Journal of Law and the Biosciences, 1–33
doi:10.1093/jlb/lsaa055
Original Article

International transfers of health data between the EU and USA: a sector-specific approach for the USA to ensure an 'adequate' level of protection

Laura Bradford*,†, Mateo Aboy‡ and Kathleen Liddell**

Centre for Law, Medicine and Life Sciences (LML), Faculty of Law, University of Cambridge, Cambridge, UK.

*Corresponding author. E-mail: lrb45@cam.ac.uk

ABSTRACT

International health research increasingly depends on collaboration and combination using medical data to advance treatment and drug discovery. The European Union (EU), through its General Data Protection Regulation, has tightened the rules for sharing data across borders to protect individual privacy. These new rules threaten cooperation between the EU and the USA, the two largest public funders of biomedical research. This article analyzes the primary pathway for sharing research data with the USA, the US–EU Privacy Shield††, and argues that the Shield is ill-suited

† Laura Bradford is a Senior Research Associate and Affiliated Lecturer in the Centre for Law, Medicine and Life Sciences at the University of Cambridge, UK where she also teaches US Corporate Law in the Masters in Corporate Law Program. She is dual qualified as an attorney in the UK and in New York. For the past three years she has served as a Senior Legal Advisor for the University of Cambridge, Cambridge, UK. In the USA she was an Assistant Professor at George Mason University Law School, and a Visiting Associate Professor at George Washington University School of Law. She graduated with honors from Stanford University Law School and Yale University.

‡ Mateo Aboy is a Principal Research Scholar (PRA) in the Centre for Law Medicine and Life Sciences at University of Cambridge and a visiting scholar at Petrie-Flom Center for Health Law Policy, Biotechnology, and Bioethics, Harvard Law School.

** Kathleen Liddell is the Director of Centre for Law, Medicine and Life Sciences at the University of Cambridge, UK.

†† This Article considered developments through May 30, 2020. On July 16, 2020 the Court of Justice for the European Union invalidated the adequacy decision for the EU-US Privacy Shield due to concerns about US government surveillance of electronic communications. C-311/18, Data Protection Commissioner v. Facebook Ireland Ltd., http://curia.europa.eu/juris/document/document.jsf?docid=228677&mode=req&pageIndex=1&dir=&occ=first&part=1&text=&doclang=EN&cid=10716034. The US and the EU are discussing replacement mechanisms. The flaws of the Privacy Shield highlighted in this Article should serve as a guide in crafting any replacement regime.

© The Author(s) 2020. Published by Oxford University Press on behalf of Duke University School of Law, Harvard Law School, Oxford University Press, and Stanford Law School. This is an Open Access article distributed under the terms of the Creative Commons Attribution NonCommercial-NoDerivs licence (http://creativecommons.org/licenses/by-nc-nd/4.0/), which permits non-commercial reproduction and distribution of the work, in any medium, provided the original work is not altered or transformed in any way, and that the work is properly cited. For commercial re-use, please contact journals.permissions@oup.com.

to support complex health studies. Its legitimacy is in question under both EU and US law, and its terms are too restrictive for the variety of exchanges underlying research, treatment, and care. As an alternative, we propose that the USA seek an additional sector-based adequacy determination based on the existing US health privacy law, the Health Insurance Portability and Accountability Act. A sector-specific approach to adequacy for health would avoid many of the most contentious issues that divide the USA and EU on data protection. It could also serve as a model for other third-party jurisdictions and facilitate international harmonization of health research practices.

KEYWORDS: GDPR, privacy and data protection, cross-border transfers, EU–US privacy shield, HIPAA

I. INTRODUCTION

The sharing of patient medical information is vital for research and drug discovery. In an effort to protect European Union (EU) data subjects' privacy, the General Data Protection Regulation (GDPR) enacted by the EU in 2016 places stringent restrictions on international transfers of personal data, including data concerning health. The threat of steep penalties for noncompliance have upended decades of accepted practice in commercial and public health research between the EU and other major research centers, especially the USA.[1] In November 2019 the director of the US National Institutes of Health, the largest public funder of biomedical studies in the world, labeled the GDPR 'a serious impediment to research' and said that progress on some important projects had 'slowed to a crawl'.[2]

The legal avenues for sharing personal health data with US entities under the GDPR are difficult and uncertain. Increasing scrutiny of US law enforcement data collection and surveillance practices led to the invalidation in 2015 of the US–EU Safe Harbor which had previously allowed exchanges of commercial data between the two regions.[3] As a fallback, the European Commission (EC) adopted a 'limited adequacy' decision in 2016 on the so-called 'EU-US Privacy Shield Framework'.[4] This Framework allows the free transfer of personal data to companies that are certified under the EU–US Privacy Shield. However, the EU–US Privacy Shield has been challenged as insufficiently protective of subject rights in the EU and is seen as overly restrictive and burdensome on companies and federal agencies in the USA.[5]

1 Tania Rabesandratana, European data law is impeding studies on diabetes and Alzheimer's, researchers warn, Science Nov. 20, 2019.

2 Id.

3 Case C-362/14, Schrems v. Data Prot. Comm'r, 2015 E.C.R. 650,191 ¶ 28, 91 (Oct. 6, 2015) [hereinafter, Schrems I].

4 Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 Pursuant to Directive 95/46/EC of the European Parliament and of the Council on the Adequacy of the Protection by the EU-U.S. Privacy Shield, 2016 O.J. (L207), http://ec.europa.eu/justice/data-protection/files/privacy-shield-adequacy-decisionen.pdf [hereinafter Privacy Shield Implementing Decision].

5 See, infra, text accompanying notes 71–136.

This paper analyses the EU–US Privacy Shield Framework from both the EU and the US perspective with particular attention to its suitability for transfers of health data. We argue that the Privacy Shield functions poorly as a mechanism for facilitating international health research and bioinnovation. It rests on an uncertain legal foundation under both EU and US law. It is neither a treaty, nor a binding agreement, nor a mandatory law; its status is therefore ambiguous under both the GDPR and the US constitutional system. Its scope is also too narrow to support the diverse health care research ecosystem.

Due to the importance of data transfers for public health and medical innovation, we suggest that one way around the inadequacy of the Privacy Shield would be to seek an additional sector-based adequacy determination based on the existing US health privacy law, the Health Insurance Portability and Accountability Act (HIPAA).[6] A sector-specific approach to adequacy for health would avoid many of the most contentious issues that divide the USA and EU on data protection. It could also serve as a model for other third-party jurisdictions and facilitate international harmonization of health research practices.

Health care research is increasingly international and data intensive. Everything from genomic research to adverse drug reaction testing to epidemiology depends on the collection, linkage, and analyzation of diverse patient indicators and disease features. Healthcare organizations are increasingly supplementing traditional controlled drug discovery pipelines with distributed, collaborative, and iterative research methods that demand large-scale combinations of patient data.[7] Research studies, including clinical trials, aim for an international scope, with results being compared and matched to achieve greater statistical significance.[8] Genomic databases need to reflect the genetic diversity of patients across the world for their value to be maximized.[9] Advances in personalized medicine and use of algorithms in diagnosis and treatment depend on the analysis of massive amounts of individual statistics. These include information about risk factors, disease outcomes, lifestyle, genetics, environment, behavior, and treatment responses.[10] Huge collections of health-related data are shared continuously

6 The Health Insurance Portability and Accountability Act of 1996 (HIPAA) P.L. No. 104–191, 110 Stat. 1938 (1996).

7 See Maria Angeles Martinez-Grau & Maria Alvim-Gaston, Powered by Open Innovation: Opportunities and Challenges in the Pharma Sector, 33 Pharmaceutical Medicine 193, 194 (2019); Alexander Schuhmacher, Oliver Gassman & Markus Hinder, Changing R&D Models in research-based pharmaceutical companies, 14 J. Transl. Med. 105 (2016)

8 See, e.g., Timo Minssen et. al., The EU-US Privacy Shield Regime for Cross-Border Transfers of Personal Data under the GDPR, 4 Eur. Pharm. L. Rev. 34, 36 (2020) (noting that multi-site trials is a necessity in many clinical trials); Grau & Gaston, supra note 7 at 196 (describing Eli Lilly's biological compound library program under which it makes its privileged compounds available to scientific institutions for testing and validation); Mark Phillips et al., Comment: Genomics: data sharing needs an international code of conduct, 578 Nature 31, 31 (Feb. 6, 2020) (describing large-scale cancer genomics collaboration which combined data from 468 institutions in 34 countries).

9 Royal College of Pathologists and British Society for Genetic Medicine, Consent and confidentiality in genomic medicine: Guidance on the use of genetic and genomic information in the clinic, Report of the Joint Committee on Genomics in Medicine 24 (London: RCP, RCPath and BSGM, 3rd ed. 2019).

10 See K.S. Cheung et al., Big data in gastrointestinal research, 25 World J. Gastroenterol. 2990, 2991, 2992, 2999 (Jun. 28, 2019); see also Timo Minssen et al., Clinical trial data transparency and GDPR compliance: Implications for data sharing and open innovation, Working Paper at 3-4 (forthcoming: Science & Public Policy (Oxford University Press 2019)).

among commercial organizations, states, and state actors such as public health bodies, universities, and research laboratories.

Differences in the data protection regimes between the USA and the EU threaten to throttle these exchanges.[11] Europe and the USA provide the lion's share of public funding for health research[12] and most of the major pharmaceutical companies have large research campuses in one or both jurisdictions.[13] Exchanges of patient and population health-related data between the two regions are vital for continued innovation in treatments and public health.

The circumstances under which organizations may wish to exchange personal health data across the Atlantic are various. Multinational pharmaceutical companies may need to send data about drug safety and efficacy in certain populations to subsidiaries and affiliates in other jurisdictions. A clinical research organization managing a clinical trial may need to share outcome data with partners and sponsors located overseas. Researchers in North America may seek to access sample or population data, including identifying phenotype characteristics, held in European biobanks, or vice versa.[14] Makers of medical devices or academic researchers may need to store patient data with cloud service providers whose servers are located in a different jurisdiction.[15]

Presently the EU–US Privacy Shield is the legal basis for many of these transfers. In section II (legal overview), we describe the legal framework that currently applies to transfers of personal health data from the EU to the USA. As well as important informational background, this section has an overarching purpose for our argument. It demonstrates the seriousness of the policy issue, first by explaining how the GDPR affects US-based companies notwithstanding that it is European legislation and second by explaining why the EU–US privacy shield often comes into play, even though technically, there are other lawful bases such as binding corporate rules (BCRs) or standard contractual clauses (SCCs) for transferring personal health data from the EU to the USA.

In section III (explanation of EU–US Privacy Shield and its limitations), we provide further information about the operation of the EU–US Privacy Shield. As well as analyzing adequacy from the EU perspective, this article is the first to look at the legitimacy of the Privacy Shield from the US vantage point, both in terms of its origins and its operation. From the EU side, the Privacy Shield lacks the force of mandatory law, which would seem to be a prerequisite for an adequacy determination, under Article 45 of the GDPR. It is also subject to multiple legal challenges due to alleged deficiencies in the underlying US legal regime. From the USA side, the Privacy Shield essentially requires US agencies to enforce EU law and so is more restrictive than an adequacy decision based on domestic US law. The authority of individual federal agencies to

11 Rabesandratana, supra note 1; see also Phillips et al., supra note 8 at 32 (describing data access hurdles for US researchers participating in an international cancer genomics study that caused the US researchers to remain "conceptually split off from the rest of the project").

12 R.F. Viergever, & T.C.C. Hendriks, The 10 largest public and philanthropic funders of health research in the world: what they fund and how they distribute their funds. Health Res Policy Sys 14, 12 (2016), https://doi.org/10.1186/s12961-015-0074-z.

13 E.g. Schuhmacher et al., supra note 7 at 8.

14 Royal College of Pathologists, supra note 8 at 24.

15 Cf. Phillips et al., supra note 8 at 31–32 (discussing the use of cloud computing services in a large-scale cancer genomics study).

agree to such enforcement commitments independent of Congressional approval or a negotiated treaty is also a concern. Finally, the Privacy Shield aims primarily at commercial transfers of data and so is ill-suited to serve as the primary mechanism for transfers of data concerning health within the highly regulated medical sector.

In section IV (HIPAA as possible solution), we argue that one way to overcome the problems with the EU–US privacy shield for EU–US transfers of health data would be to ask Europe to give a sector specific adequacy decision for the existing US health privacy law, HIPAA. A HIPAA shield would not replace the EU–US privacy shield, nor SCCs, BCRs or informed consent. It would be an additional legal basis for lawful international transfer of personal health data. In this section we briefly outline the advantages that the HIPAA shield would have over the EU–US privacy shield such as greater democratic legitimacy, a targeted health data focus; and harmonization with an existing and tested legal framework. We also discuss whether HIPAA would likely meet the 'adequacy' standard, and the modifications that are likely to be required. We consider several challenges posed by such an approach and possible alternatives.

II. THE CURRENT LEGAL FRAMEWORK FOR INTERNATIONAL TRANSFERS OF PERSONAL HEALTH DATA FROM THE EU TO THE USA

The GDPR's reach is vast. The law can apply directly to many entities based in the USA even if they have no operations in the EU and arguably even if they are not processing EU subject data. Under Article 3, the GDPR applies to any processing of personal data 'in the context of the activities of an establishment of a controller or processor in the Union, regardless of whether the processing takes place in the Union or not'.[16] It is possible then that any commercial or research collaboration anywhere in the world in which an EU-established entity participates is governed by the GDPR. This would be the case even if the data analyzed does not relate to EU subjects.[17] Furthermore, the GDPR applies directly to non-EU entities who offer goods and services to data subjects in the EU or who monitor subject behavior taking place within the Union.[18] Although this last provision seems targeted at companies who monitor behavior for advertising and marketing purposes, its reach can extend to pharmaceutical companies and researchers monitoring patient reactions to a drug.[19]

To further ensure that the protection guaranteed by the GDPR is not undermined, the regulation restricts transfers of personal data to countries outside the EU and the European Economic Area (EEA). A 'transfer' of personal data occurs any time it is sent, or made accessible, to an outside receiver.[20] If the GDPR does not apply directly to that

16 Regulation (EU) 2016/679 (General Data Protection Regulation) Art. 3(1), 2016 OJ L 119, 04.05.2016; cor. OJ L 127, 23.5.2018 ("GDPR").

17 See EDPB, Guidelines 3/2018 on the territorial scope of the GDPR (Article 3) 9–10 (2019), https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_3_2018_territorial_scope_en.pdf.

18 GDPR Art 3(2).

19 See EDPB, Questions and Answers on the interplay between the Clinical Trials Regulation and the General Data Protection Regulation, 10 (2019).

20 Information Commissioner's Office, Guide to the General Data Protection Regulation GDPR: International Transfers https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-transfers/ (last visited Jan. 22, 2020). Note that transit of the data via electronic routing through a third jurisdiction does not qualify as a restricted "transfer."

receiver because of its location, then both the processor and the controller of the data must comply with the conditions specified in Chapter 5 of the GDPR.[21]

The potential sanctions for senders and recipients that fail to comply with Chapter 5 are onerous. A noncompliant transfer of personal data to a third country is one of the infractions that invite the largest possible administrative penalty: up to €20,000,000 or four per cent of total worldwide annual turnover.[22] In July 2019, for example, the Marriott hotel group was fined £99 million pounds for a data breach incident that exposed 339 million guest records globally, of which around 30 million related to residents of 31 countries in the EEA.[23]

The landscape for transferring health data lawfully between the USA and EU is disjointed and difficult to navigate, however. Biomedical researchers lack accepted pathways to exchange patient health data impacted by the GDPR. The mechanisms prescribed to facilitate such transfers, such as BCRs, SCCs and explicit consent, are ill-suited to research scenarios and are burdensome to fulfill even where they are available.

Chapter 5 of the GDPR offers three basic pathways for a legal international transfer of data. These include:

1. Transfers on the basis of an 'adequacy decision' by the EC;[24]
2. Transfers subject to 'appropriate safeguards' by the controller/processor on condition that enforceable data subject rights and effective legal remedies for data subjects are available;[25] and
3. Derogations for specific situations.[26]

In effect, these mechanisms are intended to ensure that either (i) the country (adequacy decision) or (ii) the organization (appropriate safeguards with SCCs and BCRs) ensure an appropriate level of data protection to the data subject. If none of these routes are available, the only way to transfer data is either to seek the explicit consent of the subject or to render the data anonymous so that the rules of the GDPR no longer apply.[27]

A. Transfers on the Basis of an 'Adequacy Decision'

Pursuant to Article 45 GDPR, the EC has the power to determine whether a country outside the EU offers an adequate level of data protection. The effect of these adequacy decisions is that personal data can be transferred from the EU and the EEA to that

21 GDPR Art. 44.

22 GDPR Art 83(5).

23 Information Commissioner's Office, Statement: Intention to fine Marriott International, Inc more than £99 million under GDPR for data breach (09 Jul. 2019), available at https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/07/statement-intention-to-fine-marriott-international-inc-more-than-99-million-under-gdpr-for-data-breach/ (last visited Jan. 27, 2020).

24 GDPR Art 45.

25 GDPR Art. 46 & 47.

26 GDPR Art. 49.

27 GDPR recital 26. Technically explicit consent of the subject is one of the derogations under Article 49, and Article 49 places strict requirements on how that consent must be obtained. See infra text accompanying notes 49–51.

third country without any further safeguards.[28] At the time of this writing, the EC has recognized Andorra, Argentina, Canada (for commercial organizations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland, and Uruguay as providing adequate protection.[29]

The USA does not have a general adequacy decision as it lacks a federal general data protection legislation. Instead, the USA has instituted the Privacy Shield framework as a stopgap measure to allow transfers of data subject to the GDPR. As detailed further in Part III, the Privacy Shield framework has been judged 'adequate' by the EU, though it is subject to continuing judicial and administrative assessment.

B. Transfers Pursuant to Safeguards

In the absence of an Article 45 adequacy decision, the GDPR allows transfers of personal data outside the EU pursuant to various safeguard mechanisms specific to individual organizations under Article 46. These safeguards are applied on a case-by-case basis, under the guidance of one or more of the EU member states' data protection authorities (DPA) and are subject to their final approval.[30] The main ones are SCCs and BCRs.[31]

BCRs allow multinational companies to move data globally within a group of affiliated entities. To make use of the safeguard, a controller, or processor located within the EU must establish personal data protection policies consistent with the GDPR for transfers within a single conglomerate or within a group of enterprises engaged in a joint economic activity.[32] The obligations must be legally binding on the recipients and confer enforceable rights on data subjects.[33]

SCCs allow the transfer of personal data outside of the EU to a company that accepts the terms of standard form clauses previously approved by the EC.[34] These clauses require the data importer's agreement to the data protection law of the exporter in processing the data, to name data subjects as third party beneficiaries under the contract, and to agree to answer for breaches in a court of a member state.[35] They must be used exactly in the approved form unless an amendment is approved in advance by a DPA.[36]

---

28 GDPR recital 103.

29 See Adequacy Decisions, Eur. Commission, https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries en (last visited Dec. 31, 2019) (listing Andorra, Argentina, Canada, Faroe Island, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland, and Uruguay). The United States is also listed; however, its adequacy finding is "limited to the Privacy Shield framework." Id.

30 Jennifer Stoddart, Benny Chan, and Yann Joly, The European Union's Adequacy Approach to Privacy and International Data Sharing in Health Research 44 J. Law Med. Ethics, 143, 146 (2016).

31 Articles 40, 42 and 46 also provides for approved codes of conduct and certification schemes. However, to date there are no approved codes of conduct for international data transfers.

32 GDPR Article 47.

33 GDPR Article 47.2

34 GDPR Art. 46.2(c).

35 Commission Decision of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council (notified under document C(2010) 593) (2010/87/EU)) available at https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32010D0087&from=en.

36 GDPR Recital 109.

C. Transfers Pursuant to Derogations

The final category of permitted international transfers is derogations for specific situations.[37] Under the GDPR, the main ones are: consent by the data subject, transfers necessary for the performance of a contract between the data subject and the controller, or transfers necessary for the purposes of a legitimate interest pursued by the controller, which is available only after all other options have been tried and only for limited and infrequent transfers.[38]

D. Transfers and Health Data Under Chapter 5 of the GDPR

None of these mechanisms are ideally suited to transfers of medical data for research purposes. BCRs are a useful tool for multinationals to share data with affiliates. Outside of this scenario they have limited utility. Health organizations such as a national health service or university are not engaged in 'joint economic activity' with their research partners and so fail to qualify for BCRs. The task of writing an internal corporate code and obtaining approval from the relevant DPA is too expensive and time-consuming to pursue for temporary alliances, trials, or one-off exchanges.[39] BCRs therefore cannot facilitate most research combinations of data between multinationals, SMEs, health care organizations, and service providers.

SCCs also are problematic. Because model SCCs have to be written to cover every kind of data transfer, they contain terms too onerous for specific research purposes and relationships.[40] Parties may not negotiate any change, however without seeking official approval.[41] The three existing approved clauses apply only where an EU controller is exporting data,[42] and so cannot be used by EU processors looking to provide derived or observational data to controllers in the USA. The substantive terms of the clauses are also difficult for many US health processors. US public health bodies are not permitted to submit themselves to the jurisdiction of foreign states as required by the clauses.[43] Furthermore, standard US commercial insurance policies limit coverage to claims brought in US courts[44] and so would not cover any liabilities arising under an

37 GDPR Article 49

38 GDPR Article 49.1.

39 Aaditya Mattoo & Joshua P. Meltzer, International Data Flows and Privacy: The Conflict and its Resolution 11 (World Bank Group Policy Research Working Paper No. 8431 2018).

40 See Ropes & Gray, The GDPR One Year On (2019) available at https://www.ropesgray.com/en/newsroom/alerts/2019/07/GDPR-One-Year-On; Mattoo & Melzer, supra note 39 at 11.

41 Colin Mitchell, Johan Ordish & Alison Hall, Genomic Medicine and research: how does the GDPR apply?, 20 (2020) www.phgfoundation.org.

42 Commission Decision 2010/87/ of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council (notified under document C(2010) 593) 2010 O.J. L 39, 5 (12.2.2010); Commission Decision 2004/915/EC of 27 December 2004 amending Decision 2001/497/EC as regards the introduction of an alternative set of standard contractual clauses for the transfer of personal data to third countries 2004 O.J. L 385, 74; Commission Decision 2001/497/EC of 15 June 2001 on standard contractual clauses for the transfer of personal data to third countries, under Directive 95/46/EC, 2001 O.J. L 181, 19.

43 Rabesandratana, supra note 1.

44 See Marianne Bonner, Coverage Territory: what is it? The Balance Small Business (Jan. 23, 2019) https://www.thebalancesmb.com/coverage-territory-462649 ("For a suit to be covered under the CGL, it must be brought in the U.S.A. (including its territories or possessions), Puerto Rico or Canada.") (last visited Feb. 4, 2020).

SCC, which requires signatories to agree to be sued in the courts of the relevant Member state.[45] The clauses themselves were written over a decade ago under the GDPR's predecessor law and so imperfectly describe the controller–processor relationship.[46] Finally, the EU Advocate General examining a case (*Schrems II*) challenging SCCs with US entities has suggested that even when the approved SCCs are used, controllers must still conduct a context-specific inquiry into the underlying legal framework in the recipient state to ensure that the protections of the clauses are not undermined by local laws.[47] This case presents a particular risk for transfers to the USA under SCCs due to continuing concerns about structural deficiencies in US privacy law that potentially allow unduly extensive surveillance for the purposes of national security.[48]

The derogations under Article 49 are also quite limited. Article 49 (1) (a) states that a transfer of personal data to a third country may be made in the absence of an adequacy decision or of appropriate safeguards on the condition that 'the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards'.[49] Valid consent under this section must be specific and informed. This means that to provide a basis for transfer, consent must be given for the particular data transfer or set of transfers after the data subject is explicitly informed of the details of the transfers and the risks inherent to that specific transfer.[50] This is a difficult burden to meet for large-scale repositories of patient data typical in clinical trials and medical research studies that may be held for years and combined with other sources for new studies not anticipated at the date of collection.[51]

Similarly, 'necessary for performance of contract' is unlikely to apply as a basis for medical data transfer. In most cases, health data controllers based in the public sector are unlikely to have a commercial contract with patients or research subjects. Even where one does exist (for example, where a contract exists between a health app and a customer), the controller would have to show that the transfer of data overseas had a close and substantial link to the contract's main purpose.[52] The business convenience of the controller is not sufficient.[53] Finally, for sensitive health data, controllers still must

45 Mitchell et al. supra note 41 at 20.

46 Ropes & Gray, supra note 40.

47 See Opinion of the Advocate General, Data Protection Commissioner v. Facebook Ireland Ltd ¶¶ 127-139 (Dec. 19, 2019).

48 Id. at ¶¶ 40, 152.

49 GDPR Art. 49(1)(a).

50 Guidelines 2/2018 of the European Data Protection Board (EDPB) on derogations of Article 49 under Regulation 2016/679 7 (May 25, 2018) available at https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_2_2018_derogations_en.pdf; see also EC Commission Directorate-General for Health and Food Safety, Questions on the interplay between the Clinical Trials Regulation and the General Data Protection Regulation 9 https://ec.europa.eu/health/sites/health/files/files/documents/qa_clinicaltrials_gdpr_en.pdf.

51 Guidelines 2/2018, supra note 50 at 7.

52 See Guidelines 2/2019 of the EDPB on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects at 8-9 (Apr. 2019), https://edpb.europa.eu/sites/edpb/files/consultation/edpb_draft_guidelines-art_6-1-b-final_public_consultation_version_en.pdf.

53 Id.

demonstrate compliance with one of the additional heightened legal bases set out in Article 9(2)(b)–(j) notwithstanding anything in a contract.[54]

The ability to transfer data pursuant to a legitimate interest is also heavily circumscribed. First, the data transfer must be infrequent and limited in size, so this derogation could not be used to justify any activity that relies on regular data collection.[55] The legitimate interests necessary to justify the transfer must be more than the regular legitimate interests basis for processing under Article 6; the transfer must be 'essential' for the data controller and outweigh any 'competing' interests of the data subject.[56] Where entities seek to use this derogation, they must demonstrate that they have put in place appropriate safeguards and measures to protect the data subject's rights and must inform the EU supervisory authority and the data subject of the transfer of data.[57]

E. Anonymization

Anonymization of data places it outside the requirements of data protection legislation and so has long been the pathway of choice for sharing medical research data. Unfortunately, there is no clarity as to when health patient datasets may be considered anonymized under the GDPR. Biometric and whole genome sequence data are inherently unique to each natural subject, and thus at least potentially identifiable.[58] It is an open question whether individuation itself in data renders it 'identifiable'.[59] The GDPR links the assessment of identifiability to available technology.[60] Improvements in technology have made reidentification of even small amounts of genetic material more likely.[61] The GDPR is also unclear on whether common deidentification techniques, such as unique identifier codes held separately from the code key, are sufficient to render such data anonymous, or merely pseudonymized in which case the data would still be subject to the GDPR.[62] Furthermore, strict anonymization may render the data functionally useless for research as the most useful datasets for research are the ones that contain the greatest depth of detail about each subject.[63] Insufficient deidentification, on the other hand, carries legal and reputational risks, as a Chicago hospital recently learned when it shared what it thought was anonymous patient data with Google.[64] In this environment, many health organizations err on the side of

54 Article 29 Working Party Guidelines on consent under Regulation 2016/679 (WP259) at 19 (Apr. 10, 2018), https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051.

55 GDPR Art. 49(1) §2.

56 EDPB, Guidelines 2/2018 supra note 50 at 15–16.

57 Id. at 17.

58 E.g. GDPR Art. 4.14 (defining biometric data as personal data); Justin Banda, Inherently identifiable: Is it possible to anonymize health and genetic data?, IAPP Privacy Perspectives (Nov. 13, 2019) https://iapp.org/news/a/inherently-identifiable-is-it-possible-to-anonymize-health-and-genetic-data/.

59 See, e.g., Google Inc v Vidal-Hall [2015] EWCA Civ 311 ¶¶ 114-15; Bridges v. Chief Constable of Wales Police, [2019] EWHC 2341 ¶ 57 (2019).

60 GDPR Recital 26.

61 Mark Philips, Can Genetic Data Be Anonymised? Global Alliance for Genomics & Health (Oct. 10, 2018).

62 GDPR Article 4(5) & Recitals 26, 28 78.

63 Colin Mitchell, Johan Ordish & Alison Hall, Genomic Medicine and research: when does the GDPR apply? 7 Phg foundation (Jan. 2020) available at www.phgfoundation.org; R. Neethu & Timo Minssen, What lurks in the shadows of the openness hyperbole for biopharmaceuticals, 80 Drug. Dev. Res. 282, 283 (2019).

64 Class Action Complaint and Demand for Jury Trial, Dinerstein v. Google, LLC Case: 1:19-cv-04311 ¶¶ 5-6 (6/26/19).

caution, and treat all patient data as personal unless and until a supervisory authority assures them otherwise.[65]

F. Research Exemption

The GDPR offers expansive exemptions from notice and consent requirements where processing of personal health data is done for the purpose of scientific research in the public interest.[66] These research exemptions apply only within the supporting framework of EU or Member state law, however. [67] They cannot form the basis for a transfer of data to a jurisdiction where the laws are insufficiently protective. Indeed, as discussed further in Part III.E, US entities certified under the Privacy Shield must still comply with notice and consent requirements to use EU subject data in further research.[68]

G. Summary

To illustrate the potential risks of undertaking an international transfer of data under the current system, consider the examples from the introduction:

(1) A multinational pharmaceutical company sending data about drug safety and efficacy in certain populations to subsidiaries and affiliates in other jurisdictions;
(2) A clinical research organization managing a clinical trial in the EU may need to share outcome data with a US sponsor;
(3) Researchers in North America may seek to access sample or population data, including identifying phenotype characteristics, held in European biobanks, or vice versa;
(4) Makers of medical devices in the EU storing and accessing patient data through cloud storage providers whose servers are located in the USA.

Of these four common scenarios, only the first may definitely rely on an Article 46 safeguard (eg SCCs or BCRs), and even then, only after that safeguard has received approval from a supervisory authority. For the reasons detailed below, the other transfers will likely fail or be prohibitively difficult under Articles 46–49. Furthermore,

65 Mitchell et al., supra note 63 at 9.

66 GDPR Art. 6 (setting out lawful bases for processing, including consent and research in the public interest), 9.2 (h)(i) & (j) (allowing use of sensitive personal data for reasons of health or social care, protecting public health and for scientific research regardless of the non-profit status of the processor); Recital 159 ("For the purposes of this Regulation, the processing of personal data for scientific research purposes should be interpreted in a broad manner including for example technological development and demonstration, fundamental research, applied research and privately funded research.")

67 GDPR Art. 9.2(h)-(j) (allowing processing of sensitive data for the purposes of public health and scientific research so long as the processing is "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.")

68 United States Department of Commerce, EU-U.S. Privacy Shield Framework Principles Issued by the U.S. Department of Commerce, Supplemental Principles 14 https://www.privacyshield.gov/article?id=14-Pharmaceutical-and-Medical-Products [hereinafter Privacy Shield Principles].

depending on the outcome of the *Schrems II* decision, even SCCs may no longer be available as a mechanism to transfer data to the USA.

The European Data Protection Board (EDPB) is currently working on guidance for international transfers which may provide greater clarity on some of these issues.[69] Until then, the Privacy Shield is the most promising means for transfers of health data between the USA and EU but even that is problematic.

III. THE EU–US PRIVACY SHIELD

The US–EU Privacy Shield itself rests on a tenuous legal foundation. Although trade between the USA and the EU is extensive, finding common ground for treatment of consumer data has never been easy. The two regions approach the concept of personal privacy differently. Privacy of personal data is enshrined as a fundamental right in the EU Charter.[70] Trading in identifiable data is therefore forbidden in the EU unless a lawful basis applies.[71] In the USA, by contrast, certain forms of privacy are protected by law, but these are balanced against equally strong constitutional regard for free and unfettered speech, including commercial 'speech'.[72] In the USA, transfers of personal data are presumptively legal unless a particular prohibition applies.[73] From a regulatory standpoint, the USA favors a market-based approach wherein customers can choose levels of privacy as part of the product or service offered by a company.[74]

The Privacy Shield offers an uneasy compromise between the privacy absolutism of the GDPR and the more laissez-faire, self-regulatory approach of the USA. The Shield is an opt-in mechanism that allows US companies that want to receive transfers of personal information from EU subjects to self-certify as meeting certain standards.[75] Various arms of the US federal government have pledged to enforce those commitments, at least with respect to EU subjects.[76]

As an awkward hybrid of voluntary, private commitments and mandatory, public laws, the Privacy Shield's legal validity is doubtful under both EU and US law. From the EU side, it is vulnerable to court challenge that it does not offer adequate protection under the GDPR, both due to US law enforcement collection of personal data, and because enforcement of the Principles has been lax. From the US side, the Privacy Shield requires extensive EU monitoring and oversight of domestic federal agencies and requires the US government to create special mechanisms for EU subjects that are unavailable to US citizens. Critics contend that it neither assures adequate data

69 United Kingdom Information Commissioner's Office, Guide to the General Data Protection Regulation, International Transfers: In more detail - European Data Protection Board, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-transfers/ (visited Feb. 27, 2020).

70 Charter of Fundamental Rights of the European Union Arts 7, 8.1, 2000 O.J C 364/10, [hereinafter Charter]; see also Consolidated Version of the Treaty on the Functioning of the European Union art. 16, May 9, 2008, 2008 O.J. (C 115) 47 [hereinafter TFEU].

71 Charter Art. 52(1).

72 Paul Schwartz & Karl-Nikolaus Pfeifer, Transatlantic Data Privacy Law, 106 Geo. L.J. 115, 134 (2017).

73 Id. at 135.

74 Id. at 132.

75 Privacy Shield Principles, supra note 68 at 1.

76 Id. at 8-14, 24, Annex 1·

protection for EU subjects, nor preserves US sovereignty over its own commercial data protection policy.[77]

The Privacy Shield is an especially a poor fit for the health care sector. It omits from its coverage nonprofit research centers and health insurance providers, two major players in the US healthcare economy.[78] It also imposes special burdens on US medical research entities that are not required of similar enterprises within the EU. The Shield was designed to address concerns about law enforcement spying and internet platform monitoring that are not relevant to most transfers of health data.

A. The Origins of the Privacy Shield

The Privacy Shield was created and implemented as a stopgap. On October 6, 2015 the Court of Justice for the European Union (CJEU) invalidated the Safe Harbor Agreement, the framework that had allowed transatlantic exchanges of data for 15 years.[79] The Court found that the protections in the Safe Harbor were inadequate in light of the Snowden revelations that US law enforcement and national security agencies were obtaining and monitoring identifiable signal data obtained by US companies.[80] The *Schrems I* decision sent US and EU official scrambling to put a replacement framework in place to avoid destabilizing trillions of dollars in EU–US trade in goods and services.[81] Just under 3 months later, on February 2, 2016, the US Department of Commerce (DoC) issued the Privacy Shield Principles.

To rely on Privacy Shield to transfer commercial data from the EU, participating organizations must self-certify to the US DoC their adherence to 23 principles laying out the requirements for the use and treatment of personal data received from the EU, as well as access requests and recourse mechanisms for EU citizen complaints.[82] The EC declared on July 12, 2016 that organizations that are Privacy Shield-certified provide 'adequate' privacy protection to personal data transferred outside of the EU under the EU Data Protection Directive, which has since been superseded by GDPR.[83]

Like the Safe Harbor before it, the Privacy Shield depends on the voluntary participation of US companies. Once a company enters the program, however compliance is compulsory.[84] An organization's failure to comply is subject to prosecution under Section 5 of the Federal Trade Commission (FTC) Act prohibiting unfair and deceptive acts in or affecting commerce.[85]

B. The Privacy Shield Framework Under EU Law

Notwithstanding the Commission's 2016 decision, the adequacy of the Privacy Shield under the GDPR is far from evident. Formally, the Shield provides a lawful basis for transfer under Article 45 of the GDPR, which allows transfers to foreign jurisdictions

77 See text accompanying notes 87-119 infra.
78 See BBMI-ERIC FAQs on the GDPR V2.0 18 (2017) http://www.bbmri-eric.eu/wp-content/uploads/BBMRI-ERIC_FAQs_on_the_GDPR_V2.0.pdf.
79 Schrems I, supra note 3.
80 Id. at ¶ 94.
81 Mattoo & Meltzer, supra note 39 at 4.
82 Privacy Shield Principles, supra note 68.
83 Commission Implementing Decision supra note 4.
84 Privacy Shield Principles, supra note 68 at 1.
85 15 U.S.C. § 45(a).

deemed to have 'adequate' legal regimes. In practice, however the Shield is not a mandatory legal regime. Instead it has the characteristics of the opt-in company safeguards found in Article 46 of the GDPR, such as codes of conduct, certification schemes and BCRs. Like these mechanisms, the Privacy Shield Principles apply only when companies choose to participate.

It is unclear whether a voluntary opt-in regime can really meet the adequacy threshold under Article 45. The purpose of an adequacy inquiry under Article 45 is to examine the law and practices of the third country as a whole to ensure that the legal framework is sufficiently protective.[86] Voluntary and individual corporate codes of practice are not usually considered relevant. Even considered under Article 46, the Privacy Shield does not meet the standards for organization-specific mechanisms. Article 46 requires private entities to submit their chosen safeguards to initial approval and ongoing, direct supervision by European DPA or their delegated bodies for validity.[87] The Privacy Shield by contrast allows US companies to self-certify without independent verification even by US authorities.[88] Enforcement of its terms is in practice left almost entirely to private action—companies largely self-monitor compliance, and EU subjects must formally complain directly to have access to the limited rights of redress under its terms. There is reason to believe that dozens of companies have declared their activities to be compliant with the Shield while not complying in fact.[89] If challenged on this basis, the Shield might be vulnerable to claim that it cannot offer 'equivalent' protection to that found in the GDPR, the standard the CJEU laid down in Safe Harbor case for 'adequacy', because it does not meet even the minimum standards set out for functionally equivalent safeguard mechanisms under Article 46.[90]

The Shield is in more direct legal jeopardy in the EU from the second lawsuit by Maximilian Schrems, the plaintiff in the Safe Harbor case, alleging that the US has not substantively improved its data protection practices since the Safe Harbor was invalidated.[91] Although the *Schrems II* lawsuit aims at SCCs rather than the Privacy Shield, the allegations that intrusive US law enforcement practices undermine private contractual commitments also implicate the viability of the Privacy Shield.[92] There is also a second French lawsuit directly challenging the Privacy Shield on these grounds

86 See, e.g., Opinion of the Advocate General, supra note 47 at ¶119; cf. Schrems I, supra note 3 at ¶ 74.

87 See GDPR §§ 40 (setting out minimum standards for codes of conduct), 41 (requiring ongoing monitoring of compliance with codes of conduct), 42 (setting out minimum certification standards and requiring advance approval and periodic re-authorisation by a certification body before a certification may be used), 43 (setting out the duties of certification bodies to demonstrate expertise and monitor compliance with certification schemes), 46 (requiring advance supervisory authority approval for standard contractual clauses), 47 (requiring advance supervisory authority approval for binding corporate rules) 57 (requiring supervisory authorities to

88 Privacy Shield Principles, supra note 68 at Supplemental Principles §§ 6, 7.

89 Fabien Terpan, EU-US Data Transfer From Safe Harbour to Privacy Shield: Back to Square One, Eur. Papers Vol. 3 1045, 1053 (2018).

90 Schrems I, supra note 3 at ¶¶ 73–74, 96 (standard for adequacy is equivalency); see also Terpan, supra note 90 at 1052 (validity of the new regime remains fragil[e).]

91 Case C-311/18 Data Protection Commissioner v Facebook Ireland Limited, Maximillian Schrems, 2018 O.J. C 249, 15–17 [hereinafter Schrems II].

92 Minssen et. al., supra note 8 at 41-43 (2020); see also Terpan, supra note 90 at 1053 (US public authorities indiscriminately made use of the exemption from data protection for national security under the Safe Harbor and there is little reason to believe practices have changed under the Privacy Shield.)

that has been stayed pending the outcome of *Schrems II*.[93] The plaintiffs in these cases contend that the Privacy Shield offers no improvements to the Safe Harbor regime that are binding on national security services and so the legal framework in the USA is still inadequate notwithstanding undertakings made by private businesses.[94]

The recent Opinion of the Advocate General (AG) in *Schrems II*, which is persuasive but not binding on the CJEU, offered some assurances that SCCs and the Privacy Shield framework are not at immediate risk of being invalidated. The AG concluded that the SCC mechanism was overall adequate to protect fundamental rights of privacy and suggested that the Court does not need to render judgment on the validity of the EU–US Privacy Shield Framework to decide the case.[95] However, the AG went on to raise some concerns about whether the Privacy Shield Framework in general met the adequacy threshold.[96] Based on previous jurisprudence, the AG considered that surveillance by US authorities was generally justified on the grounds of public interest.[97] He expressed reservations, however as to whether it contained adequate safeguards enshrined in law to prevent the risks of abuse.[98] The AG advised against addressing these deficiencies for the case and noted that supervisory authorities could consider the necessity and proportionality principles as well as the fundamental right to respect for a private life on a case-by-case basis with regard to transfers made pursuant to SCCs.[99] This emphasis on case-by-case inquiry, if adopted by the Court and individual DPA, could undermine the efficiency of general transfer mechanisms such as SCCs and the Privacy Shield. Furthermore, the CJEU could still potentially decide to invalidate the EU–US Privacy Shield Framework in its decision in the *Schrems II* case, or in the subsequent direct challenge. This possibility poses substantial legal risk to companies currently relying on the adequacy of the Privacy Shield mechanism. In the meantime, the continued legal vulnerability of the regime under EU law has led many US companies to delay undertaking the time and effort required to certify under the Shield.[100]

C. The Privacy Shield Under US Law

Nor does the Privacy Shield protect US interests in domestic policy sovereignty. Many policymakers and industry representatives in the US think that its self-regulatory and patchwork approach is more hospitable to innovation than the 'one size fits all' EU privacy rules.[101] They argue that data privacy experimentation may promote advances

93 Case T-738/16 La Quadrature du Net v Commission (2017/C 006/49), ECLI:EU:T:2018:520 (4 Sept. 2018).

94 Case T-738/16 La Quadrature du Net v Commission (2017/C 006/49), https://eur-lex.europa.eu/legal-content/en/TXT/PDF/?uri=uriserv%3AOJ.C_.2017.006.01.0039.01.ENG.

95 See Opinion of the Advocate General, supra note 47 at ¶¶ 160, 182, 186

96 Id. at ¶¶ 308, 341, 342.

97 Id. at ¶¶ 282, 286.

98 Id. at ¶¶ 294-97.

99 Id. at 194.

100 Lothar Determan, Brian Hengesbaugh, & Michaela Weigl, The EU-US Privacy Shield Versus Other EU Data Compliance Options, Privacy Law Watch (Aug. 29, 2016), https://www.bna.com/uploadedFiles/BNA_V2/Legal/Pages/Custom_Trials/BLPV/Tips_for_US_Companies_EU_GDPR_Privacy_Shield_final.pdf.

101 Martin A. Weiss & Kristin Archik, US-EU Data Privacy: From Safe Harbor to Privacy Shield, Congressional Research Service 7-5700 R442574 (May 19, 2016) ("Many US officials and industry representatives

in the information technology and internet commerce sectors, whereas blanket prohibitions stifle technology firms.[102] The USA has therefore been wary of saddling itself with complex and burdensome data protection rules before their utility has been proven.

Ironically, then, the decision to operate via the Privacy Shield undermines the ability of US companies to experiment, at least with respect to any data originating from the EU. US companies that choose to receive data under the Privacy Shield are effectively promising to follow EU law. By contrast, companies in Israel, Canada, Japan, and Argentina, to name a few, can process EU data under their own law without regard to the GDPR because their governments applied for and received an 'adequacy' determination under Article 45 of the GDPR. The laws of many of these 'adequate' jurisdictions differ in material respects from the GDPR but the EU has been willing to tolerate divisions in approach so long as the overall scheme achieves the aims of data protection.[103] US companies are therefore at a comparative disadvantage because they have to assume the significant costs of compliance with US laws and the GDPR whereas their international counterparts follow only domestic law. Furthermore, because the Privacy Shield is nominally a 'voluntary' regime, US companies lack the support of domestic information agencies helping to interpret any ambiguity in the rules, and so must absorb completely as a private expense the legal compliance costs associated with a new and untested regime.[104] Companies certified under the Shield also face the threat of investigation from multiple jurisdictions as they are subject to enforcement not only from the FTC but also individual EU DPA.[105] Companies in countries that have received adequacy determinations, by contrast, are free to receive data from EU subjects under their own laws without further interference or annual audits from the EU.[106]

The US government is under a similarly tight leash. The Commission's 2016 US adequacy decision for the Privacy Shield was tentative at best, and its continuation depends on the US federal agencies submitting annually to detailed audits by the EC.[107] The Commission is empowered to investigate the functioning of all aspects of the

maintain that the US approach to data privacy is more nimble than what they view as the EU's one size fits all approach.").

102 Schwartz & Peifer, supra note 73 at 157 (2017); Weiss & Archik, supra note 102 at 4; Thomas Davenport, Should the US adopt European-style Data Privacy Protections: No, Stronger Privacy Rules Could Squelch Innovation Wall St J R.7 (Mar. 10, 2013); Natasha Singer, Data Protection Laws, An Ocean Apart, N.Y. Times Feb. 2, 2013 at B3·

103 See text accompanying notes 177- 191, infra.

104 Kirk J. Nahra, Impact of the US-EU Privacy Shield on Health-Care Data Transfers (Bloomberg Law Insights Aug. 1, 2016) (stating that the Privacy Shield is a 'significant mountain to climb for companies new to the program.') reprinted in Tips For US Companies in the Age of E.U. GDPR and Privacy Shield, supra note 101.

105 Privacy Shield Principles, supra note 68 at §11(a).

106 E.g. Opinion 28/2018 Regarding the European Commission Draft Implementing Decision on the Adequate Protection of Personal Data in Japan, Eur. Data Protection Board (Dec. 5, 2018), https://edpb.europa.eu/sites/edpb/files/files/filel/2018-12-05-opinion_2018-28_art.70_japan-adequacy-en.pdf. P 181. (requiring one review after two years, and periodic reviews of Japan's regime every 4 years thereafter); See also, Gabor Gerenscar, The European Union and Japan adopt adequacy decisions, IAPP https://iapp.org/news/a/the-european-union-and-japan-adopt-adequacy-decisions/ (Jan. 24, 2019).

107 See, e.g., Report from the Commission to the European Parliament and the Council on the first annual review of the functioning of the EU-US Privacy Shield at 2 COM (2017) 611 final (18.10.2017) (hereinafter "First Annual Report").

Privacy Shield including enforcement statistics, key staffing decisions and updates on any relevant development under US law.[108] At the first annual review, the Commission issued 10 detailed recommendations for improvement to the management of the scheme.[109] For the second and third annual reviews, the EC sought information not only from the DoC and the FTC, the agencies tasked with enforcing the Shield, but also sent questionnaires to 10 US trade associations and eight NGOs to get a broad picture of the practical implementation of the Privacy Shield framework by private entities.[110] The Commission has sought several substantive changes in the way that the DoC and the FTC implement the scheme, including more interrogation of certification claims, more spot checks on continued compliance, and more proactive investigations of false claims of compliance.[111] The EC has been vocal that making these changes is vital to the Shield's continued adequacy.[112]

The authority of DoC and the FTC to make such extensive commitments on behalf of non-US citizens is unclear. As federal agencies, the DoC and the FTC can exercise only those powers specifically granted by the Constitution to the executive branch or delegated by Congress.[113] If the Privacy Shield is a voluntary scheme for private companies, then development of the Privacy Shield Framework falls within the DoC's inherent mandate to foster and promote international commerce.[114] However, the Framework, at least as interpreted by the EU, goes beyond setting out optional requirements for private companies. It also obligates agencies of the federal government to undertake particular actions outside their usual remit. These include, for the DoC, the duty to monitor whether US companies publish their privacy commitments,[115] to conduct periodic compliance reviews[116] and audits of listed and delisted companies,[117] and to manage the establishment of special tribunals ('Privacy Shield Panels') available only to EU residents.[118]

---

108 Id. at 2-7; Commission Staff Working Document Accompanying the document, Report From The Commission To The European Parliament And The Council on the third annual review of the functioning of the EU-U.S. Privacy Shield 25-27 COM(2019) 495 final (23.10.2019) (hereinafter, "Third Review Working Document").

109 First Annual Report, at 2–7.

110 Third Review Working Document, supra note 109 at 3; Commission Staff Working Document accompanying Report from the EC to the Parliament on the second annual review of the functioning of the EU-U.S. Privacy Shield 2 COM(2018) 860 final (19.12.2018) (hereinafter "Second Review Working Document").

111 Third Review Working Document supra note 109 at 9-12; Second Review Working Document supra note 111 at 3–5, 8.

112 Report From The Commission To The European Parliament And The Council on the third annual review of the functioning of the EU-U.S. Privacy Shield 4 COM(2019) 495 final (23.10.2019) [hereinafter Third Annual Report]; see also Third Review Working Document supra note 109 at 12 ("Commission services therefore consider that the FTC should, as a matter of priority, find ways to share meaningful information on ongoing investigations with the Commission as well as with EU DPAs.")

113 US Const. Art II §2; J.W. Hampton v. United States, 276 U.S. 394 (1928).

114 15 U.S.C. § 1512.

115 Commission Implementing Decision, supra note 4 at P. 32; Third Review Working Document supra note 109 at 9–10.

116 Third Annual Report, supra note 113 at 4.

117 Commission Implementing Decision (EU), supra note 4 at P 35, 37.

118 Privacy Shield Principles, supra note 68 at 11(d)(iv) & Annex 1. While the tribunals are nominally selected and funded by individual companies operating under the Shield, DoC commits itself to unusual actions such as selecting a panel of arbitrators and negotiating the rules for such arbitration with the EU Commission, and establishing and running a fund to pay for the tribunals. Id. at Annex 1 § F.

The FTC, the agency charged with enforcing Privacy Shield commitments made by private entities, has broad enforcement authority but is similarly overextended by the EU's demands. The FTC has the power under its originating act to police deceptive conduct in interstate commerce. The US courts have tended to take a permissive stance on the question of whether the FTC's enforcement power extends to conduct directed at overseas markets. In *Branch v. Federal Trade Commission*, a case concerning misrepresentations about a correspondence course offered only to students in Latin America, the 7th Circuit Court of Appeals held that enforcement fell within the Agency's authority because (i) the deception was conceived and initiated within the USA and (ii) the agency's mandate to ensure a level playing field for the company's competitors within the USA included preventing deception targeted to overseas customers.[119] Similarly, the FTC's Privacy Shield enforcement ensures fair competition among domestic companies who seek to process EU personal data. Companies that do not comply gain an unfair advantage and risk undermining the credibility of the whole scheme.[120] However, certain agency obligations, as interpreted by the EC, seem to reach beyond this limited authority. These include a commitment by the FTC to priority review of EU complaints of noncompliance[121] and, according to the EC, an obligation to undertake proactive ex officio sweeps of listed companies without any basis for believing deceptive conduct has occurred.[122] Such promises force the FTC to prioritize EU privacy misrepresentations over other kinds of deceptive conduct and to commit scarce enforcement resources for the sole benefit of citizens of foreign states. These state-to-state commitments arguably fall well outside §5's remit, and should require specific congressional approval under the Art II Treaty Power of the US Constitution.[123] Perhaps for this reason, the US agencies have sullenly resisted meeting

119 Branch v. Federal Trade Comm'n, 141 F.2d 31, 34–35 (7th Cir. 1944).

120 Cf., Hayley Evans & Shannon Togawa Mercer, Privacy Shield on Shaky Ground—What's Up with EU-US Data Privacy Regulations, Lawfare Blog available at https://www.lawfareblog.com/privacy-shield-shaky-ground-whats-eu-us-data-privacy-regulations (last visited Dec. 9, 2019) (Actions against companies that fraudulently claim to be certified when they are not prevent bad actors from undermining the credibility of the whole framework).

121 Commission Implementing Decision supra note 4 at ¶ 54; Privacy Shield Principles, supra note 68 at §11(f)(ii).

122 Third Annual Report, supra note 113 at 5.

123 There are three ways that the executive branch of the US government may make binding agreements with foreign powers. Under Article II of the US Constitution, the President can negotiate a treaty which becomes effective upon ratification by two thirds of the Senate. US Const. Art. II §2. The President may also negotiate undertakings that are ratified by a majority vote in both houses of Congress. Michael D. Ramsey, Executive Agreements and the (Non)Treaty Power, 77 N.C. L. Rev. 133, 135 (1998). Finally, the Supreme Court has recognized that the President may enter into binding executive agreements by virtue of the President's inherent power in foreign affairs. Id. The Privacy Shield does not qualify as a treaty or undertaking ratified by Congress. It might be an executive agreement negotiated by the Department of Commerce. However, executive agencies may not commit funds or other national resources without Congressional approval, nor may they usurp Congress' authority to legislate domestically. Louis Henkin, Treaties, the Treaty Power, and Executive Agreements 206-07, 229 (Oxford UP, 1996) ("If a treaty entails domestic regulation and legal consequence in the United States, and is not self-executing, or if it requires appropriation of funds, the President has to seek Congressional action"); see also Ramsey, supra at 138 (changes to domestic legislation require Congressional approval); Saikrishna B. Prakash and Michael D. Ramsey, The Executive Power over Foreign Affairs, 3 Yale L.J. 231, 235 (2001) (stating that the executive's foreign affairs power does not extend to domestic lawmaking); Paul M. Schwartz, Global Data Privacy: the EU Way, 94 NYU L. Rev. 771, 805

the EC's demands for enhanced enforcement efforts, and so have further imperiled the 'adequacy' of the scheme under the GDPR.[124]

D. Unsuitability of the Privacy Shield for Transfers of Health Data

The Privacy Shield is not even useful as a temporary stopgap for many exchanges of healthcare data between the USA and the EU because many US health care providers and payors are excluded from its terms. The Privacy Shield is currently an option only for organizations subject to the jurisdiction of the FTC or the Department of Transportation.[125] Insurance companies in the USA are regulated primarily by state insurance commissioners and are not generally subject to enforcement by the FTC.[126] The FTC's jurisdiction also does not generally extend to nonprofit entities.[127] Health care providers, hospitals, and other care organizations that operate on this basis may be excluded from the Shield's framework entirely.[128]

When available, the Shield places asymmetric burdens on researchers in medicine, public health and social care in the USA. Under the GDPR, EU controllers of all types can process sensitive health data for purposes of treatment, social care, public health, or medical research as an independent lawful basis.[129] They need not obtain the specific consent of the subject or offer mechanisms to withdraw that consent.[130] (Ethics regimes may impose independent consent requirements, but these do not necessarily provide data subjects with an option for withdrawal).[131] This is a substantial advantage for administering complicated, multiyear clinical studies. Controllers in the USA, by contrast, must comply under the Privacy Shield with detailed and untested requirements for explicit consent from data subjects even for public health and medical research uses.[132] The Privacy Shield offers only a very narrow exception for process-

(2019) (US government formal commitments in Privacy Shield represent de jure law rather than informal commitments).

124 Third Review Working Document supra note 109 at 10–12.

125 Nahra, supra note 105.

126 Id.

127 See Letter from Federal Trade Commission Chairwoman Edith Ramirez 2 (Jul. 7, 2016), attached as Annex IV, Commission Implementing Decision supra note 4 at L207/79.

128 Id.

129 GDPR Art. 6 (setting out lawful bases for processing, including consent and research in the public interest), 9.1 (h)(i) & (j) (allowing use of sensitive personal data for reasons of health or social care, protecting public health and for scientific research regardless of the non-profit status of the processor); recital 159 ("For the purposes of this Regulation, the processing of personal data for scientific research purposes should be interpreted in a broad manner including for example technological development and demonstration, fundamental research, applied research and privately funded research.")

130 GDPR Art. 6, 7 (providing obligations required only when the lawful basis for processing is consent), & 9.1 (h)(i) & (j). See also GDPR Recitals 51–54; see also Ciara Staunton, Santa Slokenberga & Deborah Mascalzoni, The GDPR and the research exemption: considerations on the necessary safeguards for research biobanks, 27 Eur J Hum Genetics 1159, 1161 (2019) (noting the wide scope of GDPR's research exemption).

131 See Staunton, Slokenberga & Mascalzoni, supra note 131 at 1160.

132 Like the GDPR, the Privacy Shield does not define what constitutes adequate notice and consent when future research uses cannot be specified in advance. Privacy Shield Supplemental Principles, Pharmaceutical and Medical Products at b(i) & (ii). However, unlike the GDPR, which contains broad research and healthcare exemptions from consent requirements, the Privacy Shield has only a narrow exception from consent requirements for medical research purposes. Compare Privacy Shield Supplemental Principles, Sensitive Data a(iii) & (iv) (exempting organization's from affirmative consent requirements for sensitive

ing for direct 'medical care and diagnosis' or for research specifically by 'non-profit entities'.[133] Many US health providers and some research institutions operate as for-profits. Those that do operate as nonprofits are outside the jurisdiction of the FTC, and probably cannot make use of the Shield framework and its research exceptions at all. The practical impact of these additional restrictions is to impose heavier compliance burdens on US research entities than on their EU counterparts, and so to hinder cross-border research and innovation. [134] On the other hand, where use without consent for research purposes is allowed, the Privacy Shield contains none of the additional organizational and technological safeguards for such data that are set out in the GDPR.[135] The Privacy Shield is therefore both unduly burdensome on US health research and unduly lenient on actual patient protections when health data are used.

Health service providers and researchers are caught in the uncertainty surrounding the Privacy Shield even though the concerns targeted by Privacy Shield are tangential to healthcare treatment and research. Long-term health and treatment data have little direct utility in preventing terrorist attacks, and US law enforcement and national security agencies have shown little interest in monitoring it. Although there is concern over search engines, platforms, and online retailers gaining personal health data, the US domestic medical privacy law, HIPAA, could be employed to address those concerns in the same manner as the GDPR. Meanwhile, as discussed in Part I, there is a wealth of relatively uncomplicated transfers for the purposes of storage, analysis, and treatment services that are unnecessarily complicated by the theatrics surrounding the Privacy Shield's viability. If the Privacy Shield and SCC frameworks are struck down or hobbled in the *Schrems II* decision, the need for an independent basis under which to transfer health data to the USA will become even more urgent.

IV. ESTABLISHING A HIPAA SHIELD

In Section IV we argue that one way to overcome the problems with the EU–US Privacy Shield for transfers of health data would be to request a sector specific adequacy decision. Many in the health sector advocate for a sector-specific solution to allow research transfers of data to proceed internationally.[136] We support such efforts, and suspect an option is available that has been overlooked. The USA has already signaled its agreement with many of the GDPR principles as applied to data concerning health. The US has an existing health data protection law, the Privacy Rule promulgated under

data only when it is required to provide medical care or diagnosis or for research carried out by a non-profit entity) with GDPR Art 9.1 (h)(i) & (j) (providing independent legal bases for use of sensitive personal data for reasons of health or social care, protecting public health and for scientific research regardless of the non-profit status of the processor). See also Nahra, supra note 105 (use of sensitive information in research will depend on providing appropriate notice and choice in the first instance under the Privacy Shield).

133 Privacy Shield Principles, supra note 68 Supplemental Principles, Sensitive Data a(iii) & (iv); GDPR Art 9.1 (h)(i) & (j).

134 Compare Privacy Shield Principles supra note 68 at § 4 with GDPR Art 9.1 (d), (g), (h), (i), (j), 9.3 & 89 (setting out lawful bases for processing of sensitive data, including health data, such as when in the substantial public interest, for the provision of health or social care subject to safeguards, in the interest of public health, or for scientific research subject to safeguards). See also GDPR Recitals 51–54.

135 E.g. GDPR Art 6.4 (setting out organizational and technical measures that must be followed when the basis for processing is research in the public interest).

136 See, e.g., Colin Mitchell, Johan Ordish & Alison Hall, Genomic Medicine and research: how does the GDPR apply?, at 3, 23 phg foundation available at www.phgfoundation.org (last visited Jan. 31, 2020).

the HIPAA,[137] that could serve as the basis for a sector-specific adequacy decision. A health sector 'shield' based on HIPAA's Privacy Rule would not replace the EU–US privacy shield, nor SCCs, BCRs, or informed consent. It would be an additional legal basis for lawful international transfer of personal health data. In this section we outline (i) the advantages that the HIPAA shield would have over the EU–US privacy shield. We also discuss (ii) whether HIPAA would likely meet the 'adequacy' standard, and (iii) the modifications that are likely to be required.

The US legal framework for certain kinds of private information, such as health information, is not dissimilar to that of the EU. The USA has had a comprehensive medical data privacy regulation since 2002, when HIPAA's Privacy Rule was promulgated by the Department of Health and Human Services.[138] The regulation's initial reach was quite narrow; it originally prescribed privacy and patient data security rules only for 'covered entities', including clinicians, health care facilities, pharmacies, health insurance plans, and health care clearinghouses.[139] The 2009 HITECH Act extended its reach to cover practices of companies working with covered entities—'business associates' in the law's parlance—and also challenges arising from electronic health records.[140] Together with the administrative regulations promulgated under these Acts,[141] the HIPAA Privacy Rule has proved a functional and balanced approach to privacy of medical records and personal health data.[142]

HIPAA's Privacy Rule contains many similarities to the GDPR. Under HIPAA, as under the GDPR, use or disclosure of personal information is forbidden unless the subject explicitly consents or a specific exception applies.[143] Covered entities may freely use and disclose personal information without prior permission for treatment, payment, operations, and certain public benefit activities such as research or law enforcement activities.[144] These exceptions are similar to GDPR's list of lawful bases for processing such as vital interests of the subject, performance of a contract, a task carried out in the public interest, or the legitimate interests of the processor.[145] As under the GDPR, specific consent must be obtained before using or disclosing personal health information in a situation that is not one of the listed exceptions.[146]

137 Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub. L. No. 104–191, §§ 261–64, 110 Stat. 1936 (1996) ("HIPAA").

138 Standards for Privacy of Individually Identifiable Health Information, 67 Fed. Reg. 53,182 (Aug. 14, 2002).

139 I. Glenn Cohen & Michelle D. Mello, HIPAA and Protecting Health Information in the 21st Century, 320 JAMA 231, 231 (2018).

140 Health Information Technology for Economic and Clinical Health Act, Pub. L. No. 111–5, § 13001–13424, at 13401, 123 Stat. 227-279, at 260 (2009) codified at 42 U.S.C. 17931.

141 Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. 82,462 (Dec. 28, 2000); Standards for Privacy of Individually Identifiable Health Information, 67 Fed. Reg. 53,182 (Aug. 12, 2002); Privacy of Individually Identifiable Health Information, 45 CFR §§ 164.500–164.534.

142 Cohen & Mello, supra note 140 at 231.

143 45 C.F.R. § 164.508(a)(1); see also U.S. Dept. of Health and Human Services, Summary of HIPAA Privacy Rule, https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html. ("A major purpose of the Privacy Rule is to define and limit the circumstances in which an individual's protected heath information may be used or disclosed by covered entities. A covered entity may not use or disclose protected health information, except either: (1) as the Privacy Rule permits or requires; or (2) as the individual who is the subject of the information (or the individual's personal representative) authorizes in writing.").

144 Stacey A. Torvino, The HIPAA Privacy Rule and the EU GDPR, 47 Seton Hall L. Rev. 973, 982–83 (2017).

145 GDPR Art. 6(1).

146 See 45 C.F.R. §§ 164.502, 164.508(a)(1) .

HIPAA defines Protected Health Information (PHI) broadly to include any health-related information that can be used to identify a particular individual.[147] This can be information related to an individual's past, present, or future physical or mental health or condition, any provisions of healthcare to an individual, and any past, present, or future payment for the provision of healthcare to an individual.[148] This scope is similar to the definition of Data Concerning Health under the GDPR.[149] The HIPAA Privacy Rule does not define 'authorization' in the same detail that the GDPR defines consent, but both laws require notice and transparency to the subject about specific uses for consent to be considered valid.[150] Both laws require additional disclosures and safeguards before individual data can be used for 'marketing' purposes.[151] Under both frameworks, individuals have a right to withdraw consent, although this right is less robust under HIPAA.[152] Both frameworks require use of technical and organizational measures to protect the security of data concerning health, although in the case of HIPAA, this rule applies only to records kept in electronic form.[153]

The main difference between the GDPR and HIPAA is HIPAA's narrower application. Where the GDPR governs any entity that processes personal information of EU subjects, HIPAA applies only to regulated health care entities such as clinicians, hospitals, and insurance companies.[154] It also permits disclosure of PHI to 'business associates' of covered entities subject to contractual restrictions ensuring appropriate use and storage.[155] Business associates covered by the Privacy Rules are persons or organizations that provide legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services to a covered entity.[156] A business associate processing personal health data covered by the HIPAA Privacy Rule must do so under prescribed terms. Covered health entities must impose through agreements with their business associates (i) obligations to use protected data only as permitted under the contract and (ii) appropriate safeguards to prevent unauthorized use or disclosure.[157] Under 2009 amendments, business associates and their

147 45 C.F.R. § 160.103 (2016) (definition of Individually Identifiable Health Information & Protected Health Information).

148 Id.

149 GDPR Article 4(1).

150 GDPR Article 4(11).

151 Torvino, supra note 145 at 989.

152 45 CFR § 164.508(b) & (c); EU GDPR Art 7 § 3. Note that this right is more limited under the HIPAA Privacy Rule, and patients under HIPAA have no 'right to erasure' as under the GDPR. Torvino, supra note 145 at 988, 991.

153 Security Standards for the Protection of Electronic Protected Health Information, 45 C.F.R. Subpart C § 164.302 et. seq.; GDPR Art. 32. State laws governing confidentiality of medical information could also apply in the U.S.

154 HIPAA § 262(a) ("Any standard adopted under this part shall apply, in whole or in part, to the following persons: '(1) A health plan. (2) A health care clearinghouse. (3) A health care provider who transmits any health information in electronic form in connection with a transaction referred to in section 1173(a)(1)."'); Standards for Privacy of Individually Identifiable Health Information, 64 Fed. Reg. at 59,918. See generally Standards for Privacy of Individually Identifiable Health Information, 64 Fed. Reg. 59,918 & 59,924 (proposed Nov. 3, 1999) (to be codified at 45 C.F.R. pts. 160–64) (explaining that HHS did not directly regulate any entity that was not a covered entity in the Privacy Rule because it did not have the statutory authority to do so).

155 See 45 C.F.R. §§ 164.308(b)(1)–(3), 164.314(a)(1)–(2).

156 45 C.F.R. § 160.103 definition of 'business associate'.

157 45 CFR 164.504(e).

subcontractors can be held directly liable for breach of HIPAA's Privacy Rule.[158] HIPAA's reach is narrower than the GDPR but it provides strict, GDPR-like rules for an important subsection of the US economy.

A. Advantages of Sector-Specific Adequacy Under HIPAA

Pursuing an adequacy determination based on HIPAA has several advantages. For the USA, an adequacy determination would allow transfers of data without continued oversight and monitoring by the EU. US health companies could obey one set of rules and need only submit to the jurisdiction of one set of regulators. Given the similarities between the two frameworks for healthcare, the process to obtain adequacy based on HIPAA could be relatively quick. Tailoring privacy rules to a sector where there is already substantial convergence in values and approach will allow for easier resolution of new policy challenges specific to the health sector, such as consent for follow on research studies, or the meaning of anonymization in the case of biometric data. Such a resolution can provide a useful model to other non-EU countries who may lack the resources to develop comprehensive data regulation but want to preserve open data exchanges for critical sectors.

The main advantage of an adequacy determination is that it will greatly simplify exchanges of health data critical for care, treatment, research, services, and public health. Once a country or an individual sector is deemed 'adequate' by the EC, personal data may then be transferred from EU Member States without additional guarantees or constant monitoring being necessary.[159] Under the GDPR, the only continuing assessment required are periodic reviews at least every four years.[160] US entities would benefit because they would need to comply with only one well-established Privacy Rule about patient data. They could save the considerable costs of annual self-certification under a second, conflicting regime at continual risk of being struck down.

Second, a limited HIPAA-based 'shield' would be managed and maintained by US regulators without undue interference from Brussels. US citizens would be equally entitled to its protections, and US enforcement efforts would not be inappropriately tilted toward EU citizens. The legislature writing the rules would have democratic accountability to both the data subjects and the affected businesses. Legislative competition between the US and the EU, both for healthcare and for sectors outside the HIPAA shield, could promote legal innovation in response to rapidly changing technologies and business models.

Third, pursuing a sector-based adequacy determination is achievable in the short term, whereas efforts to craft a comprehensive US privacy regime could take years. The US has pursued a sector-based approach to data protection because little consensus exists outside certain fields about what kinds of rules should govern uses of consumer data. Where states have filled in the gaps with their own comprehensive schemes,

158 Health Information Technology for Economic and Clinical Health Act, § 13401, 123 Stat. at 260.

159 Mark Phillips, International data-sharing norms: from the OECD to the General Data Protection Regulation (GDPR), 137 Hum Genet. 575, 562 (2018) ("Because the decisions generally cover legal frameworks of general application, in these situations virtually no extra effort is required to operationalize adequacy as justification.")

160 GDPR Art. 45(3).

such as the new California Consumer Protection Act (CCPA),[161] they have drawn intense opposition from the retail and technology industries.[162] Business lobbies are now more amenable to the idea of a federal bill, if only to displace the stricter GDPR-like rules of the CCPA.[163] All of the federal bills are still in early stages of consideration and would face concentrated opposition in both houses of Congress before becoming law.[164] Should a scheme acceptable to US industry be enacted, it is unlikely it would be stringent enough to meet the EU definition of adequacy.[165] Even the CCPA itself, which represents the vanguard of general US privacy legislation, is narrow in some respects. It is a consumer protection statute that governs only large businesses and those holding large amounts of consumer data of the residents of one state.[166] It allows the transfer and sale, even of sensitive data, to third parties for any purpose unless consumers affirmatively 'opt-out'.[167] The CCPA also permits differential pricing and services to be offered to consumers who opt-out, unlike the GDPR, so long as the difference is 'reasonably related to the value to the business provided to the business by the consumer's data'.[168] In contrast, one sector of the USA, healthcare, already obeys comprehensive GDPR-like rules. A limited healthcare adequacy ruling could provide an end-run around the US legislative logjam.

In addition to being procedurally easier to achieve, a privacy regime tailored to healthcare data is likely to be superior substantively at responding to new challenges and legal gray areas specific to the sector. The era of 'big data' and the use of large datasets to train algorithms to tailor products and services creates regulatory challenges throughout the economy. However, regulatory responses arguably should differ between retailers and hospitals because the public benefit calculus between research enabling personalized medicine, for example, is different than the calculus underlying the development of personalized advertising. Health-specific gray areas, such as whether initial consent for research allows for use of personal health information in new and unanticipated projects, or how to measure whether a patient dataset has truly been anonymized, are easier to solve when the context is limited to the already highly regulated health sector. The hardest cases, which surround tracking by unregulated internet platforms, device companies, and online retailers, can be left for further negotiation without interrupting research and development for human health. International bodies already exist to coordinate harmonized approaches to health challenges and regularly

161 California Consumer Privacy Act of 2018 (CCPA), Cal. Civ. Code §§ 1798.100–1798.199

162 See, e.g., Issie Lapowsky, Tech Lobbyists Push to Defang California's Landmark Privacy Law, WIRED 4/29/2019 available at https://www.wired.com/story/california-privacy-law-tech-lobby-bills-weaken/ (last visited Dec. 16, 2019).

163 See, e.g. David McCabe, Congress and Trump Agreed They Want a National Privacy Law. It Is Nowhere in Sight. NY Times (Oct. 1, 2019) (reporting that industry groups flooded Washington urging Congress to pass a national privacy law to supersede and neutralize any state legislation on the issue).

164 Muze Fazlioglu, Tracking the politics of US privacy legislation, Intl. Assoc. of Privacy Practitioners (Dec. 13, 2019) available at https://iapp.org/news/a/tracking-the-politics-of-federal-us-privacy-legislation/ (last visited Dec. 16, 2019).

165 E.g. McCabe supra note 164 (noting lack of consensus over a right for consumers to bring an action for violations, which has been considered an important safeguard in EU adequacy determinations).

166 CCPA § 1798.140(c).120. The CCPA also specifically excludes health data covered by HIPAA and similar state laws from its scope. CCPA § 1798.145(c).

167 CCPA § 1798.120.

168 CCPA §§ 1798.120 & 1798.125.

issue guidance for global health regulators.[169] A sector-specific privacy regime can more quickly adapt such guidance without drawing opposition from other, unrelated sectors of the economy.

Finally, a sector-specific approach offers a useful model for other regions that hope to collaborate with the EU on healthcare and medical research but who may have different regulatory priorities regarding the balance between safeguarding privacy and promoting economic and technological development.[170] India is an example of a country with a thriving cloud-computing sector that may wish to provide data management services to healthcare providers in the EU and the USA.[171] It also has a different historical approach to individual rights, and, as a developing economy, may have different priorities with respect to the balance between privacy and economic development.[172] Many developing economies may not want to allocate resources to policing data privacy, nor would their existing law enforcement sectors be well-suited to such a task.[173] A limited sector-specific approach to data protection can promote important international harmonization in healthcare, a field where harmonization is urgently needed,[174] while still allowing developing economies to pursue comprehensive regulatory reform at their own pace.[175]

B. Is HIPAA Adequate Under the GDPR?

1. The Adequacy Test

For the level of protection in a third country to be considered adequate under the GDPR, it must offer guarantees to the data subject 'essentially equivalent' to those offered in the EU.[176] The means of protection, however may differ from that in the EU, so long as they prove as effective in practice.[177] The objective is not to mirror point by

169 See, e.g., David Birnbaum et al., Revisiting public health informatics: patient privacy concerns, 23 Int'l J. Health Governance 149, 150 (2018) (noting the role of the World Health Organization in establishing internationally harmonized conceptual framework for healthcare information systems generally); Menno Mostert et al., Big Data in medical research and EU data protection law: challenges to the consent or anonymise approach, 24 Eur. J. Hum. Genetics 956, 959 (2016) (noting that initiatives within the medical research community to coordinate the development of harmonised approaches to research and privacy concerns are vital); Staunton et al., supra note 131 at 1159.

170 See Mattoo & Meltzer, supra note 39 at 5 (noting that countries differ in how much they value public services and economic activity that erode individual privacy).

171 Id. at 14.

172 Id. at 5, 14–15

173 See, e.g., Alex Boniface Makulilo, Data Protection Regimes in Africa: too far from the European 'adequacy' standard? 3 Int. Data Privacy L. 42, 48 (2013) (noting the concerns of the EU evaluator judging the adequacy of the Tunisian privacy regime that the Tunisian data protection authorities were not sufficiently independent from the regular police agencies.).

174 Birnbaum, supra note 170 at 152.

175 Cf. Stoddart et al., supra note 30 at 151 (noting that holding everyone to GDPR gold-standard is problematic for legal pluralism, developing countries, and legal innovation).

176 GDPR rec. 104; Schrems I supra note 3 at ¶ 73 (holding that "while the term 'adequate' cannot require a third country to ensure a level of protection identical to that guaranteed in the EU legal order, ... [it still] must be understood as requiring the third country in fact to ensure, by reason of its domestic law or its international commitments, a level of protection of fundamental rights and freedoms that is essentially equivalent to that guaranteed within the European Union by virtue of Directive 95/46 read in the light of the Charter [of Fundamental Rights of the European Union].")

177 Schrems I, supra note 3 at ¶ 74.

point the European legislation, but to establish the essential core requirements of that legislation.[178]

This inquiry has a substantive and procedural component.[179] The EC evaluates the text of rules applicable to personal data transferred to a third country or an international organization, and also the system in place to ensure the effectiveness of such rules.[180] Beyond the data protection regime itself, the EC also considers contextual factors such as the rule of law, respect for human rights and fundamental freedoms, relevant legislation, the existence and effective functioning of one or more independent supervisory authorities, and the international commitments the third country or international organization has entered into.[181] Since 1995, only 12 countries have been found adequate under this standard.

Although this may seem a high bar, the EC has been willing to apply the adequacy standard in a flexible and pragmatic manner.[182] In 2003, the EC found Argentina to have an adequate level of protection even though its data protection law was brand new, and its DPA was not yet in existence.[183] To observers, the finding seemed a reward to Argentina for enacting a comprehensive EU-style data protection law when such regimes were relatively rare, especially in Latin America.[184] Similar pragmatic considerations may have influenced the recent adequacy decision for Japan, which was able to obtain a coveted adequacy determination based on promises of future enforcement notwithstanding a largely symbolic track record in fact.[185] A respected third country in a strategically important region willing to enter into a 'privacy dialogue' with the EU is likely to find a receptive collaborator.[186]

Also important to the EC in measuring adequacy has been the significance of a trading partner, both commercially and in terms of geographic or cultural ties to the EU.[187] The history of the development of the Safe Harbor and the Privacy Shield programs with the USA, the EU's largest trading partner, shows the EU bending over backward to find a way to preserve data flows with the USA, while gaining just enough

178 Article 29 Data Protection Working Party, Adequacy Referential (updated), WP 254 at 2 (6 Feb. 2018) https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614108.

179 Id. at 3.

180 Id. at 3.

181 GDPR Art. 45(2).

182 See Schwartz, supra note 124 at 786.

183 Commission Decision of 30 June 2003 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data in Argentina (2003/490/EC) at P14 (noting that a data protection authority had only just been constituted).

184 Schwartz, supra note 124 at 806; European Commission Memo/17/15, Digital Single Market – Communication on Exchanging and Protecting Personal Data in a Globalised World Questions and Answers (Jan. 10, 2017), http://europa.eu/rapid/press-release_MEMO-17-15_en.htm; see also Stoddart et al. supra note 30 at 147 .

185 Graham Greenleaf, Japan's Proposed EU Adequacy Assessment: Substantive Issues and Procedural Hurdles, 154 Privacy Laws & Bus. Int'l Report 1, 10 (2018), http://www.austlii.edu.au/au/journals/UNSWLRS/2018/53.html.

186 Schwartz, supra note 124 at 806-07; European Commission Memo/17/15, Digital Single Market – Communication on Exchanging and Protecting Personal Data in a Globalised World Questions and Answers (Jan. 10, 2017) (noting EU's willingness to pursue a 'dialogue on adequacy' with pioneer countries), http://europa.eu/rapid/press-release_MEMO-17-15_en.htm.

187 European Commission Memo/17/15, supra note 187.

commitments to appease lawmakers at home.[188] Similar motivations helped push the adequacy evaluations of Canada and New Zealand over the line even though investigators found some flaws in both regimes.[189] Where a third country has significant commercial and cultural ties to the EU, these considerations can outweigh a few gaps in the data protection template.[190]

The EDPB, formerly known as the WP 29, has explicitly noted in its guidance on adequacy determinations that, for some countries, a sector-based finding of adequacy will be sufficient. The EDPB recognized that requiring blanket GDPR-like coverage in every case risked discriminating against divergent legal systems and so violating international trade rules.[191] For example, nations with a federalist constitutional system have limited authority to impose uniform standards. For this reason the EDPB has cautioned that 'a positive finding on adequacy should not in principle be limited to countries having horizontal data protection laws, but should also cover specific sectors within countries where data protection is adequate, even though in other sectors the same country's protection may be less than adequate'.[192] The same report singled out the USA as a jurisdiction where a sector-based enquiry might be suitable.[193]

2. HIPAA Is Adequate

Based on this guidance, HIPAA has a chance of earning an adequacy determination because it contains the core requirements of the GDPR. The Privacy Rule is comprehensive in substance. As noted above, it is largely on all fours with the GDPR with respect to use and disclosure of sensitive health data. With respect to the fundamental privacy principles under GDPR Article 5, HIPAA can be said to embody the principles of lawfulness, transparency,[194] purpose limitation,[195] data minimization,[196] accuracy,[197] security[198], confidentiality, and accountability.[199] Although the US lacks an independent data enforcement agency generally, the HIPAA Privacy Rule is enforced by an independent office, the Office of Civil Rights (OCR), within the Department of Health and Human Services. Comprehensive administrative and judi-

188 Schwartz, supra note 124 at 804–05.

189 Paul Roth, Adequate level of data protection' in third countries post-Schrems and under the General Data Protection Regulation, 25 J.L. Inf. & Sci. 49, 61 (2017); Stoddart et al. supra note 30 at 147–49.

190 Roth, supra note 190 at 60.

191 Working Party on the Protection of Individuals with regard to the Processing of Personal Data, Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive WP 12 DG XV D/5025/98 (Adopted by the Working Party on 24 Jul 1998) at 26.

192 Id. at 27.

193 Id. at 26.

194 45 C.F.R. § 164.510 (2016) (permitting certain uses of information after notice and consent by patients); § 164.508(a)(1) (requiring written patient authorization for certain uses); § 164.508(c)(2) (regulating information disclosure to patients); § 164.524 (right of access), §164.526(a)(1) (right of rectification).

195 Id. at §§ 164.502-164.514 (permitted bases for use of health data).

196 Id. at §§ 164.502(b) and 164.514 (d) (A covered entity must make reasonable efforts to use, disclose, and request only the minimum amount of protected health information needed to accomplish the intended purpose.)

197 Id. at §§ 164.524 & 164.526(a)(1) (rights to access and rectification).

198 Security Standards for the Protection of Electronic Protected Health Information, 45 C.F.R. § 164.306(a) et. seq.

199 Pub. L. 104-191; 42 U.S.C. §1320d-5, §1320d-6 (setting out civil and criminal penalties for non-compliance).

cial remedies, including monetary penalties, are available in the event of a breach.[200] The OCR has an established and extensive track record of investigating and resolving privacy-related complaints and issues. In contrast to FTC enforcement actions under the Safe Harbor, which totaled 11 cases in its first 13 years and only 39 overall,[201] OCR investigates and resolves tens of thousands of complaints every year.[202] It also conducts proactive audits of covered entities and their business associates to ensure compliance.[203] In 2009, the OCR's enforcement authority was extended directly to reach 'business associates' who provide services to covered entities.[204] Enforcement at the federal level is complemented by state laws protecting against discrimination based on genetic data.[205]

A finding of adequacy is also more likely because the exchange of health data between US and EU entities is commercially and culturally important to both regions. Together the USA and the UK spend more on healthcare research and development than all of the other OECD nations combined.[206] The USA and its research institutions are members of and comply with all of the major international bodies and conventions surrounding ethics and good clinical practice in healthcare and research.[207] Cooperation specific to research and care therefore poses minimal risk to EU patients. Greater global harmonization in healthcare information is a priority and need not wait for harmonization of practices across all industries.

To be sure, the EU is likely to require some alterations. HIPAA's Privacy Rule is nearly 20 years old and needs updating.[208] The EC is likely to require a private right of action for individual data subjects, at least those from the EU.[209] It may also seek greater

200 45 C.F.R. §§ 160.304-404; Office of Civil Rights, Department of Health and Human Services Health Information Privacy: Enforcement Highlights, https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/data/enforcement-highlights/index.html (visited Feb. 25, 2020).

201 Anna Myers, FTC Enforcement of The U.S.-EU Safe Harbor Framework 5, https://iapp.org/media/pdf/resource_center/IAPP_FTC_SH-enforcement.pdf

202 Office of Civil Rights, Department of Health and Human Services Health Information Privacy: Enforcement Results by Year, https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/data/enforcement-results-by-year/index.html (visited Feb. 26, 2020).

203 Office of Civil Rights, Department of Health and Human Services, Health Information Privacy, HIPAA Privacy, Security, and Breach Notification Audit Program, https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/index.html (visited Feb. 26, 2020).

204 Health Information Technology for Economic and Clinical Health Act, § 13401, 123 Stat. at 260; see also 78 FR 5566 (Jan. 25, 2013).

205 Ellen Wright Clayton et al., The law of genetic privacy: applications, implications, and limitations, J. L. Biosci. 1, 12–13 (2019).

206 See Association of the British Pharmaceutical Industry, Global public funding of health R&D, https://www.abpi.org.uk/facts-and-figures/science-and-innovation/global-public-funding-of-health-rd/ (last visited Feb. 26, 2020) (collecting statistics through 2017 from the OECD STAN database (Science, Technology and Patents)).

207 E.g. Organization for Economic Co-operation and Development, The OECD Privacy Framework (2013) 'Guidelines Governing the Protection of Privacy and Trans-border Data Flows of Personal Data', available at http://www.oecd.org/internet/ieconomy/privacy-guidelines.htm (accessed 19 Dec. 2019); see also 4th International Conference on Harmonisation of Technical Requirements for Registration of Pharmaceuticals for Human Use, ICH Harmonised Tripartite Guideline, 'Guideline for Good Clinical Practice E6 (R1)', 10 Jun. 1996, available at: <http://apps.who.int/medicinedocs/documents/s22154en/s22154en.pdf>.

208 See, e.g., I. Glenn Cohen & Michelle M. Mello, Big Data, Big Tech, and Protecting Patient Privacy, 322 JAMA 1141, 1141 (2019) ("HIPAA is a 20th-century statute ill equipped to address 21st-century data practices.").

209 WP 254, supra note 179 at 8.

commitments on onward transfer by business associates.[210] As discussed in Part IV.C below, more rigorous definitions of consent for further use may be required.

The EC's adequacy determination for Canada, which is limited to commercial sector data processing, provides an indication for how the EC might approach the complications of a sector-specific adequacy ruling. In the Canadian case the relevant data protection legislation applied initially only to private sector organizations regulated by the federal government and was scheduled to come into broader effect in three stages.[211] There was some complexity around health data as well as the interplay of the Canadian legislation and laws enacted by specific provinces that might supersede the federal law. Rather than demand that all of the potential inconsistencies be resolved, the EDPB Opinion for Canada noted approvingly the establishment of federal working groups tasked with pursuing harmonization across federal, provincial, and territorial governments and public and private sector organizations.[212] This approach suggests that the EDPB and the EC are comfortable with sector-specific adequacy determinations so long as competent and effective domestic agencies are available to address inconsistencies and boundary issues. Within the USA, the relevant agency could be the Department of Health and Human Services, the FTC, a combination of both, or a specialized body empowered to bring together public and private stakeholders to achieve consensus. The EC could monitor ongoing compliance, as with every adequacy determination, under Article 45 of the GDPR.

3. Clarification and Improvement of HIPAA and GDPR for Health Data

A virtue of a sustained dialog between the USA and the EU on health data privacy is that the two regions could clarify several gray areas under both HIPAA and the GDPR. For example, the GDPR has generous exceptions from consent and withdrawal requirements for research; however it is not clear to what extent commercial entities may rely on these exceptions when they conduct healthcare research.[213] Similarly, under HIPAA, covered entities are permitted to provide data to business associates for 'data aggregation' and analysis.[214] It is not clear though whether such analysis has to be related to the services provided to the covered entity or if the business associate may

210 See Kevin Coy & Neil Hoffman PhD, Big Data Analytics Under HIPAA, JDSUPRA Mar. 16, 2016 available at www.jdsupra.com/legalnews/bid-data-analytics-under-hipaa-80678 (last visited Dec. 19, 2019) (permitted onward disclosure by business associates for 'management and administration' purposes is unclear under Privacy Rule).

211 Commission Decision of 20 December 2001 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided by the Canadian Personal Information Protection and Electronic Documents Act (2002/2/EC), 2002 O.J. (L 2/13) at ¶¶ 5–7.

212 Opinion 2/2001 of the EDPB on the adequacy of the Canadian Personal Information and Electronic Documents Act — WP 39 of 26 Jan. 2001 4-6 available at http://europa.eu.int/comm/internal_market/en/media/dataprot/wpdocs/index.htm. (recommending that the EC monitor the activities of these groups and "encourage . . . initiatives that will foster coherence of rules throughout Canada").

213 GDPR recital 159 (research exception includes not only fundamental and applied research, but also privately funded research.); see also W. Nicholson Price et al., Shadow Health Records Meet New Data Privacy Laws, Science vol. 363, 448, 450 (Feb 1, 2019); Chih-Hsing Ho, Challenges of the EU General Data Protection Regulation for Biobanking and Scientific Research, 25 J.L. Inf. Sci. 84, 91, 98 (2017).

214 U.S. Department of Health & Human Services, Standards for Privacy of Individually Identifiable Health Information. Final Privacy Rule Preamble, Section 164.504(e) 65 Federal Register 82461, 82505 (Dec. 28, 2000) (codified at 45 C.F.R. 160–164).

use personal health information for their own commercial data-analytic purposes.[215] Greater clarity under both laws about the boundary between research and care in the public interest, on the one hand, and secondary commercial research that should require additional consent, on the other, would be beneficial.[216] Both regimes also exempt anonymized or 'deidentified' health data from any restrictions. A common definition of effective anonymization in health data would be welcome on both sides of the Atlantic.[217]

Further discussion could also clarify the definition of 'specific and informed consent' in the context of healthcare research. Both HIPPA and the GDPR require that data subjects receive information about how their data will be used and, if an exemption does not apply, that they consent explicitly to any such use. This standard can be difficult to apply in medical research, where personal data are expected to be available for linkage, reuse, and analysis for largely undetermined future research purposes.[218] Commentators have proposed a model of dynamic, 'broad' consent for scientific research where participants authorize unspecified future medical research uses, but researchers must seek ethics committee or some other form of representative participant committee review for each new category of use.[219] That way, the risks if reidentification or other participant harms can be considered in real time and balanced against the benefits of the new use. On the flip side, the GDPR requires a stricter standard of consent where subjects are asked to approve use of sensitive health data for purposes beside research or care. If the USA were to adopt similar safeguards around meaningful patient consent, including rights of withdrawal and erasure outside of a care or bona fide research context, this would go a long way toward quieting fears about slippage of sensitive data from the regulated health sphere into the more rapacious commercial sector.[220] Linking the two healthcare data regimes through an adequacy assessment would pave the way for common adoption of such standards.

C. Challenges With the Proposed Approach

Our recommendation for a HIPAA Shield is based two assumptions: (i) that the USA is not poised to pass comprehensive data protection legislation in the near term and (ii) that the US medical establishment will remain committed to following international norms of patient confidentiality and ethical practice. Given the wide divergence between the EU and the USA on how to approach data privacy in most fields, but the substantial convergence as to information governance in the healthcare field, we think that a HIPAA based Shield offers the easiest and most promising way forward.

---

215 Coy & Hoffman, supra note 211.

216 For discussion of how such a definition might be achieved, see infra text accompanying notes 228231.

217 See, e.g., Minssen, supra note 8 at 4546.

218 GDPR Recital 33 ("It is often not possible to fully identify the purposes of personal data processing for scientific research purposes at the time of data collection"); Mostert et al, supra note 170 at 2.

219 Ho, supra note 214 at 93; Minssen et al., supra note 10 at 17; Cohen & Mello, supra note 209 at 1142; Melanie Bourassa Forcier, et al., Integrating Artificial Intelligence into health care through data access: can the GDPR act as a beacon for policymakers? J. L. Biosci. 317, 329 (2019).

220 See BBC News, Project Nightingale: Google accesses trove of US patient data, https://www.bbc.co.uk/news/technology-50388464; Natasha Singer, When Apps Get Your Medical Data, Your Privacy May Go With It, NY Times Sept. 3 2019.

A potential weakness of a HIPAA Shield is that the same concerns about US government surveillance that underlie the cases against the Privacy Shield could also sink a HIPAA Shield. The Snowden revelations concerned a program called Prism that allowed the government to track online communications between US citizens and foreign nationals.[221] At present, there have not been credible reports of a similar widespread data collection program for surveillance of healthcare records. However, electronic health records are certainly exchanged electronically and so could be subject to US government surveillance through the existing programs. These records are not likely to be of much use for national security priorities at present, but as technologies develop and surveillance methods evolve, it is possible that health data held by providers and researchers could become useful for such purposes. If EU controllers have reason to believe that these data are likely to surveilled inappropriately by US government authorities, the AG Opinion in *Schrems II* has suggested that they must refuse the transfer notwithstanding the presence of a shield or other general legal basis.[222]

A more immediate drawback to a sector-specific regime is that it would only apply to certain custodians of information. Much information concerning health is collected by companies and actors outside the healthcare field, through apps, wearables, and search requests and posts on social media.[223] The GDPR protects the fundamental rights of the data subject no matter who holds or processes the data. The US system places no restriction on actors outside the health sector using such information to track, monitor, and advertise to individuals based on intimate health details.[224] This kind of information may even lead to discrimination in employment or insurance if businesses can easily reidentify subjects.[225] Perhaps even more worrisome, the current US administration in the process of proposing new rules that would require health care providers to send full electronic medical records to third party apps after a patient has authorized the exchange.[226] Patients may provide consent to such transfers without fully understanding that once the records leave the care of an entity covered by HIPAA, the information therein can be used for any purpose whatsoever.[227] A comprehensive rule like the GDPR that applies to all custodians of sensitive personal information, rather than to only certain kinds of processors, is more protective. This is true but not yet attainable in the USA. A Shield based on an enhanced version of HIPAA would be an incremental first step toward more comprehensive rights for individuals and details

221 Schrems I, supra note 3 at ¶¶ 14–15, 22, 28, 30.

222 Opinion of the Advocate General, supra note 47 at ¶¶ 128–139.

223 See Cohen & Mello, supra note 140 at 232; Price et al., supra note 214 at 449.

224 The CCPA places some limits on sale or transfer of such data, including inferences drawn from the data. CCPA, at § 1798.140 (o)(1)(K). However, as noted, the consumer must affirmatively 'opt-out' of third-party sale and collection. If a HIPAA Shield were adopted, it could strengthen consent protections to require affirmative, specific and informed consent for follow-on use. It could also go beyond the GDPR to include inferential data, as defined by the CCPA, as part of protected health care information that cannot be processed without a lawful basis.

225 See Singer, supra note 221.

226 Center for Medicare and Medicaid Services, Trump Administration Announces MyHealthEData Initiative to Put Patients at the Center of the US Healthcare System, (Mar. 6, 2018) https://www.cms.gov/newsroom/press-releases/trump-administration-announces-myhealthedata-initiative-put-patients-center-us-healthcare-system (visited Feb. 27, 2020).

227 See Singer, supra note 221.

about their health. As part of the adequacy process, the EC can require that enhanced standards of consent apply to any patient authorization to disclose medical record data.

Some have proposed that medical charities and data protection bodies in Europe craft an overarching code of conduct or certification scheme under Article 40 of the GDPR that is specific to using personal data, including genetic and biometric data, in medical research.[228] We support this idea, which has the benefit of linking protection to the type of data and use, rather than the type of organization undertaking the processing. However, precisely because of the diversity of parties, interests and uses that must be covered, drafting and implementing such a code may be difficult. The Biobanking and BioMolecular Resources Research Infrastructure-European Research Infrastructure Consortium has been working on such a code just for Europe since 2017 but has yet to release a draft.[229] Even if such a Code were approved, other regions may object to following a Code monitored and overseen by a European supervisory authority.[230] An 'adequacy' approach that builds off existing law in each region may be politically easier to achieve. An optional code of conduct, developed among and between an appropriately representative group of stakeholders, could then sit alongside sector-specific rules and provide guidance as to when onward transfers of medical data from primary caregivers or research studies might be appropriate.

V. CONCLUSION

International transfers of personal health data from the EU to the USA are vital for continued innovation in public health and biomedicine. Uncertainty about the application of the GDPR is threatening to unravel decades of productive research collaborations and networks of international expertise. Researchers and patients on both sides of the Atlantic require rules that protect the fundamental rights of individuals although also allowing research on treatments and therapeutics to move forward as swiftly as possible.

The US–EU Privacy Shield cannot facilitate international transfers of medical data. It is neither fully adequate under EU law, nor democratically legitimate under the US legal system. Its scope is too narrow to allow for the kinds of frequent, large-scale research transfers of medical data required for innovation in drug discovery, personalized medicine, and new uses of AI in medical devices.

A HIPAA shield could offer a better approach that is tailored to use of data in research and is simple to achieve in the near term. A comprehensive data protection regime for the entire USA is still years away. Building upon existing law in an area where US and EU values fundamentally align is a pragmatic approach that sidesteps the most contentious issues although advancing important public policy aims.

---

228 See, e.g., Mitchell et al. supra note 41 at 3, 20; Phillips, supra note 8 at 33 ("An international code of conduct could help investigators to overcome some of the current hurdles, as well as others that might arise as legislation on data protection evolves.").

229 A Code of Conduct for Health Research, http://code-of-conduct-for-health-research.eu, (visited Feb. 27, 2020); BBMRI-ERIC, Code of Conduct for Using Personal Data in Health Research, http://www.bbmri-eric.eu/news-events/code-of-conduct-for-using-personal-data-in-health-research/ (visited Feb. 27, 2020).

230 EDPB Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679 at p. available at pp. 19-24 https://edpb.europa.eu/sites/edpb/files/consultation/edpb20190219_guidelines_coc_public_consultation_version_en.pdf (last visited Jan. 31, 2020).

ACKNOWLEDGMENTS

The authors thank anonymous reviewers for their helpful comments. The authors acknowledge the support by the Novo Nordisk Foundation for the scientifically independent Collaborative Research Program for Biomedical Innovation Law (grant NNF17SA0027784).