Journal of Law and the Biosciences, lsae022
https://doi.org/10.1093/jlb/lsae022
Essay

OXFORD

The new EU–US data protection framework's implications for healthcare

Charlotte Tschider[1], Marcelo Corrales Compagnucci[2] and Timo Minssen[2]

[1]Beazley Institute for Health Law and Policy, Loyola University Chicago School of Law, 25 E. Pearson Street, Chicago, Il 60611 USA
[2]Centre for Advanced Studies in Bioscience Innovation Law, University of Copenhagen, Karen Blixens Plads 16, DK-2300 Copenhagen S
*Corresponding author. E-mail: ctschider@luc.edu

ABSTRACT

In July 2023, the United States and the European Union introduced the Data Privacy Framework (DPF), introducing the third generation of cross-border data transfer agreements constituting adequacy with respect to personal data transfers under the General Data Protection Regulation (GDPR) between the European Union (EU) and the US. This framework may be used in cross-border healthcare and research relationships, which are highly desirable and increasingly essential to innovative health technology development and health services deployment. A reliable model meeting EU adequacy requirements could enhance the transfer of patient and research participant data. While the DPF might present a familiar terrain for US organizations, it also brings unique challenges. A notable concern is the ability of individual EU Member States to establish individual and additional requirements for health data that are more restrictive than GDPR requirements, which are not anticipated by the DPF. This article highlights the DPF's potential impact on the healthcare and research sectors, finding that the DPF may not provide the degree of lawful health data transfer desirable for healthcare entities. We examine the DPF against a background of existing Health Insurance Portability and Accountability Act obligations and other GDPR transfer tools to offer alternatives that can improve the likelihood of reliable, lawful health data transfer between the US and EU.

KEYWORDS: privacy law, data protection, data sharing, international collaboration, medical research

I. INTRODUCTION

Health professionals, such as physicians, medical researchers, and support staff, often collect sensitive personal data like health data. This data predominantly includes health

information from patients and research participants, a group that is increasingly becoming more diverse, with many individuals residing outside the United States.[1] This trend, exacerbated by the rapid advancement of artificial intelligence (AI) in healthcare, underscores the expanding scope of data collection in global healthcare and research contexts. The integration of AI simultaneously fuels a growing need for data optimization in research while needing access to larger and more diverse datasets. These datasets are essential for accurately representing various populations and geographical regions.[2] Consequently, there is a significant uptick in data transfers from the European Union (EU) to the US, catering to a range of purposes including research collaborations, clinical trials, obtaining second opinions, coordinating treatment, and using technological resources and services. This evolution illustrates that the future of healthcare and medical research is inherently global, driven by technological advancements and the need for extensive, varied data.

Due to legal challenges associated with transferring personal information (US) and personal data (EU) between the US and EU countries, many research institutions have been hesitant to engage in collaborative research, despite its potential benefits. These legal constraints have affected a wide range of organizations and sectors, especially those providing services that require the transfer of personal data from the EU to the US. Even more, many US organizations have not sought independent compliance with the EU General Data Protection Regulation (GDPR).[3] Instead, they have relied on the US Privacy Shield, an agreement constituting adequacy between the US and the EU that has recently been invalidated. To remedy these legal limitations, the European Commission (EC) adopted the third version of an EU–US Data Privacy Framework (DPF) in July 2023.[4] This framework is designed to reasonably align US data protection standards with specific EU requirements, while ensuring US access to data for intelligence purposes.[5]

II. THE DPF'S FRAUGHT HISTORY

Due to differing legal requirements between the US and EU, it became necessary for both parties to establish an agreement that would qualify for adequacy, legally permitting the transfer of data from the EU to the US. Fundamentally, both the GDPR

1 Timo Minssen & Sarah Gerke, *Ethical and Legal Challenges of Digital Medicine in Pandemics*, in Pandemics and Ethics 165–67 (Andreas Reis et al. ed., 2023), https://doi.org/10.1007/978-3-662-66872-6_12

2 Charlotte Tschider, *Prescribing Exploitation*, 82 Md. L. Rev. 857, 861 (2023), https://digitalcommons.law.umaryland.edu/cgi/viewcontent.cgi?article=3967&context=mlr

3 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protectionof natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC [2016] OJ L119/1 (General Data Protection Regulation, GDPR).

4 European Commission, *Data Protection: European Commission adopts new adequacy decision for safe and trusted EU-US data flows,* European Commission Press Release (July 10, 2023), https://ec.europa.eu/commission/presscorner/detail/en/ip_23_3721.

5 *Id.* Although the *Schrems III* decision created the impetus for the Safe Harbor Agreement and focused specifically on intelligence access to EU personal data, the US naturally sought to reinforce its previous law enforcement access. For example, the press release specifically retained access to what is 'necessary and proportionate.' It may be that other motivations beyond addressing its invalidation that existed for the EU and US, but interrogation of these motivations is beyond the scope of this article.

and its predecessor, the Data Protection Directive,[6] required 'an adequate level of protection' in any receiving country as a basis for international data transfer.[7] The DPF and its predecessors aimed to achieve this adequate level of protection through legally enforceable instrument, a treaty between the US and the EU, deemed an 'agreement,' which is used as the basis for adequacy determined by the EC. However, achieving this level of protection has largely been a moving target over the past 13 years, marked by the passage and invalidation of various transfer agreements' adequacy status.[8]

The evolution of data protection in the EU and US, respectively, can be traced back to the same legal origin with markedly different results. These differing models of data protection created a need for some agreement to establish adequacy and enable cross-border data flows that have become necessary with the rapid evolution of computing and the internet in business relationships. In 1968, the broad principles for data protection worldwide were established at the United Nations International Conference on Human Rights, of which EU Member States and the US were signatories.[9] Since that time, the US and the EU have adopted various privacy and data protection laws. In 1970, Germany's Hesse state passed its own data protection measures, broadly regulating personal data use, which was expanded to the country in 1978.[10] Around that same time, the US passed the Privacy Act, restricting the use of personal information by government entities. In the 1990s, the EU passed its landmark directive, the Data Protection Directive, which required each EU member state to adopt their own version of the Directive.[11] Due to its status as a 'directive,' states could alter the details of the Directive when passed locally. The Data Protection Directive incorporated principles developed as part of the Organization for Economic Cooperation and Development (OECD) Guidelines in 1980 and applied to commercial and government data processing.[12]

Around the same time as the Directive, the US passed laws regulating commercial entities: the Gramm-Leach Bliley Act, governing financial institutions and associated transactions, and the Health Insurance Portability and Accountability Act (HIPAA), governing largely healthcare insurance transactions involving healthcare providers.[13]

6 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection ofindividuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L281/31.

7 *See* GDPR, *supra* note 3, Art. 2(1); Paul M. Schwartz & Karl-Nikolaus Peifer, *Transatlantic Data Privacy*, 106 Geo. L.J. 115, 158 (2017).

8 See, e.g., generally, Timo Minssen et al., *The EU-US Privacy Shield Regime for Cross-Border Transfers of Personal Data under the GDPR: What are the legal challenges and how might these affect cloud-based technologies, big data, and AI in the medical sector?*, 4(1) Eur. Pharma. L. Rev. 34 (2020), https://doi.org/10.21552/eplr/2020/1/6

9 Fred H. Cate, *EU Data Protection Directive, Information Privacy, and the Public Interest,* 80 Iowa L. Rev. 431, 431 (1995); Joel R. Reidenberg, *The Privacy Obstacle Course: Hurdling Barriers to Transnational Financial Services*, 60 Fordham L. Rev. S137, S143–48 (1992).

10 Julius Feldmann & Olga Stepanova, *In a nutshell: data protection, privacy and cybersecurity in Germany*, Lexology (Oct. 22, 2020), https://www.lexology.com/library/detail.aspx?g=c9f86639-8e64-433f-b1d7-bee9430eaa50.

11 Charlotte A. Tschider, International Cybersecurity and Privacy Law in Practice (2d Ed. 2023); *See* Cate, *supra* note 9, at 433.

12 Organization for Economic Cooperation and Development, *OECD Guidelines on the Protection of Privacy and Transborder Flows on Personal Data* (Sept. 23, 1980), https://doi.org/10.1787/9789264196391-en.

13 *See* Tschider, *supra* note 11, at 106, 111.

These laws were not written to address privacy as such; they were drafted to regulate against harmful business practices impacting financial services consumers and insurance beneficiaries. Although adopted in 1996, HIPAA would not include any specific privacy, security, or data breach notification rules until the early 2000s.[14]

These two approaches illustrated a generalized divide between the US and the EU: the so-called 'sectoral' approach in the US regulating sectors of risky behavior first, and the EU establishing a foundation of expected behavior across industry and government, the 'omnibus' approach. The expansion of the internet into e-commerce activities in the late 1990s and a desire to transfer data across borders created a need to bridge two different geographical, social, and legal privacy and data protection regimes. The Safe Harbor Agreement, established following the EU's Data Protection Directive, attempted to create a model for data transfers between EU countries and the US, which did not have a compatible or comparable omnibus federal law.[15]

The Data Protection Directive's Article 36 permitted data transfer under limited circumstances to 'third countries' with an adequate degree of protection outside of the EU.[16] This required the EC to determine adequacy status for third countries, which involved a lengthy process of countries applying for adequacy and review of each country's data protection laws. The Safe Harbor Agreement, a self-certification program that qualified companies in the US (a country that would not holistically qualify for adequacy) for adequacy status, served as a bridge, a treaty designed to effectively facilitate trade between the EU and the US.[17] The Safe Harbor Agreement achieved a balance between two distinct approaches to privacy and data protection through a largely self-certification model.[18]

The Safe Harbor was designed for broad, omnibus use, and it was not specifically focused on healthcare data transfer. HIPAA, however, created fairly rigorous obligations for healthcare providers, clearinghouses, and health plans in the US. Despite the differences between a narrowly applied, sector-specific HIPAA and the broad Data Protection Directive, there were marked similarities in their details. For example, the regulated entities' relationships under HIPAA and the Data Protection Directive mirrored each other, with covered entities and business associates under HIPAA and controllers and processors under the Data Protection Directive. Covered entities and controllers determine the purpose and use of protected health information or personal data, respectively, while business associates and processors follow the direction of the former.[19] Perhaps the EU and US' failure to define a data-sharing model specifically

14 *Id.*, at 106.

15 *See supra* note 7, at 158.

16 Directive 95/46/EC Art. 36 [2016] OJ L119/1.

17 *Id.* The US Department of Commerce's recent involvement is a result of their original framing of this treaty as a question of trade.

18 *Id.*, at 159. *See also*, Marcelo Corrales Compagnucci et al., *Cross-Border Transfers of Personal Data after Schrems II: Supplementary Measures and New Standard Contractual Clauses (SCCs)*, 4(2) Nordic J. Eur. L. 37(2021).

19 Carter Manny, *Privacy Protection for Health Information Transferred between the European Union and the US: A Comparison of Legal Frameworks*, 36 Bus. L. J. 107, 109, 111. It should be noted that one significant difference is the breadth of scope. HIPAA notably defines covered entities as only those who are health care providers, health plans, or healthcare clearinghouses. This presumably can leave out research interests and other healthcare companies that do not fit this definition.

tailored for the health sector was a missed opportunity, given the greater similarity between HIPAA's requirements with the Data Protection Directive.[20]

Although it is unknown to what degree health organizations relied upon the Safe Harbor, policymakers at least considered the impact on researchers. This was noted in the FAQs, where it is mentioned that additional research based on previously collected data could potentially qualify as purposes not incompatible with the original purposes for processing. It also stated that third-party processing could occur following explicit consent from the individual data subject.[21] However, the Safe Harbor was not designed for health data transfer specifically.

In 2015, the Court of Justice of the European Union (CJEU) invalidated the Safe Harbor Agreement in the *Schrems I* case,[22] prompting the development of the Privacy Shield as its successor. The Snowden revelations prompted Safe Harbor's invalidation by exposing the extent of US resident surveillance, destroying its status as 'adequate.'[23] Following the invalidation of the Safe Harbor, the EU and the US almost immediately began negotiating a replacement agreement, recognizing that many organizations had already been relying on Safe Harbor for existing international transfers. The Privacy Shield was seen as an opportunity to enhance privacy protection in the US while addressing the reasons for Safe Harbor's invalidation.[24]

One key change in the Privacy Shield was the enhancement of purpose limitation and the restriction on processing personal data for incompatible purposes.[25] This requirement significantly curtailed what US organizations receiving personal data under the Privacy Shield could do, particularly limiting data reuse or processing for purposes that might solely benefit a US organization, financially or otherwise. Consistent with its predecessor, the Privacy Shield also mandated that US organizations obtain express, explicit consent for processing sensitive personal data, such as health data.[26] These two requirements, collectively, greatly restricted any additional processing or data sharing that was incompatible with the original purpose for processing, based on what was disclosed at the time of collection.[27]

Perhaps the most significant contribution of the Privacy Shield was its enforcement, redress, and liability mechanisms, where EU residents were informed of their rights and given the ability to file complaints for redress.[28] They were also granted legal avenues to pursue action against US companies failing to fulfill their obligations under the Privacy Shield. The US Federal Trade Commission (FTC) was designated as the enforcement agency for EU judgments and complaint investigations. Critically, the

20 *Id.*, at 128. Differences included a limited range of remedies in the US compared to the EU, as well as some differences in limitations in transfer to third parties contractually (in the degree of detail included in such contracts, though the Business Associate Agreement under HIPAA integrates Rule requirements by reference, similar to the detailed standard contractual clauses developed under the Data Protection Directive).

21 *See* Manny, *supra* note 19, at 125.

22 Case C-362/14, Schrems v. Data Prot. Comm'r, 2015 E.C.R. 650 (Oct. 6, 2015).

23 *See supra* note 7, at 159.

24 Paulius Jurcys et al., *The Future of International Data Transfers: Managing New Legal Risk with a 'User-Held' Data Model*, 46 Comp. L. & Sec. Rev. 105,691, https://doi.org/10.1016/j.clsr.2022.105691

25 *See supra* note 7, at 162.

26 *Id.*

27 *See* GDPR, *supra* note 3, at Art. 4(2).

28 *Id.*, at 164–65.

Privacy Shield also addressed internal changes within Congress and the Executive Branch to surveillance practices, intended to rectify the overreach highlighted by the Snowden revelations referenced in *Schrems I*.[29]

Despite substantial concessions that brought the model closer to the EU standards, the introduction of the GDPR in 2016 further widened the gap between the EU and the US in their data protection and privacy practices. Despite the reformed surveillance practices that underpinned the enactment of the Privacy Shield, it suffered the same fate as the Safe Harbor. In July 2020, the CJEU, in the *Schrems II* case,[30] invalidated the Privacy Shield on two main grounds. First, it found that US surveillance programs, as evaluated by the Commission, did not meet EU law's strict necessity and proportionality requirements, violating Article 52 of the EU Charter of Fundamental Rights (CFR). Second, the Court determined that EU data subjects lacked effective judicial remedies against US surveillance, infringing their right to redress under Article 47 of the EU CFR.

However, the Court upheld the validity of Standard Contractual Clauses (SCCs). It mandated a 'case-by-case' assessment for their application. Data controllers and processors exporting data must evaluate whether the legislation and practices of the third country undermine the efficacy of the safeguards outlined in Article 46 of the GDPR. The *Schrems II* ruling requires data exporters to implement 'supplementary measures' to address any deficiencies and ensure compliance with EU law. Unfortunately, the CJEU did not provide a clear definition or specification of supplementary measures, leading to intense debates and prompting the issuance of numerous guidelines and recommendations on implementing additional safeguards.[31]

This led to further challenges in achieving a harmonized approach to data transfer between the US and the EU.[32] For a timeline of the relevant law passages and agreement adequacy invalidations, see Exhibit 1.

The recently negotiated EU–US DPF was an agreement designed to succeed the Privacy Shield, address previous concerns, and establish adequacy. However, despite the protracted negotiations to establish Privacy Shield, it was not without complications. Following the *Schrems II* decision and invalidation of Privacy Shield as an adequate basis for cross-border transfer, the European Data Protection Board proposed guidance on cross-border data transfers, which received hundreds of comments during the public consultation.[33] These comments revealed the significant impact of additional

29 *Id.*, at 164.

30 C-311/18, *Data Protection Commissioner v. Facebook Ireland Limited, Maximilian* Schrems (*Schrems II*).

31 See, e.g., European Commission implementing decision of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council, C(2021) 3972 final; EDPB Recommendations on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data. Adopted on 10 November 2020, https://www.edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012020-measures-supplement-transfer_en (Accessed 4 July 2024).

32 Marcelo Corrales Compagnucci et al., *Lost on the High Seas without a Safe Harbor or a Shield? Navigating Cross-Border Transfer in the Phamaceutical Sector After Schrems II Invalidation of the EU-US Privacy Shield*, 4(3) European Pharma. L. Rev. 153, 155 (2020), https://doi.org/10.21552/eplr/2020/3/5; Laura Bradford et al., *Standard contractual clauses for cross-border transfers of health data after Schrems II*, 8(1) J. L. & Biosciences 1, 25 (2021), https://doi.org/10.1093/jlb/lsab007.

33 Anupam Chander & Paul Schwartz, *Privacy and/or Trade*, 90 U. Chi. L. Rev. 50, 82 (2023).

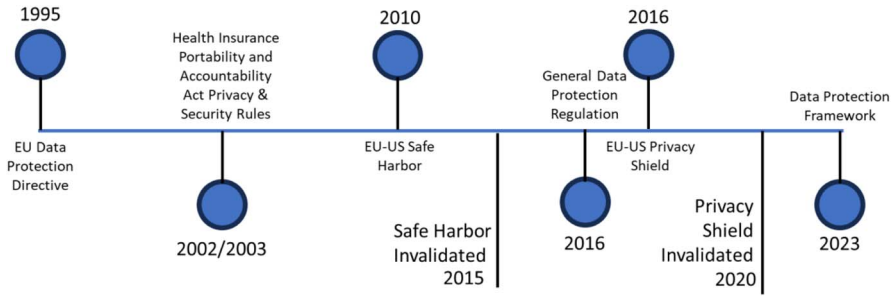

Exhibit 1. EU–US Agreement Timeline. Author-created, Author's recording of healthcare-impacting privacy agreements for US organizations

hurdles on smaller companies and European enterprises.[34] Issues raised included the complications of intercompany data transfers for international human resources, the potential isolation of Europe from the global economy, and the loss of essential technological services from US companies. Startup associations across the EU criticized the proposed rules as harmful to their growth. For instance, Belgian app developers expressed concerns about the disadvantages to small businesses, while Allied for Startups highlighted the 'additional costs' of supplementary measures required for cross-border data transfers, noting startups' limited resources. A recurring theme concerned excessive costs associated with the proposed guidelines. Danish entrepreneurs argued that the measures failed to consider the realities of startups, which cannot afford the detailed analyses and multi-jurisdictional legal advice required. Similarly, a Spanish digital industry association warned that the rules would necessitate costly evaluations of non-EU laws, an unrealistic burden for most small and medium-sized enterprises, research institutions, and others.[35]

In its response to Privacy Shield invalidation, the DPF aimed to simplify cross-border transfer by introducing additional constitutional protections for EU residents through President Biden's Executive Order.[36] This Order established additional safeguards and recourse mechanisms for signals intelligence activities, imposing binding requirements on federal agencies and significantly limiting expansive collection of personal data by US organizations.[37] It also created a Data Protection Review Court to enhance enforcement and provide direct legal recourse.[38] In large part, however,

34 *Id.*

35 *Id.*, at 82–83.

36 Exec. Order No. 14,086, 87 Fed. Reg. 62,283 (Oct. 14, 2022)

37 *Id.*; Sara Gerke & Delaram Rezaeikhonakdar, *Privacy Shield 2.0—A New Trans-Atlantic Data Privacy Framework Between the European Union and the United States*, 45 Cardozo L. Rev. 353, 375–380 (2023). As Gerke & Rezaeikhonakdar describe, several organizations are involved in the process of reviewing draft adequacy decisions under Article 45, and likely because so much of the DPF is based on US President Biden's Executive Order (which was not updated to reflect amendments recommended and adopted by these committees), there may still be Member States that are unsatisfied with the results. *Id.*, at 386, 390.

38 However, this court is part of the Executive Branch, not the Judiciary, which could mean that the independence of judges and any advocate positioned on behalf of an EU resident, could be challenged. Moreover, the results of any decisions are generally not made available to a complainant. *See* Gerke & Rezaeikhonakdar, *supra* note 37, at 398.

the DPF reinforced the other substantive aspects of the Privacy Shield that were not invalidated in the *Schrems II* decision.

III. USING THE DPF FOR HEALTHCARE RELATIONSHIPS

The DPF is designed to make the transfer of personal data between the EU and the US for healthcare relationships and health research engagements easier by establishing common legal standards that align well with GDPR requirements.[39] Ideally, under the DPF, US healthcare organizations, research institutions, and health technology companies, could collaborate with EU institutions with minimal friction. Furthermore, even for organizations not planning to receive EU patient data in the near future, the DPF provides a framework that could collectively improve organizational privacy and bolster patient or research participant trust, a critically important goal in today's increasingly interconnected healthcare environments.[40]

The DPF aims to provide a reliable foundation for transatlantic data flows and may act as a catalyst for collaborative data sharing among health professionals and researchers between the EU and the US. The DPF operates as a self-certification framework—organizations can sign up by attesting to GDPR-consistent principles after ensuring they can meet these requirements. Information required for self-certification includes contact information of data protection leaders, annual revenue, data processed and purposes for processing, details of a complaint handling and dispute resolution process, and a copy of any privacy notices used and their effective date(s).[41] Organizations must also attest to follow framework requirements (disclosure, data subject rights, management of third parties).[42]

The US Department of Commerce administers the framework, and the US FTC enforces compliance with the framework's obligations.[43] The DPF program website offers guidance materials and resources, including the DPF Principles, a self-certification submission portal, and a list of active DPF organizations.[44] While the DPF aims to facilitate broad data exchange between the two regions, it also could offer a legally enforceable method for transferring medical practice and research data involving personal data of US and European patients and research participants. Despite its highly publicized potential benefits, it remains unclear whether the DPF can be effectively used for health information transferred from certain EU countries to the US.

39 International Trade Administration, *Important Privacy Shield Program Update* (Jul. 11, 2023), https://tinyurl.com/bdz4b8mk

40 Deven McGraw et al., *Privacy as an Enabler, Not an Impediment: Building Trust into Health Information Exchange*, 28(2) Health Affairs 416, 417 (2009), https://doi.org/10.1377/hlthaff.28.2.416.

41 U.S. Dept. Commerce, *Key Requirements for DPF Program Participating Organizations,* Data Privacy Framework Program, https://www.dataprivacyframework.gov/key-requirements (last accessed: June 25, 2024).

42 *Id.*

43 International Trade Administration, *Administration of the Data Privacy Framework (DPF) Program* (2023), https://www.dataprivacyframework.gov/s/article/Administration-of-the-Data-Privacy-Framework-DPF-Program-dpf

44 International Trade Administration, *Data Privacy Framework Program* (2023), https://www.dataprivacyframework.gov/s/

IV. NAVIGATING COMPLIANCE CHALLENGES FOR CROSS-BORDER HEALTH DATA TRANSFER

Although data can be functionally transferred between organizations in different geographies easily, complying with each geography's laws, at least when personal data are involved, is comparatively difficult. One of the biggest impediments to cross-border data sharing involves differences in privacy regulations. Some regions have restricted transfer unless certain legal steps are taken, such as consent, use of contractual clauses between private entities, or adequacy of the receiving country's data protection laws.

The incompatibility of sectoral and omnibus legal frameworks complicates cross-border healthcare activities, despite somewhat similar legal frameworks. The US requires HIPAA compliance for covered entities, which is a subset of healthcare organizations including healthcare providers, healthcare clearinghouses, and health plans. In clinical research settings, while HIPAA may be applicable, most research processes are governed by the Common Rule and the direction of internal Institutional Review Boards as mandated by the US Food and Drug Administration (FDA).[45] In these settings, HIPAA operates under a somewhat more flexible framework, allowing clinical treatment to be conditioned upon execution of an authorization and permitting data sharing for limited datasets.[46] However, the US lacks a generally applicable, comprehensive, omnibus data protection law or a broad healthcare privacy law at the federal level, with such regulations existing primarily at the state level.[47]

In contrast, the EU's omnibus GDPR has a comprehensive reach, broadly binding Member States to adhere to its strict requirements with few exceptions. Compliance with the GDPR is necessary not only when collecting data directly from EU residents but also when receiving and processing data from an EU organization. In the EU context, 'processing' encompasses a range of activities, including accessing, using, exchanging, sharing, anonymizing, or simply incorporating EU personal data of any kind in datasets or for algorithmic training. If a US organization intends to process EU personal data, they must either self-certify under the DPF or fulfill an alternative legal mechanism guaranteeing an adequate level of protection under the GDPR for such transfer.

At present, the methods for establishing such an adequate level of protection under GDPR's Articles 44–50 include:[48]

1) **Adequacy Decision:** The EC determines whether a country or international organization's legal protections, or one or more specified sectors within a country, sufficiently ensures an adequate form of protection.[49] It should be noted that to date, traditional adequacy decisions are typically limited to omnibus country-level data

45 45 CFR 46 et seq.; Kate Fultz Hollis, *To Share or Not to Share: Ethical Acquisition and Use of Medical Data*, 2016 AMIA Jt. Summits Transl Sci Proc. 420 (Jul. 20, 2016), https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5001759/. Notably, additional data use beyond what is included in informed consent forms in a clinical setting can be referred to the Institutional Review Board. *See* U.S. Dep't Health & Human Svcs. NIH, *Institutional Review Boards and the HIPAA Privacy Rule* (Aug. 2003), https://privacyruleandresearch.nih.gov/irbandprivacyrule.asp.

46 45 CFR 164.508(b)(4), 164.502(a)(1).

47 Lucia Savage, *To bring Health Information Privacy Into the 21 Century, Look Beyond HIPAA*, Health Affairs Forefront (Jul 5, 2018), https://doi.org/10.1377/forefront.20180702.168974

48 *See* Corrales Compagnucci, *supra* note 18, at 37.

49 Regulation 2016/679 Art. 45.

protection legal schemes, though under Article 45, the GDPR does permit agreements based on sector or organization.[50]

2) **Appropriate Safeguards:** Transfer may occur when the receiving country or organization has provided appropriate safeguards: those that enforce data rights and effective legal remedies for data subjects.[51] These include a legally binding and enforceable instrument, binding corporate rules submitted and approved by the EC, standard data protection clauses adopted by the EC or approved by the EC combined with effective transfer impact assessments,[52] an approved certification mechanism, or an approved code of conduct combined with binding and enforceable commitments.[53] These safeguards are generally intended for organizational use when an organization exists in a country that is not deemed adequate.

3) **Derogations:** Transfer may be accomplished absent an adequacy decision or appropriate safeguards for specifically defined derogations, such as vital interest, reasons of public interest (established in member state law), under conditions of legitimate interest, following explicit consent and risk advisement, or to execute a contract of which an individual data subject is a party.[54] Derogations are generally considered less favorable transfer mechanisms, for use when the other bases for transfer are unavailable.[55] Derogations also require independent risk evaluation and documentation of suitable safeguards.[56]

Under the GDPR, data should be transferred under one of the enumerated means: adequacy or appropriate safeguards. Both of these legal mechanisms provide some assurance to data subjects that their personal data will be protected when transferred to a third country or entity and provide some enforcement mechanism consistent with the EU's approach.

V. DPF PRINCIPLES IN PRACTICE

To comply with the DPF, health professionals must adhere to principles aimed at protecting patient and research participant privacy and ensuring compliance with data protection regulations when transferring data between the US and Europe. These principles can be satisfied through an organization's overall policies and practices. The primary principles include:

- Notice
- Choice
- Accountability for Onward Transfer
- Security
- Data Integrity and Purpose Limitation

50 *Id.*
51 Regulation 2016/679 Art. 46.
52 European Data Protection Board, *Recommendations 01/2020 on measure that supplement transfer tools to ensure compliance with the EU level of protection of personal data (Version 2.0)* (June 18, 2021), https://www.edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012020-measures-supplement-transfer_en, at 13–17.
53 *Id.*; Regulation 2016/679 Art. 47.
54 Regulation 2016/679 Art. 49.
55 *Id.*
56 *Id.*

- Access
- Recourse, Enforcement and Liability[57]

The data integrity and purpose limitation principle mandates that the collection and use of personal data, especially sensitive health data, should be limited to specific, explicit, and legitimate purposes. Should there be a need to use the data for additional activities, obtaining patient consent for these secondary uses may be necessary. Moreover, it is crucial to limit the collection of personal data to what is necessary for these purposes, especially when dealing with identifiable health data ('data minimization').

Health professionals should also update their 'privacy notices', including any language related to privacy in research participation disclosures. These notices must clearly describe how patient or research participant personal data will be used. Additionally, they should specify the rights that patients or research participants have, as well as the procedures for filing a complaint with both the organization and an EU data protection authority if an individual is concerned their information is not being appropriately collected, used, or processed. US organizations required to comply with HIPAA should either update their Notice of Privacy Practices or create an alternative notice specific to EU patients. Similarly, US researchers who aim to leverage EU research participant data should also create a privacy notice for EU research partners. These policies are essential for informing patients about an organization's data protection practices.

Organizations are also advised to create a 'data subject rights' request process, empowering patients to exert control over the handling of their data and require organizations to respond within a specified and mandatory timeframe. These requests may cover various actions, such as accessing and correcting records, transferring requested data, deleting data, or requesting limitations on processing, including decisions about the inclusion or exclusion from AI training algorithms. Organizations handling EU patient or research participant data should be equipped to effectively process and respond to data subject rights requests within 30 days or less under most circumstances.

Another important key principle relates to 'data security'. Although the DPF (and indeed the GDPR) is not specific about what counts as reasonable security measures, organizations may find guidance from HIPAA's Security Rule.[58] Other resources to consider include the NIST Cybersecurity Framework, HITRUST certification requirements, or international standards like ISO 27001 and 27701.[59] Effective implementation of any of these models could demonstrate adequate data protection for cross-border transfers of personal data.[60] For examples of security frameworks, see Exhibit 2.

57 Data Privacy Framework Program, *Participation Requirements Data Privacy Framework (DPF) Principles* (last accessed: June 20, 2024), https://www.dataprivacyframework.gov/program-articles/Participation-Requirements-Data-Privacy-Framework-(DPF)-Principles.

58 HHS Administrative Data Standards, 45 CFR 160, 164.

59 U.S. National Institute for Standards and Technology, *Cybersecurity Framework* (Apr. 19, 2022), https://csrc.nist.gov/Projects/cybersecurity-framework/nist-cybersecurity-framework-a-quick-start-guide; HITRUST Alliance, *HITRUST CSF Download* (Apr. 4, 2023), available from: https://hitrustalliance.net/csf-license-agreement/

60 International Standards Organization, *ISO/IEC 27001:2022* (2022), https://www.iso.org/standard/27001; International Standards Organization, *ISO/IEC 27701:2019* (2019), available from: https://www.iso.org/standard/71670.html

Exhibit 2. 'Reasonable Safeguard' Security Frameworks

NIST Cybersecurity Framework	HITRUST Framework	ISO 27001/ISO 27701
• Created in 2016 • Includes 'cross-roads' to other security frameworks • Designed to be industry agnostic • NIST is a government entity	• Created in 2007 • Is mapped to HIPAA Security Rule requirements • Designed for the healthcare industry • HITRUST is an independent, non-profit entity based in the US	• Created in 2005 • Was the first standard for information security • Based on 'domains' of activity • ISO is a non-governmental, independent, international organization

Source: Author-created, Author's analysis of security frameworks used in healthcare practice

Healthcare professionals should advise concerned patients and research participants to familiarize themselves with their rights and obligations specified in these privacy notice documents, and, if necessary, seek legal advice or consult with EU data protection authorities. While organizations may choose not to participate in the DPF process, opting instead for alternative models, implementing these proactive measures can help organizations demonstrate compliance with EU requirements. Even more, these activities are vital for safeguarding patient rights, ensuring adequate privacy protection, and reinforcing trust between healthcare entities and individuals.

In the event data subjects like patients or research subjects file a complaint, US organizations may face audits of their DPF self-certification. If a complaint is filed, the FTC will assess whether the organization has adhered to the DPF principles. This review includes evaluating the organization's response time to complaints, its efficiency in fulfilling data subject rights requests, and whether its privacy notices are both visible and updated to reflect current practices. Organizations that are not subject to the FTC or the Department of Transportation are not eligible for the DPF framework, and the DPF requires organizations and independent recourse mechanisms maintained by these agencies to investigate and expeditiously resolve complaints and disputes from EU residents about their data.[61]

The FTC's broad enforcement role under Article 5 of the FTC Act likely encompasses most organizations, though it is theoretically possible that research institutions might be alternatively regulated under the Common Rule and outside the primary FTC purview. However, the FTC has worked alongside HHS to complement its enforcement goals for organizations currently outside HIPAA and the Common Rule.[62] Administrative agencies like the US Department of Health and Humans Services may need to explain its plans with respect to working alongside the FTC for DPF enforcement. Organizations working directly with EU data protection authorities must

61 Data Privacy Framework Program, *Enforcement of the Data Privacy Framework (DPF) Program* (2023), https://www.dataprivacyframework.gov/s/article/Enforcement-of-the-Data-Privacy-Framework-DPF-Program-dpf.

62 Carmel Shachar et al., *Beyond HIPAA: The FTC's Increasing Focus on Protecting Health Data,* 10 Health Affairs Forefront (Aug. 31, 2023), http://dx.doi.org/10.1377/forefront.20230830.592387.

respond directly to them and similarly resolve complaints and disputes expeditiously.[63] Resolution will typically be accomplished through arbitration but may be heard by an Independent Data Protection Review Court under the executive branch.[64]

VI. FUTURE CHALLENGES

After two failed agreements for purposes of adequacy, Safe Harbor and Privacy Shield, healthcare organizations may wonder whether relying upon the DPF may be a reliable strategy for cross-border data sharing. As described earlier in this article, the DPF and its predecessors, despite calls for a health research safe harbor, were not specifically designed for the health sector.[65] Further, the inability of previous agreements deemed adequate to maintain their adequacy after legal challenges leaves healthcare entities on shaky footing. This means organizations may wish to consider alternative data transfer methods based on appropriate safeguards rather than adequacy.

One limit to healthcare organizations' reliance on the DPF is the enforcement model, which seemingly leaves healthcare regulators out of the loop. While HIPAA *is* specifically designed for health data, with compliance regulated by the US Department of Health and Human Services (HHS),[66] the DPF is only regulated by general consumer and trade agencies. Because the DPF and its predecessors have not created any synchronicity or sharing of information with the US Department of Health and Human Services, the DPF may not be the sole framework applicable to the processing of health data, meaning that organizations will likely have to demonstrate compliance with HIPAA as well as the DPF.

One potential challenge concerns whether the DPF adequately meets the EU's individual country requirements above and beyond the EU's GDPR. The GDPR, which forms the basis for the DPF, allows some flexibility for EU Member States to mandate additional protections for 'special categories' of data, such as more sensitive biometric, genetic, and health data.[67] This implies that individual countries may impose additional legal requirements on health data within a particular country. Although these additional legal requirements are not specific to third-country data transfer, countries could elect to localize such data or establish additional obligations

63 Data Privacy Framework Program, *Data Privacy Framework Principle 7. Recourse, Enforcement and Liability* (2023), https://www.dataprivacyframework.gov/s/article/7-RECOURSE-ENFORCEMENT-AND-LIABILITY-dpf?tabset-35584=2.

64 *Id.*; The White House, *Fact Sheet: United States and European Commission Announce Trans-Atlantic Data Privacy Framework* (Mar. 25, 2022), https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/25/fact-sheet-united-states-and-european-commission-announce-trans-atlantic-data-privacy-framework/. At this time, it is unknown how this court will be run, though it is likely it will operate more similarly to an administrative court, as it is not part of the judicial branch.

65 Laura Bradford et al., *International transfers of health data between the EU and the USA: a sector-specific approach for the USA to ensure an 'adequate' level of protection*, 7(1) J. Law & Biosciences 1, 19–20 (2020), https://doi.org/10.1093/jlb/lsaa055

66 Charlotte A. Tschider, *AI's Legitimate Interest: Towards a Public Benefit Privacy Model*, 21(1) Hous. J. Health L. & Pol'y 125, 149–50 (2021), https://houstonhealthlaw.scholasticahq.com/article/31666-ai-s-legitimate-interest-towards-a-public-benefit-privacy-model

67 Regulation 2016/679 Art. 9. Article 9 consists of a wide variety of categories, including racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, health data, and sex life or sexual orientation. Many of these categories are captured along with health data for both treatment and research purposes.

that follow the data with its transfer. These additional requirements could conflict with or establish additional requirements for DPF participants. Although EU organizations transferring data should be aware of these requirements that apply whether or not data are transferred, it is equally important for US organizations to verify that compliance with the DPF will suffice for data transfers if they rely upon the DPF to transfer personal data to the US.

The idea that additional requirements may apply to health data in Member States is not merely conceptual. In addition to the passage of country laws based on GDPR, EU Member States have established a variety of legal frameworks regarding health data. For instance, in 2020, Germany adopted the Patient Data Protection Act, which was intended to enhance patient medical record digitization.[68] German residents are allowed to make their data available for research purposes through data donation and informed consent. However, some public health registries may require an ethics review, a licensing application, and possibly localized access to data within a specific tool.

Although these restrictions apply to data within a Member State, additional limitations on transfer extra-territorially introduce complexity to a purposefully streamlined framework. For healthcare, more complexity could affect the development of innovative healthcare technologies and delivery of essential health services.[69] If the DPF can be reliably used for health data transfers without additional complexity and additional requirements, the DPF will be a valuable tool for organizations engaged in collaborative efforts between the US and EU countries.

One advantage, at least legally, is that adequacy, which the EU has claimed the DPF agreement achieves, is the strongest justification for data sharing outside the EU.[70] However, organizations relying upon the DPF might not meet all the requirements for health data sharing in every EU country and therefore must proactively stay informed about any developments in this area to ensure compliance with DPF specific requirements and potentially consider alternative (though less-favorable) bases for transfer, such as EU-approved contractual agreements and associated Transfer Impact Assessments (TIA).

Organizations that may not want to rely on the DPF may meet the GDPR's requirements under Article 46 by establishing reasonable safeguards using process and contractual obligations.[71] Following *Schrems II*, EU organizations transferring data to the US, 'exporters,' should perform a TIA on an 'importer' to ascertain potential risks, such as security risks,[72] associated with transfer to the importer in a third country.[73] If the risks are reasonable, the exporter can use EU-approved standard contractual agreements as one adequate basis for cross-border transfer, called the 'Standard Contractual

68 Bundesministerium für Gesundheit, *Cabinet adopts Patient Data Protection Act* (Apr. 1, 2020), https://www.bundesgesundheitsministerium.de/presse/pressemitteilungen/2020/2-quartal/pdsg.html

69 Heidi Beate Bentzen et al., *Remove obstacles to sharing health data with researchers outside of the European Union*, 27 Nat Med 1329, 1329 (2021), https://doi.org/10.1038/s41591-021-01460-0

70 *Cf.* Corrales Compagnucci, *supra* note 18, at 37, 38.

71 *See* note 3, Art. 46.

72 *See supra* note 23, at 44.

73 European Data Protection Board, *Supplementary Measures Transfer Tools* (Jun 18, 2021), https://edpb.europa.eu/system/files/2021-06/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_en.pdf; CNIL, *Draft Practical Guide Transfer Impact Assessment* (Feb. 12, 2024), https://www.cnil.fr/sites/cnil/files/2024-01/draft_practical_guide_transfer_impact_assessment.pdf.

Exhibit 3. Data Transfer Legal Models

	Data Protection Framework	**Standard Contractual Clauses (SCCs)**
Qualifying	• Self-certify at the DPF Website • Ensure organization has internal practices to fulfill principles	Add unedited SCCs to all research or data-sharing contracts between organizations and assess potential transfer risks prior to transfer
Status	• Adequate as of July 2023, previous challenges invalidated earlier versions	Upheld through previous challenges
Changes Needed	• No re-certification needed if current • Update internal practices • Update privacy notice	• Use 2021 SCC version (may require contract renegotiation) • Conduct Transfer Impact Assessment

Source: Author-created, Author's analysis of applicability and potential differences between DTF and Standard Contractual Clauses

Clauses (SCCs) as the basis for establishing reasonable safeguards.'[74] The SCCs are a collection of contract clauses, typically added as an addendum to agreements between two entities. Organizations relying on the SCCs must ensure these clauses remain unedited.

Although these steps may seem extensive, maintaining this vigilance is essential to protect patient privacy and may be a more reliable way of facilitating collaboration between the EU and the US. *See* Exhibit 3 for a comparison of both DPF and contract models.

It is also important to note that the current DPF does not incorporate any specific requirements related to the EU's AI Act, which has now completed its adoption process and introduces additional obligations for AI applications.[75] For example, certain types of AI classified as 'hazardous' or excessively high-risk may be prohibited for use in the EU.[76] Additionally, organizations will be required to register high-risk AI applications and perform extensive risk assessments.[77] In some cases, these findings may need to be reviewed by regulators. AI systems used in conjunction with patient health data, such as EU Class IIa or higher medical devices (some of which will be created or outfitted with AI by US organizations), could be considered 'high-risk' in various applications.[78]

74 EC Implementing Decision 2021/914; European Commission, *Standard Contractual Clauses* (Jun 4, 2021), https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en;

75 European Parliament, *EU AI Act: first regulation on artificial intelligence* (Jun 14, 2023), https://www.europarl.europa.eu/news/en/headlines/society/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence

76 Laying Down Harmonized Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts, EU 2021/0106 (COD), Art. 6(2); Annex III.

77 *Id.*, at Art. 51.

78 Sharon Lamb et al., *EU regulation: AI Act will mean a raft of new requirements for 'high-risk' systems*, DIGITALHEALTH (Apr. 24, 2024), https://www.digitalhealth.net/2024/04/eu-regulation-ai-act-will-mean-a-raft-of-new-requirements-for-high-risk-systems/.

AI applications may be used in conjunction with the receipt of EU personal data for health-related purposes, creating EU compliance issues.

VII. THE URGENT NEED FOR ROBUST DATA-SHARING FRAMEWORKS

During the COVID-19 pandemic, health data sharing emerged as a crucial tool for achieving common goals: to eliminate and slow the transmission of the virus.[79] Recent calls for collaboration have involved genomic registries, infectious disease research, and rare disease research, though theoretically, any kind of healthcare research could benefit from cross-border data sharing.[80] However, many research collaborations are not possible due to incompatible privacy and data protection legal obligations. In response, some have explored alternatives like synthetic data generation, which is the process of creating new data that can function as an alternative to personal data and is not derived from personal data (as pseudonymization, de-identification, and anonymization are).[81] Because synthetic data is not personal data or derived from personal data, it is not regulated under the GDPR and would operate outside the DPF and other mechanisms for transfer. However, the healthcare industry tends to be risk-averse due to potential safety issues, so generally identifiable personal data are preferred over synthetic data.[82] The prevailing trend towards big data and AI amplifies the complexity of achieving privacy compliance.[83]

AI is positioned to overcome the most intractable of health challenges, but it requires high-quality, representative, contextual data appropriate for planned health applications.[84] These data can be difficult to generate, collect, create, or otherwise aggregate from a variety of sources, and the volume of data needed to power any AI applications is extremely high. Machine learning, currently the most prevalent AI methodology, forms the basis for more advanced forms of AI, such as neural networks and deep learning applications. Machine learning is a learning model based on large statistical analysis of big data sets, and neural networks and deep learning more intensely use such data for complex decisional systems.

Although there are a variety of different challenges with AI-supported healthcare, or even the use of AI to develop healthcare products, one of the primary challenges

79 Lyndsay T. Glass et al., *Cross-border healthcare: A review and applicability to North America during COVID-19*, Health Policy OPEN 1, 2 (Dec. 2022), https://doi.org/10.1016/j.hpopen.2021.100064

80 Genya Dana & Arnaud Bernaert, *Sharing Sensitive Health Data in a Federated Data Consortium Model: An Eight-Step Guide*, World Economic Forum 1, 3 (Jul. 2020), https://www.weforum.org/reports/sharing-sensitive-health-data-in-a-federated-data-consortium-model-an-eight-step-guide; Marco Liverani et al., *Sharing public health data and information across borders: lessons from Southeast Asia*, 14(94) Globalization and Health 1, 8 (2018), https://doi.org/10.1186/s12992-018-0415-0

81 August DuMont Schütte et al., *Overcoming barriers to data sharing with medical image generation: a comprehensive evaluation*, 4 npj digital medicine 1, 1 (2021), available from: https://www.nature.com/articles/s41746-021-00507-3; Luca Bonomi et al., *Privacy challenges and research opportunities for genomic data sharing*, 57(7) Nature Genetics 645–46 (2020), https://doi.org/10.1038/s41588-020-0651-0

82 Mauro Giuffré & Dennis L. Shung, *Harnessing the power of synthetic data in healthcare: innovation, application, and privacy*, npj digital medicine (2023), https://www.nature.com/articles/s41746-023-00927-3.

83 W. Nicholson Price II & I. Glenn Cohen, *Privacy in the age of medical big data*, 25 Nature Medicine 37–38 (2019), https://www.nature.com/articles/s41591-018-0272-7; Nicolas P. Terry, *Big Data Proxies and Health Data Exceptionalism*, 24 Health Matrix 66, 97 (2015). Big data implementation, such as those used for AI algorithmic development and for broad research uses, frustrate traditional notions of privacy as an individualistic endeavor.

84 W. Nicholson Price II, *Medical AI and Contextual Bias,* 33 Harv. J. L. & Tech. 66, 77–79 (2019).

involves use of previously collected data, both access to volumes of data and whether AI training might be consistent with previous processing limitations. The EU has determined that AI training and development based on previously processed personal data, may be considered a distinct and separate processing activity.[85] For processing health data, particularly in the context of AI training, the GDPR typically requires obtaining explicit consent from the individuals whose data is being used. Explicit consent is a clear, affirmative action that signifies agreement to the processing of personal data.

However, there are specific circumstances, outlined in Article 49 of the GDPR, where derogations (exemptions) may apply.[86] These derogations allow for the transfer of health data without explicit consent under certain conditions, for example when it's necessary for important reasons of public interest or for the protection of vital interests where the data subject is physically or legally incapable of giving consent. This may be favorable for these limited purposes. However, as explained earlier in this article, derogations related to special categories of personal data, which permit Member States to adopt country laws that create different obligations (ie more restrictive limits) with respect to these special categories, such as health data, could create challenges for adequacy decisions involving sector-specific data transfers.

HIPAA permits some exceptions to processing restrictions for similar limited purposes, too, such as in emergency situations that could affect the vital interests of an individual or for public health purposes.[87] In some cases, such exceptions are broader than the GDPR. Under the Department of HHS' interpretation of HIPAA, data reuse for AI (and lack of specificity in its use) within the context of research may be waived by an Institutional Review Board.[88] Outside a research context, HIPAA does require explicit consent for additional processing of protected health information outside treatment, payment, and healthcare operations, with the ability to revoke consent and restrict any further processing.[89] Following the Roundtable on Sharing and Utilizing Health Data for AI Applications, an HHS-hosted event in 2019, a report was distributed, specifically calling out the need for more robust health data sharing for AI.[90]

The roundtable pinpointed key data types that are considered 'high value' for future AI applications: administrative and claims data, clinical data, clinical trials data, EHR

85 European Parliament, *The impact of the General Data Protection Regulation (GDPR) on artificial intelligence* (June 2020), https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641530/EPRS_STU(2020)641530_EN.pdf, at I-II. (describing AI processing as context dependent – potentially separate processing that is incompatible with original purposes for processing and in other cases internally compatible with original processing justification and lawful bases).

86 *See* GDPR, *supra* note 3, Art. 9(4).

87 45 CFR 164.512(b)

88 U.S. Dept. Health Hum. Svcs., *Institutional Review Boards and the HIPAA Privacy Rule* (Aug. 2003), https://privacyruleandresearch.nih.gov/pdf/IRB_Factsheet.pdf#:~:text=If%20certain%20conditions%20are%20met%2C%20an%20IRB%20may,are%20in%20section%20164.512%28i%29%20of%20the%20Privacy%20Rule, at 3. In 2022, HHS called for additional development of research-specific examination of AI development in relation to Common-Rule regulated data gathering. U.S. Dept. Health Hum. Svcs., *IRB Considerations on the Use of Artificial Intelligence in Human Subjects Research* (Oct. 19, 2022), https://www.hhs.gov/ohrp/sachrp-committee/recommendations/irb-considerations-use-artificial-intelligence-human-subjects-research/index.html.

89 Protected health information, or PHI, is a statutorily defined data type including past or present health conditions and is identifiable. 45 CFR 160.103.

90 The Center for Open Data Enterprise, *Sharing and Utilizing Health Data for AI Applications Roundtable Report* (2019), sharing-and-utilizing-health-data-for-ai-applications.pdf (hhs.gov).

data, genomic data, patient-generated data, Internet of Things data, social media data, social determinants of health data, surveillance data, registry data, survey data, and vitals data.[91] Out of these various data types, six were profiled explicitly as both highly critical and especially difficult to obtain and share: administrative and claims data, clinical data, genomic data, patient-generated data, social determinants of health data, and surveillance data.[92] The challenges identified by this group included inconsistent restrictions on data use, including differences in the US system between data covered by HIPAA and consumer health products, underlying bias in some data sets, the siloing of data within countries, and perceptions of a more restrictive legal regime than actually exists.[93]

Another challenge to effective sharing involves a lack of interoperability and common data models between systems, complicating the free flow of otherwise legal data sharing.[94] Model data sharing/use agreements, the contractual basis for data sharing often used internationally, were also identified as an area of potential development, since negotiations of these agreements often last 12 months or more.[95] The policy surrounding model data sharing and use agreements was updated in 2023 to reflect some of these changes, including:

- Comprehensive security domains (referenced in Exhibit 2);
- Disclosure of purposes for use;
- Robust description of the data;
- Plans for reducing identifiability through de-identification;
- Data quality management;
- Limits on disclosure and use;
- Specific limitations for linkage between data sets and reuse;
- Disposition and retention limitations.[96]

While these updates featured much welcomed improvements and clarifications, it is clear that much more needs to be done to improve transatlantic data sharing models. This is particularly true in the health sector, where more effective and robust US/EU collaborations hold much potential for medical innovation and the advancement of medical care and the health sciences.

VIII. TOWARDS AN EFFECTIVE DATA SHARING MODEL

Despite the extensive negotiations and efforts put into the DPF, the DPF alone will not likely encompass all the necessary measures to effectively address the complexities faced by organizations engaged in the exchange of sensitive health data between the

91 *Id.*, at 10.
92 *Id.*, at 10–12.
93 *Id.*, at 13.
94 *Id.*, at 13, 16.
95 *Id.*, at 16.
96 U.S. Dept. of Health & Hum. Svcs., *HHS Policy for the Common Data Use Agreement (DUA) Structure and Repository* (Jan. 2023), https://www.hhs.gov/web/governance/digital-strategy/it-policy-archive/hhs-policy-common-data-use-agreement-structure-repository.html.

US and specific EU countries. As a result, healthcare professionals collaborating with organizations in EU countries may encounter additional limitations and requirements when transferring health data across the Atlantic, potentially undermining the key goals of the DPF.

First, because the DPF is not explicitly designed for health data transfer, additional requirements may apply to data shared from the US to the EU to meet HIPAA requirements. For example, data used for treatment, payment, and healthcare operations are limited in scope by a primary privacy notice, but no lawful basis for these purposes is required, including consent, even though the data processed are considered 'special categories.'[97] For the EU, all processing activities require some lawful basis for that processing, which means that each processing activity will require clearly articulating the lawful basis for each activity.[98] The concept of justifying the lawful basis for processing for each activity may be a new exercise for US organizations that principally rely on implied consent for most data collection and use.

Additionally, while the DPF may accommodate EU requirements, it may not contain HIPAA requirements, such as requiring disclosure of a terminating date or event for secondary processing activities and disclosure of any third party receiving such data's specific name, which under HIPAA requires express authorization.[99] This means that data transferred from the US to the EU could require additional steps, as well. While the DPF and HIPAA are not completely incompatible, some of these differences create challenges in relying on the DPF completely for transfer of health data between the US and EU. Although the DPF offers a potential avenue for broad health data sharing, we strongly advise organizations build DPF-compatible programs while also exercising caution and avoiding sole reliance on it. There are a variety of approaches that could feasibly be used to accomplish these goals, and which would more holistically facilitate data sharing, through private legal options or public legal agreement.

One potential legal option would involve combining the EU SCCs, a model data use agreement (potentially based on US agency agreements, such as those for CMS data),[100] and HIPAA contractual requirements, combined together for EU–US health data sharing. The SCCs, as a contractual commitment to follow most, if not all of GDPR's requirements, are enforceable in many courts and have been upheld as valid. Data use agreements (DUA) are used both outside the US government and within it prior to transferring data between two parties.[101] They typically include many of the same restrictions and obligations the SCCs require, with less standardization.

This model of establishing obligations is also consistent with many modern health data-sharing practices, which usually include a business associate contract (known as

97 Organizations must develop both an externally facing privacy notice, a 'Notice of Privacy Practices,' and internal policies and procedures. 45 CFR 164.520(a), (b); 45 CFR 164.530(i).

98 *See* GDPR, *supra* note 3, Art. 9(4).

99 45 CFR 164.508; 45 CFR 164.532.

100 U.S. Dept. Health & Hum. Svcs., *HHS Policy for the Common Data Use Agreement (DUA) Structure and Repository* (Jan. 2023), https://www.hhs.gov/web/governance/digital-strategy/it-policy-archive/hhs-policy-common-data-use-agreement-structure-repository.html#appendix-d.

101 *Id.*

a business associate agreement or BAA).[102] BAAs are required under HIPAA when transferring protected health information to a third party doing work on behalf of that entity and are executed as a contractual addendum.[103] The BAA contractually exports HIPAA requirements to third parties that may or may not be regulated under HIPAA, similar to the SCCs under the GDPR. However, a key difference between SCCs and the BAA is that HIPAA obliges a primary entity to execute a BAA when transferring protected health information to another third party—regardless of whether any other lawful basis exists for its processing and regardless of the third party's geographic location.[104]

At minimum, an organization could incorporate, individually, the SCCs, a DUA, and a BAA into a contract between two entities, one in the EU and another in the US, as individual addenda. Although organizations *could* include all three addenda individually to an agreement between organizations or institutions, linguistic differences ('processing' v. 'collection and use') and slightly different protective measures could create inconsistencies. For example, there are several linguistic differences between HIPAA and GDPR—including the name of entities (covered entity v. controller), actions related to data (processing v. collection and use), reduced identifiability characteristics (de-identification v. pseudonymization and anonymization), and rights (amendment v. correction), amongst others. Most prominently, however, is the difference in the required lawful basis for processing, especially for special categories of data like health data, which usually mandates express consent.[105]

Although there is much more consistency between HIPAA and the GDPR than most US privacy laws, specified standards also differ. For example, the US adheres to a de-identification safe harbor (of which pseudonymization qualifies) to remove protected health information from HIPAA's obligations, while anonymization (a higher standard than de-identification, which expressly does not include pseudonymized data) is required under the GDPR.[106] Even anonymizing data is a processing activity, requiring a lawful basis.[107] HIPAA requires no such additional justification for de-identification and subsequent unrestricted use. In some cases, HIPAA establishes more comprehensive standards. The GDPR only requires organizations to implement 'reasonable technical and organisational measures' to protect data, while HIPAA requires compliance with the Security Rule, which is extensive.[108] On the other hand, the GDPR includes extensive privacy right articulation, which is not as fully developed under HIPAA, including objection to automated processing and a right of erasure.[109]

102 *Business Associate Contracts*, U.S. Dept. Health & Hum. Servs. (Jan. 25, 2013), https://www.hhs.gov/hipaa/forprofessionals/covered-entities/sample-business-associate-agreement-provisions/index.html [https://perma.cc/AS4R-MH62].

103 *Id.*

104 45 CFR 164.502(e); 164.504(e); 45 CFR 164.532.

105 45 CFR 164.502(a)(1); *see* GDPR, *supra* note 3 Art. 9; Rec. 53.

106 Info. Comm. Office, *What is personal data?* https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/personal-information-what-is-it/what-is-personal-data/what-is-personal-data/ (last accessed: June 28, 2024).

107 *Id.*

108 *See* GDPR, *supra* note 3, Art. 32;

109 *See* GDPR, *supra* note 3, Art. 17; Art. 21.

These key differences could create internal inconsistencies that ultimately lead to contractual reformation in court or potentially invalidation of SCCs as the basis for transfer to the US.[110] However, taken together, these documents could also minimally provide a complementary framework for data sharing that more fully reflects special considerations for health data. Indeed, many multinational companies today execute some version of a contract with multiple addenda, including these. However, the potential for issues in a multi-addenda approach demands a better solution.

The EC has begun expanding its view of internationally oriented cross-border transfers through model clauses, including a wide variety of contractual clauses, such as the ASEAN model clauses, as valid contractual mechanisms.[111] This new openness to consider alternative model clauses could provide the necessary support to enable a similar approach for the EU, US, and possibly other data-sharing countries in a combined, EC-approved and adopted health data-sharing contractual clauses. To accomplish this, entities within the EU and HHS would likely need to work together to develop a unified standard clause model for EU and US health data that the EC could approve. This model could include sensitive health data provisions, such as specific placeholders for extra steps organizations must take with respect to countries with specific requirements.[112] An EU and US working group would need to decide which terms of art from both laws should be included, and which more restrictive provisions should be included from either law. If successful, this effort could open a wide variety of opportunities for collaboration in research and commercial activities.

Another alternative that may require broad stakeholder involvement from Data Protection Authorities (DPAs) in several Member States but could receive support involves adopting alternative SCCs within individual Member State jurisdictions. Article 28(8) of the GDPR does permit national DPAs to approve alternative SCCs, as well, although these only are enforceable for the Member State that has accepted them.[113] If individual countries seek to promote data sharing for health data, for example in collaborative research, this may provide an alternative vehicle that does not require EC adoption.

With health data model clauses available, both private and public entities could leverage a common standard where sensitive data can be transferred based on an accepted model, consistent with the SCCs and HIPAA BAA requirements. However, a serious impediment to relying on new EU–US health data SCCs involves GDPR derogations. As described earlier in this paper, the GDPR expressly prohibits the processing of special categories of data, including genetic data, biometric data, or data concerning health. Processing of any kind, which includes transfer to third countries, is prohibited unless: (i) the data subject expressly consents, (ii) processing is in furtherance of a contract to which the data subject is party, (iii) it is necessary to protect

110 The SCCs may not be edited except in limited cases, and provisions must not be contradicted by other clauses. *See* European Comm'n, New Standard Contractual Clauses – Questions and Answers overview, https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/new-standard-contractual-clauses-questions-and-answers-overview_en#General (last accessed: July 1, 2024).

111 ASEAN & European Commission, *Joint Guide to ASEAN Model Contractual Clauses and EU Standard Contractual Clauses* (May 2023), https://commission.europa.eu/system/files/2023-05/%28Final%29%20Joint_Guide_to_ASEAN_MCC_and_EU_SCC.pdf.

112 *See* GDPR, *supra* note 3, Art. 9.

113 *Id.*, Art. 28(8).

the vital interests of the data subject, (iv) processing is performed by a not-for-profit or similar body in its course of legitimate activities, (v) for reasons of substantial public interest, (vi) processing is necessary for preventative or diagnostic medicine, provision of healthcare treatment, or (vii) for public health.[114] Additionally, under a derogation in Article 9, states may permit processing of such data under local exceptions: 'member states may maintain or introduce further conditions, including limitations, with regard to the processing of genetic data, biometric data or data concerning health.'[115]

In some cases, countries may impose stricter requirements for special data categories specific to data transfer processing, potentially including localization requirements, for a variety of reasons including perceived risk of transfer or even economic interests.[116] Recital 53 of the GDPR cautions against over-restriction of data flows, in that 'this should not hamper the free flow of personal data within the Union when those conditions apply to cross-border processing of such data,' though it is unknown whether this would prohibit localization requirements or more extreme limits on data transfer out of country.[117] At the time of writing, no express health data localization laws exist in the EU. While health data standard clauses might not overcome localization requirements or extreme limits, they could be a first step for EU Member States aligned with data-sharing goals. The possibility of country-specific health data requirements or restrictions should not be a complete bar to exploring a contractual basis for health data transfer outside the DPF.[118]

Another approach could be developing a health data-specific framework for organizations to transfer health data. As mentioned in previous sections, HIPAA is the most comprehensive federal data protection law in the US; it is more like the GDPR than any other US privacy law. Both bodies of law could benefit from a complementary approach that integrates elements of both and establishes a common language. Instead of creating new contractual clauses, adopting a framework similar to the DPF in function and approval process, consistent with the GDPR's Article 45 permitting an adequacy decision for a 'specified sector,' could eliminate the need for individual contracts between organizations wishing to share data, thereby saving time.[119] Choosing a framework tailored to the health sector could facilitate a realignment of priorities between the EU and US healthcare systems, focusing on healthcare rather than solely on global trade. Unlike most commercial activities, data sharing in healthcare primarily benefits healthcare research and healthcare activities that will improve the life of human beings if not

114 *See* GDPR, *supra* note 3 Art. 9; Art. 9(4). Additional exception-based lawful bases for processing special categories of data exist, as well (a total of 10 bases).

115 *Id.*

116 Organisation for Economic Co-operation and Development (OECD), *The Nature, Evolution and Potential Implications of Data Localisation Measures*, OECD Trade Policy n°278 (Nov. 2023), https://www.oecd.org/en/publications/the-nature-evolution-and-potential-implications-of-data-localisation-measures_179f718a-en.html, at 3 (describing health data as typically a target of more restrictive localization laws world-wide).

117 *See* GDPR, *supra* note 3 Rec. 53.

118 It should be noted that there are alternative methods for justifying reasonable safeguards for transfer, including approval of internal commercial practices, binding corporate rules. *See* GDPR, *supra* note 3 Art. 47. This requires approval of the binding corporate rules and practices of a specific organization. Although this could be a useful approach for large and especially multi-national organizations with multiple legal entities, small to medium entities will not likely benefit.

119 *See* GDPR, *supra* note 3, Art. 45(1).

collective public health. The challenge, however, is the complexity of approving such a framework and the time needed to adequately negotiate an appropriately restrictive model that is both legally robust and reasonably consistent with both bodies of law.

IX. CONCLUSION

The DPF's 2023 adequacy determination represents a crucial advancement in the realm of cross-border data exchange but not the end of necessary discussions on the topic. As this paper has explored, the DPF may streamline the transfer of sensitive health data between the EU and the US, fostering enhanced collaboration in healthcare and research. However, as we have examined, the DPF, while a significant step forward, is not a panacea for all the complexities inherent in the global exchange of health data, and perhaps a more coordinated and focused effort is necessary.

The DPF, despite its advancements, may not fully encapsulate the varied and specific health privacy requirements of individual EU Member States or of US HIPAA legal requirements. This gap requires a cautious and well-informed approach to compliance, particularly where full GDPR adherence is required. The suggested synergy of the EU SCCs with a Model DUA and BAA provisions presents a viable pathway to bridge these gaps, offering a more comprehensive and complementary system for data sharing. Organizations may wish to combine addenda for the time being but may also consider proposing combined provisions in Member States where data will be transferred for adoption as approved SCCs that account for two bodies of law.

Moreover, the exploration of alternative mechanisms, such as the development of regional health data model clauses or a health data-specific framework that is deemed adequate by the EC, underscores the need for ongoing innovation and collaboration in this field. These alternatives, while challenging to implement, could provide more tailored solutions that align more closely with the intricate requirements of health data protection laws in both regions. Even if the EC does not wish to prioritize these efforts, regional collaboration between DPAs and healthcare organizations could provide the needed momentum to develop alternatives to purely private contractual and broad DPF models.

In conclusion, the DPF can be regarded as a significant milestone in the journey towards a more fluid and legally sound data exchange between the EU and the US. However, not only in light of the foreseeable challenges to the DPA, but also to diversify the available pathways for health data exchange, it is imperative that healthcare and research organizations not solely rely upon this framework. Rather, they must continue to explore and develop additional legal mechanisms and collaborative strategies. This will ensure that the exchange of health data not only complies with the stringent privacy standards on both sides of the Atlantic but also effectively supports a more robust global advancement of healthcare and medical research. As the landscape of data protection continues to evolve, so, too, must our approaches to ensuring the secure, ethical, and efficient transfer of health data in an increasingly interconnected world.

ACKNOWLEDGEMENTS

This research was supported, in part, by a Novo Nordisk Foundation Grant for a scientifically independent Collaborative Bioscience Innovation & Law Program (Inter-

CeBIL program – grant no. NNF23SA0087056), and by the European Union project CLASSICA, Horizon Europe (grant no. 101057321). Views and opinions expressed are, however, those of the author(s) only and do not necessarily reflect those of the NNF, the European Union or the Health and Digital Executive Agency. Neither the NNF, nor the European Union nor the granting authority can be held responsible for them.

Charlotte Tschider: Professor Tschider is the author of International Cybersecurity and Privacy Law in Practice (Wolters Kluwer 2018, 2023) and Cybersecurity Law (with David Thaw, Gus Hurwitz, and Derek Bambauer, West 2021). Her primary scholarship examines legal issues in artificial intelligence, international data protection, information privacy, cybersecurity law, and healthcare medical device technology. Professor Tschider's academic writing have appeared or are forthcoming in the Yale Journal of Law & Technology, the Yale Journal of Law & Policy, Washington University Law Review, Iowa Law Review, Maryland Law Review, and the BYU Law Review, amongst others. She has appeared on NPR's All Things Considered and has been featured in a variety of news media publications, including USA Today, Forbes, The Hill, Stat, and Foreign Affairs. Prior to her time in academia, Tschider served in various senior corporate management capacities in information technology, cybersecurity, privacy, and legal compliance, for two decades.

Marcelo Corrales Compagnucci: Marcelo Corrales Compagnucci is an Associate Professor & Associate Director at the Center for Advanced Studies in Bioscience Innovation Law (CeBIL), Faculty of Law, University of Copenhagen in Denmark. His past activities have included working as a consultant and lawyer for law firms and IT companies. He was also a research associate with the Institute for Legal Informatics (IRI) at Leibniz Universität Hannover in Germany, and a visiting research fellow in various research centers around the world in the United States, the United Kingdom, Germany, Japan, Italy, and Taiwan. He has a Doctor of Laws (LL.D.) degree from Kyushu University in Japan. He also holds a Master of Laws (LL.M.) in international economics and business law from Kyushu University, and an LL.M. in law and information technology and an LL.M. in European intellectual property law, both from the University of Stockholm in Sweden. His expertise spans across the intersecting domains of IT and Law, where he has made significant contributions through his extensive academic and professional pursuits. Marcelo's scholarly output encompasses 12 books (3 monographs and nine anthologies) and over 90 articles and book chapters published in high-impact journals and by renowned publishing companies.

Timo Minssen: Timo Minssen is Professor of Law at the University of Copenhagen (UCPH). He is the Founding Director of UCPH's Center for Advanced Studies in Bioscience Innovation Law (CeBIL), an LML Research Affiliate at the University of Cambridge, and an Inter-CeBIL research affiliate of the Petrie-Flom Center for Health Law Policy, Biotechnology, and Bioethics at Harvard Law School. His research, supervision, teaching & part-time advisory practice concentrates on Intellectual Property-, Competition & Regulatory Law, as well as on the law & ethics of emerging health & life science technologies, such as genome editing, big data, artificial intelligence and quantum technology. Timo serves as an advisor to the WHO, WIPO, EU Commission, various organizations, companies,

national governments, and law firms. He has been a visiting scholar at the Technical University of Munich, and at the Universities of Cambridge, Oxford, Harvard, and the Chicago Kent College of Law. Timo frequently presents his research at international symposia and major law firms,. His publications comprise seven books, as well as 200+ articles and book chapters. Timo's research has been featured in The Economist, The Financial Times, El Mundo, Politico, WHO Bulletin, Times of India & Times Higher Education, and was published in Science, JAMA, NEJM Catalyst, Harvard Business Review, Harvard Business Manager, Nature Biotechnology, Nature Genetics, and many more.