU member states plus Iceland, Liechtenstein, and Norway, we use the term "EU" throughout this paper as a matter of efficiency. References herein to the EU should generally be read also to include the EEA.

[5] *See*, *e.g.*: (i) EDPB, *EDPB Document on response to the request from the European Commission for clarifications on the consistent application of the GDPR, focusing on health research*, February 2021; and (ii) Ropes & Gray, LLP *New European Data Protection Board (EDPB) Guidance Highlights – but Leaves Unresolved – Several GDPR Compliance Issues Facing Clinical Researchers*, February 2021.

1. Cross-Border Transfers: The EU to the U.S. and Beyond

2. Bases for Processing Personal Data for Clinical Research, Transparency, and Status of Parties as Controller vs. Processor

3. Secondary Research Under the GDPR

4. Anonymization and Pseudonymization

This discussion paper describes these and other topics that we will be addressing at the roundtable, including suggested questions to be discussed by each panel. However, we would strongly encourage attendees — both in person and virtually — to also consider any questions, comments, or concerns that you would like the panelists to discuss. As is the custom of MRCT R3 meetings, we will produce a discussion paper coming out of the meeting that synthesizes key points of discussion, offers potential solutions, and highlights items for further discussion.

1. Cross-Border Transfers: The EU to the U.S. and Beyond

Standard Contractual Clauses

- The European Commission ("Commission") standard contractual clauses ("SCCs") of June 4, 2021 remain the safeguard most commonly used by research stakeholders to transfer personal data from the EU to the United States ("U.S.") and other "third countries" that lack an "adequacy decision" from the European Commission. Unless and until the European Commission finalizes an "adequacy decision" based on the Trans-Atlantic Data Privacy Framework to which it agreed in principle in March 2022[6] — which, we understand, is tentatively expected to be issued in the first half of 2023 — the use of SCCs will continue as the status quo for transfers of personal data from the EU to the U.S. Moreover, because any adequacy decision issued pursuant to the Trans-Atlantic Data Privacy Framework will legitimize transfers of personal data only to U.S. entities that self-certify to the EU-U.S. Privacy Shield ("Privacy Shield") (or its successor certification scheme), SCCs are likely to remain the primary basis used to legitimize transfers of personal data from the EU to geographies located outside of the U.S. Additionally, because we understand that the revised Privacy Shield is unlikely to be available to nonprofit organizations, we expect many research data transfers to the U.S. that involve data transfers to nonprofit organizations will continue to rely on SCCs as the basis for transfer.

- In what would seem to be a significant oversight, the SCCs that were released by the European Commission in June 2021 and that must replace all existing SCCs by December 27, 2022 were drafted so as not to apply to data importers based outside of the EU if the relevant processing activity by the importer is subject to the GDPR.[7] Put

[6] *See*, for example: (i) https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/25/fact-sheet-united-states-and-european-commission-announce-trans-atlantic-data-privacy-framework/ and (ii) https://ec.europa.eu/commission/presscorner/detail/en/IP_22_2087.

[7] Article 1 of Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council; European Commission, *The New Standard Contractual Clauses – Questions and Answers*, pp. 13 and 14. Importantly, the UK's International Data Transfer Agreement that came into force in

another way, if a clinical trial sponsor based in a "third country" (e.g., the U.S.) is subject to the GDPR on an extraterritorial basis under Article 3(2), which will frequently be the case in practice, it needs to find another safeguard to legitimize its transfers.[8] This has understandably created a dilemma for the research community: do they (i) strictly follow the wording of the SCCs and look to rely on an alternative transfer mechanism or derogation provided by the GDPR (most of which apply in only limited circumstances); or (ii) enter into the SCCs on the basis that doing so provides a technical basis to legitimize the cross-border transfer and the protection for data subjects that the SCCs are designed to ensure, even though doing so may not fully align with the Commission's intention for the SCCs.

- For those organizations that do rely on the SCCs, a common concern has been how lawfully to conduct onward transfers to parties that cannot — or will not — agree to comply with the data importer's onward transfer obligations by entering into SCCs with the importer. Helpfully, in May 2022, the Commission confirmed that there may be scenarios in which a data importer may further share data received under the SCCs in circumstances where it cannot flow down its obligations under the SCCs to recipient third parties. Given that regulatory authorities will, in almost all cases, refuse to enter into the SCCs, the Commission's acknowledgement that "*a pharmaceutical company that needs to share data with a domestic regulatory authority in order to obtain approval of its products*" is one such scenario that should provide comfort to researchers that further share personal data received from the EU pursuant to SCCs with regulatory bodies.[9]

- Another potential mechanism to legitimize onward transfers that may exist in a revised Privacy Shield would be for an organization that is certified under the revised Privacy Shield to make an onward transfer of personal data to an organization that is not certified under the Privacy Shield. If the revised Privacy Shield continues to follow the onward transfer requirements of the existing Privacy Shield, such a transfer would necessitate a contract between the parties but would not necessitate use of SCCs.[10]

Discussion Point: Is there any thought that in the future the revised Privacy Shield may be made available to nonprofit organizations located in the U.S.?

Discussion Point: Will there be a Privacy Shield available for UK-U.S. data transfers?

Discussion Point: The Privacy Shield Supplemental Principle 14 ("Pharmaceutical and Medical Products") currently states that a transfer from the EU to the U.S. of key-coded or pseudonymized data does *not* constitute a transfer of personal data that is subject to the Principles. Will the revised Privacy Shield cover such transfers? What other changes might be made to Supplemental Principle 14 in light of changes made by the GDPR?

Discussion Point: If your organization is subject to the GDPR under Article 3(2), to what extent does it rely on SCCs as a mechanism to transfer personal data from the EU to the

---

March 2022 does *not* have this shortcoming and thus applies international data transfers under the UK GDPR to organizations in third countries that are subject to Article 3(2) of the UK GDPR.

[8] Article 3(2) of the GDPR extends the jurisdiction of the GDPR to organizations not established in the EU that process personal data of data subjects located in the EU in relation to (i) offering goods or services to data subjects located in the EU, or (ii) monitoring the behavior of data subjects located in the EU.

[9] European Commission, *The New Standard Contractual Clauses – Questions and Answers*, p. 18.

[10] *See* Principle 10, Obligatory Contracts for Onward Transfers.

U.S. despite the technical exclusion from the use of such clauses of entities subject directly to the GDPR?

Discussion Point: The European Commission has stated that it is developing a new set of standard contractual clauses for use with data importers whose processing operations are subject to Article 3(2) of the GDPR ("Article 3(2) SCCs"); our understanding is that these will be issued at some point during 2023. Given that organizations have until December 27, 2022 to migrate all of their existing (i.e., old) standard contractual clauses to the revised SCCs, does your organization anticipate undertaking another contract-updating exercise when the Article 3(2) SCCs are released?

Discussion Point: The revised SCCs released by the European Commission in June 2021 require the parties to conduct a data transfer impact assessment assessing the extent to which the laws of the destination country offer "substantially equivalent" safeguards to personal data as those offered by EU law. What strategies has your organization developed to conduct such assessments for new geographies to which research data are transferred? How could the transfer impact assessment process be eased?

<u>GDPR Derogations</u>

- Article 49(1) of the GDPR states that, in the absence of an adequacy decision or of appropriate safeguards, data exporters may transfer personal data to third countries by relying on one or more of the derogations provided in Article 49(1). Guidelines issued by the EDPB on these derogations[11] — as well as, arguably, the text of Article 49 itself — make clear that derogations should be interpreted and applied restrictively such that data exporters should not seek to rely on them in relation to the type of systematic or repeated transfers that are commonplace in the research setting.

- In the context of clinical trials, the derogation at Article 49(1)(a) for transfers based on the explicit consent of the data subject, after having been informed of the possible risks of such transfers due to the absence of an adequacy decision and appropriate safeguards, is frequently the basis for transfer despite the presence of repetitive and systematic transfers in the clinical trial context. This has particularly been the case for instances in which SCCs have not been appropriate (e.g., transfers to entities that refuse to sign SCCs). It may also stem from persisting confusion regarding the distinction between consent to participate in a clinical trial and consent for the processing of personal data under the GDPR or for the international transfer of personal data.

- While there may be scenarios in which a data exporter may have good cause to use one or more of the Article 49 GDPR derogations (such as to comply with legal proceedings to which it is subject), the primary use case for clinical trial stakeholders other than consent is likely to be Article 49(1)(d), i.e., where the transfer "*is necessary for important reasons of public interest*." Guidelines issued by the EDPB in the context of the COVID-19 outbreak strongly suggests that while organizations conducting clinical research may rely on the Article 49(1)(d) derogation in relation to such research, the derogation should be used only to legitimize initial transfers and another mechanism should be used to legitimize subsequent transfers. The guidelines further suggest that such transfers will be appropriate only in "*an exceptional sanitary*

[11] EDPB, *Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679*, p. 4.

crisis of an unprecedented nature and scale … [that] may require urgent action in the field of scientific research."[12]

Discussion Point: To what extent does your organization rely on consent as the basis to transfer personal data to third countries lacking an adequacy decision? How do you ensure that consent is freely given in this context in line with EDPB guidance?

Discussion Point: How should researchers rely on the other Article 49(1)(d) GDPR derogations, if at all? Would it be helpful to have further guidance from the EDPB on the scope of the derogation for transfers of personal data in the public interest?

Provision of Information

- Articles 13(1)(e) and 14(1)(e) of the GDPR state that the controller must provide to the data subject, at the time when personal data are obtained, information about "*the recipients or categories of personal data, if any.*" Articles 13(1)(f) and 14(1)(f) further require controllers to provide information on, where applicable, "*the fact that the controller intends to transfer personal data to a third country or international organisation*…" Given the number of collaborators, vendors, and other stakeholders that may be involved in a multi-regional clinical trial, including sponsors, contract research organizations, central laboratories, and data monitoring committee members, the research community typically addresses these requirements in a similar way — namely, by providing information in as granular a fashion as possible while accepting that it may not be feasible to list all countries to which personal data are sent.

Discussion Point: Guidelines on transparency, issued by the Article 29 Working Party ("WP29"), which have subsequently been adopted by the EDPB, state that "*the information provided on transfers to third countries should be as meaningful as possible to data subjects; this will generally mean that the third countries be named.*"[13] In the context of a multi-national clinical trial, is it realistic to expect that all possible destination countries are named?

Discussion Point: To what extent do ethics committees require granularity regarding recipient countries and organizations that goes beyond that required by the EDPB guidance stated above? What strategies has your organization developed to address such challenges?

2. Bases for Processing Personal Data for Clinical Research, Transparency, and Status of Parties as Controller vs. Processor

Status of Stakeholders

- Determining whether an organization acts as a controller, a processor, or both in its processing of personal data is one of the fundamental questions in any activity to which the GDPR applies. Yet, there remains a lack of consistency around the role that clinical trial sites take in relation their processing of health data. That the sponsor of a clinical trial acts as a controller is well settled. Indeed, it is difficult to conceive of a scenario in which the sponsor would not act as a controller of personal data, whether as an independent controller or a joint controller with another organization. Similarly, it is

[12] EDPB, *Guidelines 03/2020 on the processing of data concerning health for the purpose of scientific research in the context of the COVID-19 outbreak*, pp. 12 and 13.
[13] Article 29 Working Party, *Guidelines on transparency under Regulation 2016/679*, p. 38.

generally understood and accepted that a contract research organization acts as a processor in providing its services to the sponsor on a contracted basis.

- Here, though, the consensus ends — including between EU data protection regulators. In an opinion issued in 2010 on the concept of controllers and processors, the WP29 took the position that sponsors and trial sites typically act as joint controllers. An exception to the rule, the WP29 stated, is "*where the sponsor determines the purposes and the essential elements of the means and the researcher is left with a very narrow margin of manoeuvre*,"[14] in which case the site (presumably) will act as a processor. By contrast, the EDPB's own guidance on controllers and processors, issued in 2020, takes a narrower view on the conception of controllers in the clinical trials context by suggesting that a trial site will act as a processor if it does not participate in the drafting of the study protocol: "*In the event that the investigator does not participate to [sic] the drafting of the protocol … and the protocol is only designed by the sponsor, the investigator should be considered as a processor and the sponsor as the controller for this clinical trial*."[15] We are aware that ethics committees in different EU member states continue to express different, and sometimes strongly held, positions on this point. Differences in position also persist with respect to the proper role of ancillary service providers, including pharmacies, central laboratories, and specialized medical service providers, such as radiologists.

Discussion Point: Confusion remains as to the role of study sites under the GDPR, with positions varying (sometimes significantly) between member states, sponsors, and sites alike. What is your organization's strategy(ies) for navigating this landscape? Have any best practices emerged?

Discussion Point: What should be the position taken with respect to the role of clinical trial sites in research? How can we increase harmonization in approach across the EU?

<u>Lawful Bases for Processing Personal Data for Research</u>

- For many organizations, consent has been the default lawful basis for processing of health data that are subject to the GDPR and its predecessor, the Data Protection Directive 95/46/EC. This is despite the challenges of obtaining GDPR-compliant consent from vulnerable patients, some of whom may be children or persons with diminished capacity, as well as the difficulty for some non-legal professionals working in the research industry of distinguishing between an informed consent for the purposes of clinical trials legislation and consent for processing and/or transfer of personal data under the GDPR. The clinical trial landscape is further complicated by the fact that clinical trials generally require processing of "special categories" of personal data (e.g., health data, genetic data, biometric data), which necessitates establishing both a lawful basis for processing under Article 6 of the GDPR and satisfying one of the conditions for processing "special categories" of personal data under Article 9 of the GDPR.[16]

[14] *Id.,* p. 30.
[15] EDPB, *Guidelines 07/2020 on the concepts of controller and processor in the GDPR*, p. 23.
[16] The full list of "special categories" of personal data include "*personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation*."

- In 2019, the EDPB and the Commission proposed a major departure from the view that consent is the most appropriate lawful basis on which to process sensitive personal data in the research context.[17] According to the Commission, sponsors and sites should instead rely on: (i) Articles 6(1)(c)[18] and 9(2)(h)[19] of the GDPR in respect of processing relating to safety reporting, archiving of clinical data, and disclosure of such data to regulatory authorities; and (ii) Articles 6(1)(e),[20] 6(1)(f),[21] 9(2)(i),[22] and 9(2)(j)[23] in respect of processing purely related to research activities. As a result of this guidance, researchers are now taking a variety of approaches to legitimizing their processing — for example, involving informed consent for clinical trials purposes, reliance on Articles 9(2)(h), 9(2)(i), and 9(2)(j) for sensitive data processing, and explicit consent under the GDPR in respect of international data transfers. Moreover, in the context of a clinical trial, it is not always straightforward to distinguish between activities that are conducted for safety reporting and submissions to regulatory authorities as opposed to those that are conducted primarily to advance scientific research.

- Given the lack of harmonization among EU member state laws as to the extent to which they permit processing of special categories of personal data on the basis of Articles 9(2)(i) and 9(2)(j), different approaches to this issue persist across sites in multinational clinical trials.

- By comparison, in the U.S., there has been a proliferation in recent years of omnibus state privacy laws that impose new requirements on businesses that process personal information of such states' residents, such as the California Consumer Privacy Act. These laws impose certain obligations that are similar to those imposed by the GDPR, including transparency (or notice) obligations, provision of rights to data subjects, and security measures. Notably, to date, each of these state laws contains an exception for personal information collected in the context of research activities, including clinical

---

[17] EDPB, *Opinion 3/2019 concerns Questions and Answers on the interplay between the Clinical Trials Regulation (CTR) and the General Data Protection regulation [sic] (GDPR) (art. 70.1.b))*, p. 7; European Commission, *Question and Answers on the interplay between the Clinical Trials Regulation and the General Data Protection Regulation*, pp. 4 and 5.

[18] Art. 6(1)(c) GDPR: "*[P]rocessing is necessary for compliance with a legal obligation to which the controller is subject*."

[19] Art. 9(2)(h) GDPR: "*[P]rocessing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3 [i.e., relating to professional secrecy]*."

[20] Art. 6(1)(e) GDPR: "*[P]rocessing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller*."

[21] Art. 6(1)(f) GDPR: "*[P]rocessing is necessary 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 which require protection of personal data, in particular where the data subject is a child.*"

[22] Art. 9(2)(i) GDPR: "*[P]rocessing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy.*"

[23] Art. 9(2)(j) GDPR: "*[P]rocessing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.*"

trials conducted in accordance with requirements of the International Conference on Harmonization Good Clinical Practice ("ICH GCP") guidelines or U.S. regulations on human subject research (e.g., the Common Rule and FDA regulations on human subject research). One approach that might be considered under the GDPR is the creation of similar exceptions from certain GDPR requirements for personal data collected in research activities subject to ICH GCP and/or other regulations on human subject research.

Discussion Point: What is your organization's experience in navigating different bases for processing across EU member states?

Discussion Point: What should be the Article 6 basis and Article 9 condition under the GDPR for processing personal data and special categories of personal data, respectively, in the context of a clinical trial? What guidance would help to achieve greater harmonization on this issue?

Discussion Point: What should the role of a contract research organization (CRO) be in assisting with determinations of legal basis for processing?

Discussion Point: As part of its post-Brexit data strategy, the UK government proposed amending the UK GDPR to permit processing of personal data for research purposes in a wider range of circumstances.[24] Would this be a helpful solution for the EU to pursue with respect to the EU GDPR?

Discussion Point: Would it be helpful to follow the approach taken by U.S. state privacy laws in their exemptions for personal information collected in certain research activities subject to ICH GCP or other regulations on human subject research? What might be the contours of such an exemption?

<u>Provision of Notice, also referred to as the provision of "Fair Processing Information"</u>

- Transparency enables individuals to understand and, if necessary, challenge the processes involved in collecting, using, disclosing, and retaining their personal data. Provision of granular transparency information to data subjects is especially important in the context of medical research but can be impractical where an organization does not directly collect personal data from data subjects, as is often the case in the context of secondary research. Indeed, a particular challenge concerns the provision of transparency information by collaborators or vendors engaged by a sponsor organization that seek to repurpose clinical trials data for their own use.

- Guidance issued in January 2022 by the French data protection authority, the *Commission nationale de l'informatique et des libertés* ("CNIL"), on the reuse of personal data by processors for their own purposes makes clear that information relating to further processing must be provided to data subjects — both by the initial controller and the processor (in its subsequent role as a controller).[25] This approach raises a variety of practical challenges, such as how a processor that receives only

[24] *See*, for example, Data Protection and Digital Information Bill, ss. 2, 3, and 22.
[25] CNIL, *Sous-traitants: la réutilisation de données confiées par un responsable de traitement*.

pseudonymized information can effectively provide notice to data subjects whose contact information it does not possess.

- Article 14 of the GDPR creates an exception to the transparency requirement when data are not collected directly from the data subject and providing notice to data subjects would be impossible or involve disproportionate effort. The regulatory text states that reliance on this exception may be available "*in particular for processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to the conditions and safeguards referred to in Article 89(1) or in so far as the obligation referred to in paragraph 1 of this Article is likely to render impossible or seriously impair the achievement of the objectives of that processing.*" We are aware that a great deal of confusion persists in the research community concerning the extent to which this exception may be relied upon in practice.

- Exceptions to transparency requirements could be broadened, for example, (i) where processing relates to public health or similar purposes, and data are not collected directly from the data subject, and (ii) in respect of further processing for secondary research purposes where the data are initially collected *directly* from the data subject, in line with the UK government's 2021 proposal on this topic.[26] In such cases, transparency information could be provided on a non-individualized basis (such as via a general website privacy notice), provided that a mechanism exists to direct relevant data subjects to such notice.

Discussion Point: To what extent does your organization rely on the exception in Article 14 of the GDPR for impossibility or disproportionate effort in the research context? How does your organization evaluate the "impossibility or disproportionate" effort criteria? To what extent should this exception be available in the research context? What guidance could assist the research community in understanding when reliance on this exception is appropriate?

Discussion Point: The UK's Data Protection and Digital Information Bill includes an exemption to a controller's transparency obligations under Article 13 of the UK GDPR such that, in the context of processing personal data for research, archiving, or statistical purposes, the provision of fair processing information would not be required where doing so "*is impossible or would involve disproportionate effort*" even in instances in which data have been collected directly from the data subject. Would reliance on such an exemption result in a reduction in transparency and individuals losing control of their sensitive health-related personal data?

3. Secondary Research Under the GDPR

Real-World Evidence

- The use and reuse of data collected in treatment as real-world evidence ("RWE") helps to better understand disease and treatment and supports research and development to

[26] UK Department for Digital, Culture, Media & Sport, *Data: a new direction – government response to consultation*, Chapter 1.2.

improve therapy. Authorities that regulate clinical trials worldwide increasingly also rely on RWE for regulatory decision-making and safety monitoring purposes. The ability to use data beyond the original purpose for collection in a lawful manner — for example, to do so without receiving the specific consent of and/or providing additional notice to the patient — is therefore vital for stakeholders across the healthcare spectrum, including by parties other than those that originally collected the data.

- The GDPR stipulates that personal data must be: (i) "*collected for specific, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes*" (per Article 5(1)(b)); and (ii) "*adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed*" (per Article 5(1(c)). Article 5(1)(b) provides that "further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purpose."[27] Unless the identifying personal data contained in RWE are anonymized — thereby potentially reducing their utility — they are subject to the GDPR's requirements on lawful basis and notice, among others. As discussed elsewhere in this paper, the latter requirement in particular can be challenging to meet in practice.

- A further challenge arises if the personal data were originally collected on the basis of consent (which, as we have seen, historically has been the predominant lawful basis used to process health data in the clinical research context). In such cases the principle of "compatibility" does not apply, and data subjects must be re-consented in order to conduct the secondary processing. However, sponsor organizations will typically not have access to (or even the ability to contact) data subjects, making it extremely difficult to refresh consent in a GDPR-compliant manner. In what appears to be an attempt to combat this problem, the UK's Data Protection and Digital Information Bill proposes to expand the application of consent for the purposes of scientific research by allowing consent to be given to scientific research-related processing in cases in which it is not possible, at the time of obtaining consent, to fully identify the purposes for which personal data will be processed.[28]

- One solution to the above challenge of consent could be to obtain a broad consent from data subjects at the outset of a research project. It remains unclear the extent to which a "broad consent" can be obtained from data subjects to permit future uses of their data. GDPR Recital 33 provides that "[i]t is often not possible to fully identify the purpose of personal data processing for scientific research purposes at the time of data collection. Therefore, data subjects should be allowed to give their consent to certain areas of scientific research when in keeping with recognised ethical standards for scientific research." The EDPB has, however, in guidance on consent suggested that "Recital 33 does not disapply the obligations with regard to the requirement of specific consent" and that when health data are involved, "applying the flexible approach of Recital 33 will be subject to a stricter interpretation and requires a high degree of scrutiny." EDPB has gone on to suggest that in circumstances in which research

[27] *See*, for example, the Information Commissioner's Office ("ICO"), *Draft guidance on the research provisions within the UK GDPR and the DPA 2018*, Version 1.0 for public consultation, February 2022 ("ICO Research Guidance"), which confirms that scientific research "*should be understood broadly," including "the full range of academic research … [b]ut it can also include research carried out in commercial settings*."
[28] *See* the Data Protection and Digital Information Bill, cl. 3.

purposes cannot be fully specified, as the research advances, consent for subsequent steps in a project should be obtained before the next stage begins.[29]

Discussion Point: How does your organization currently — or intend to — utilize RWE? How comfortable are you with conducting these activities within the GDPR's guardrails?

Discussion Point: What legal basis under Article 6 and condition under Article 9 does your organization rely upon when processing data for RWE purposes? If you rely on compatibility, how do you evaluate which purposes are compatible?

Discussion Point: How can notice, or fair processing information, be provided to data subjects in the context of RWE activities?

Discussion Point: To the extent your organization participates in the Data Analysis and Real World Interrogation Network (DARWIN EU), what challenges for DARWIN EU have been created by GDPR?

Discussion Point: What role do ethics committees play in overseeing RWE or other secondary research activities?

Discussion Point: Would the GDPR benefit from a uniform definition of public health activities that could be conducted absent patient consent? For example, should the broad interpretation of such activities under the U.S. Health Insurance Portability and Accountability Act of 1996 ("HIPAA")[30] be used an example of the way in which the GDPR can include processing of personal data for RWE?

<u>European Health Data Space</u>

- The European Health Data Space ("EHDS") is an ambitious ecosystem of rules, common standards, and a governance framework to enable responsible health data sharing and use in the EU. Among other things, the EHDS is intended to allow individuals the ability to better access, share, and update their data while giving researchers large sets of high-quality data on which to carry out research. Given its remit, the EHDS Regulation (the "Regulation") — which, at this stage, remains a legislative proposal[31] — will necessarily involve the processing of large amounts of personal and pseudonymized data by stakeholders across the research community and thus is expected to have significant interplay with the GDPR.

- The Regulation seeks to address some of the concerns described elsewhere in this paper regarding the GDPR's limitations on research processing — including on the lawful

[29] EDPB, *Guidelines 05/2020 on consent under Regulation 2016/679*, pp. 30-31.
[30] HIPAA defines public health activities to include uses and disclosures of protected health information ("PHI") for purposes of (i) preventing or controlling disease, injury, or disability, including, but not limited to, the reporting of disease, injury, vital events such as birth or death, and the conduct of public health surveillance, public health investigations, and public health interventions, (ii) disclosing PHI to public health authorities authorized by law to receive reports of child abuse or neglect; (iii) disclosing PHI to persons subject to the jurisdiction of the FDA with respect to an FDA-regulated product or activity for which the person has responsibility, (iv) disclosing PHI to persons potentially exposed to communicable disease, (v) medical surveillance in the workplace, and (vi) school immunization requirements. 45 C.F.R. § 164.512(b).
[31] European Commission, *Proposal for a Regulation of the European Parliament and of the Council on the European Health Data Space*.

bases for processing health data[32] — by unlocking secondary uses of personal data. By contrast, the concept of "electronic health data" set out in the Regulation is much broader than would be captured under the GDPR,[33] such that there currently are legal and operational uncertainties regarding how the frameworks will work together. For example, how will the emphasis on enabling data subject rights in the Regulation work in the context of clinical research where such rights cannot always be exercised (i.e., where the controller only processes key-coded data)? And where should the line be drawn between using data for "innovation" activities that are not directly related to the original purpose for processing — such as internal training and testing — and limiting such activities due to an insufficiently strong connection with the public health benefits?

Discussion Point: To what extent are your organizations monitoring or engaging with the Regulation specifically and the EHDS more widely? Would the involvement or creation of industry groups (such as MRCT) be welcomed in helping to shape the Regulation and the EHDS?

Discussion Point: The EDPB and European Data Protection Supervisor ("EDPS") have expressed concern that the Regulation as drafted could lead to legal uncertainty, such as regarding its nomenclature around "primary use" and "secondary use"[34] — terms that may not always align neatly with the GDPR's concept of "further processing." Do you share this concern?

Discussion Point: The EDPB and EDPS have further noted that the Regulation lacks clarity as to when different provisions of Article 9 of the GDPR would permit secondary data processing. Does this represent a continuation of challenges seen in interventional research with respect to establishing the proper basis for processing personal data?

<u>Biospecimens</u>

- Research on biospecimens has led to significant breakthroughs in the treatment of cancers and other diseases. Nevertheless, the treatment of such data under the GDPR has led to confusion for many of the organizations involved biobank research, including in respect of how they interpret and apply the GDPR's provisions on extraterritoriality, lawful bases for processing, pseudonymization, and anonymization, and data subject rights.[35] While the EDPB has sought to clarify the application of the GDPR to health

[32] For example, Recital 37 of the Regulation makes clear that processing of electronic personal data under the Regulation can, for the purposes of the GDPR, be processed under a range of lawful bases, including Articles 6(1)(c), (e), and (f) and Articles 9(2)(g), (h), (i), and (j) of the GDPR.

[33] Recital 38 of the Regulation states: "*The categories of electronic health data that can be processed for secondary use should be broad and flexible enough to accommodate the evolving needs of data users, while remaining limited to data related to health or known to influence health. It can also include relevant data from the health system (electronic health records, claims data, disease registries, genomic data etc.), as well as data with an impact on health (for example consumption of different substances, homelessness, health insurance, minimum income, professional status, behaviour, including environmental factors (for example, pollution, radiation, use of certain chemical substances))*."

[34] EDPB, *EDPB-EDPS Joint Opinion on 03/2022 on the Proposal for a Regulation on the European Health Data Space*, July 2022.

[35] *See*, *e.g.*, D. Peloquin et al., *Disruptive and avoidable: GDPR challenges to secondary research uses of data*, European Journal of Human Genetics, 2020.

research,[36] its guidance to date has dealt only peripherally with the issues that are central to biospecimens. Moreover, as discussed further above, while the EDPB has indicated that it intends to provide further clarification on further processing of personal data in the context of scientific research, it is unclear when or if such guidance will materialize.

Discussion Point: There is an ongoing debate about whether genetic data alone (i.e., with no patient identifiers attached) should be considered "identifiable" for the purposes of the GDPR. Notably, the EDPB "*strongly advise[s] that such genetic data is treated as personal data and that the processing thereof is conducted with the implementation of appropriate technical and organisational measures to ensure compliance with the [GDPR]*".[37] In light of the EDPB's guidance, is it no longer feasible — or advisable — to take a contrary position in respect to the processing of genetic data?

Discussion Point: What basis under Articles 6 and 9 of the GDPR does your organization rely upon for secondary processing of residual biospecimens collected in clinical care or other research projects?

4. Anonymization and Pseudonymization

Anonymization

- Recital 26 of the GDPR states that the Regulation does not apply to the processing of "*an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable*." As discussed further below, the GDPR applies to pseudonymized data, even when held by an entity that lacks the key needed to re-identify the data. An alternative approach of "relative anonymization" is found in the UK's Data Protection and Digital Information Bill, in which anonymization is judged by the ability of the party holding the data to re-identify the data.[38]
- HIPAA, the primary federal health privacy regulation in the U.S., sets out two clear pathways for data to be de-identified and thus removed from the ambit of the regulation: (i) the "safe harbor" method, which requires the removal of 18 specified identifiers; and (ii) the "expert determination" method, which permits a statistical expert to certify that the risk of re-identification with respect to a particular data set is very low. The GDPR's regulatory text does not provide specified pathways for anonymization, which has, at least in some contexts, resulted in greater confusion as to the extent to which data are properly considered "anonymized."

Discussion Point: Given the difficulty in ensuring that data are ever *truly* anonymized, does a relative approach better reflect the standards that are currently adopted by — and, arguably, sufficient for the purposes of — stakeholders across the research community?

Discussion Point: We discussed in the panel on secondary research the ongoing debate about whether genetic data alone (i.e., with no patient identifiers attached) should be

[36] EDPB, *EDPB Document on response to the request from the European Commission for clarifications on the consistent application of the GDPR, focusing on health research*, February 2021.
[37] *Id.*, p. 12.
[38] Under this approach, data could be considered "anonymized" and thus no longer subject to the data protection law if held by a party lacking the means to re-identify the data, provided that adequate technical and organizational measures are in place to prevent re-identification (e.g., contractual arrangements prohibiting the party holding the key needed to re-identify the data from sharing the key with the party holding the data).

considered inherently "identifiable" for the purposes of the GDPR. Is it no longer feasible to take a position that genetic data can be anonymized?

Discussion Point: To what extent are voiceprints and retinal images capable of anonymization?

Discussion Point: To what extent does the GDPR permit an "expert determination" as to anonymization that is analogous to the "expert determination" method of de-identification under HIPAA? Does your organization rely on such an expert determination approach to anonymization?

Discussion Point: How do de-identification expert determinations under HIPAA differ in practice from expert determinations under the GDPR?

Discussion Point: What guidance could assist the research community in determining whether data have been properly "anonymized" under the GDPR?

Pseudonymization

- Article 4(5) of the GDPR defines pseudonymization as "*the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.*" Unlike anonymous information, data that have been pseudonymized fall within the scope of the GDPR — a distinction that, for organizations in the research sector, continues to result in confusion as to where anonymization begins and pseudonymization ends. For example, it is not always clear to researchers that where re-identification risks cannot be sufficiently mitigated (for example, because the data set is too small), the data may not be capable of being anonymized. Similarly, there is always the possibility — however small — that anonymized records may be re-identified; this is particularly the case where the data are easily capable of being singled out prior to being anonymized.

- Regulatory authorities in the EU have been clear to reiterate the distinction between pseudonymization and anonymization, and so it is interesting to see that some organizations, particularly in the United Kingdom, continue to take the position that pseudonymized data fall outside the scope of the GDPR with respect to international data transfers — a view that likely reflects, at least in part, Principle 14 of the Privacy Shield Framework Principles discussed further in footnote 1 above.

Discussion Point: Given that the restrictions on international data transfers in Chapter V of the GDPR are designed to ensure that data subjects do not lose the protection of EU data protection laws when their data are sent to and processed in a third country, if the data are securely pseudonymized in such a way that neither the data importer nor foreign government authorities can identify data subjects and none of the parties in the third country can access the additional information needed for re-identification, is it arguable that the key code received and processed by the data importer should not be subject to the same restrictions as directly identifiable personal data under the GDPR?