Emory International Law Review

Volume 37 | Issue 1

2022

Stifling Innovation: How Global Data Protection Regulation Trends Inhibit the Growth of Healthcare Research and Start-Ups

Ryan Preston

STIFLING INNOVATION: HOW GLOBAL DATA PROTECTION REGULATION TRENDS INHIBIT THE GROWTH OF HEALTHCARE RESEARCH AND START-UPS

TABLE OF CONTENTS

INTRODUCTION: MEDICINE AND THE USE OF DATA PROCESSING 135
I. DATA PROTECTION REGULATION AND PATIENT PROTECTIONS 139
A. The United States 140
1. HIPAA and Other Federal Policies 140
2. State Regulations 142
B. The European Union 143
C. The United Kingdom 149
D. Canada 149
E. China 150
II. BENEFITS AND RISKS OF DATA PROCESSING AND SHARING 152
A. Benefits and Risks for Researchers, Start-Ups, and Medical Professionals 152
B. Risk Prevention for Researchers, Start-Ups, and Medical Professionals 154
1. Anonymization 154
2. Consent 156
C. Risks to Individuals 157
III. IMPROVING DATA ACCESS POLICIES FOR HEALTHCARE AND TECH START-UPS 160
A. International Policy and Reduction of Penalties 160
B. Encouraging Data Sharing 162
C. Ensuring Protection of Individual Data Rights 163
CONCLUSION 165

INTRODUCTION: MEDICINE AND THE USE OF DATA PROCESSING

Between December 10, 2014 and February 4, 2015, a health insurer Anthem, Inc.'s data warehouse was hacked, and this resulted in the theft of personally identifiable information and the personal health information of some eighty

million individuals.[1] By 2020, Anthem paid $39.5 million as part of a settlement.[2] On average, the cost to a company for a healthcare data breach has increased to $9.23 million per incident.[3] Similar data breaches could cost companies even more outside of the United States, where data protection regulations are more stringent.[4] Despite the high costs associated with data breaches, companies continue to invest in healthcare data across the world as the data is incredibly valuable for healthcare innovation and progress. This data is often the key for existing companies to stay afloat or for new companies to successfully innovate.

Individuals across the world divulge the protected health data that these companies need every day. Often without thinking twice, people give companies and healthcare systems their name, address, birth date, and more. Regulations protecting this type of data vary from country to country under various different terms. In the United States, it is best known as protected health information (PHI), according to the Health Insurance Portability and Accountability Act of 1996 (HIPAA).[5] PHI is defined as "all '*individually identifiable health information'* held or transmitted . . . in any form or media, whether electronic, paper, or oral."[6] On the other hand, the European Union's data protection regulation, the General Data Protection Regulation (GDPR), refers to this data as personal data and defines it as "any information that relates to an individual who can be directly or indirectly identified."[7] Even within the European Union (EU) the definitions and terms may vary by country, though countries frequently look to EU regulations as a framework for their own statutes.[8]

---

[1] In re Anthem, Inc. Data Breach Litig., 236 F. Supp. 3d 150 (D.D.C. 2017).

[2] *Anthem to Pay Nearly $40 Million to Settle Data Breach Probe by U.S. States*, REUTERS (Sep. 30, 2020 10:20 AM), https://www.reuters.com/article/us-anthem-cyber/anthem-to-pay-nearly-40-million-to-settle-data-breach-probe-by-u-s-states-idUSKBN26L2PW.

[3] *IBM Report: Cost of a Data Breach Hits Record High During Pandemic*, IBM NEWSROOM (Jul. 28, 2021), https://newsroom.ibm.com/2021-07-28-IBM-Report-Cost-of-a-Data-Breach-Hits-Record-High-During-Pandemic.

[4] *See* Ben Wolford, *What are the GDPR Fines?*, GDPR.EU (2020), https://gdpr.eu/fines/ [hereinafter Wolford, *GDPR Fines*].

[5] UNITED STATES DEPT OF HEALTH & HUMAN SERV, SUMMARY OF THE HIPAA PRIVACY RULE, OCR PRIVACY BRIEF 3–4 [hereinafter OCR PRIVACY BRIEF].

[6] *Id.*

[7] Ben Wolford, *What is GDPR, the EU's New Data Protection Law?*, GDPR.EU (2020) https://gdpr.eu/what-is-gdpr/ [hereinafter Wolford, *What is GDPR*], .

[8] *See, e.g.*, Todd Liao, *Personal Information Protection Law: China's GDPR is Coming*, MORGAN LEWIS (Aug. 24, 2021), https://www.morganlewis.com/pubs/2021/08/personal-information-protection-law-chinas-gdpr-is-coming; DELOITTE, CHINA DRAFT PERSONAL INFORMATION PROTECTION LAW (PIPL): GENERAL INTRODUCTION AND IMPACT ANALYSIS 1 (2021).

From the perspective of a consumer, it may seem beneficial to strictly regulate data that can identify individuals. However, this data is also incredibly important to various companies, especially those within the healthcare industry, to boost research and innovation. Many companies collect and maintain records of consumer personal data, which many people understand as "Big Data."[9] Similarly, medical professionals and facilities maintain their own electronic records with more intimate information, including procedures, health risks, and more.[10] In fact, the National Institutes of Health (NIH) started the *All of Us* Research Program to gather health data from more than one million people living in the United States to accelerate health research.[11] Any company working to improve medical outcomes by developing pharmaceuticals, medical devices, or medical software must be able to send or receive this type of data because healthcare facilities and systems rely on this information.[12] Hospitals rely upon integrated networks to deliver large amounts of data for further processing (such as incorporated into medical records, forwarded to specialists, or analyzed with additional data sets), and they store this information on clinic information systems (CIS).[13] Also, especially with the COVID-19 pandemic, telemedicine has grown in popularity, requiring remote access to patient information.[14] Additionally, there are a wide variety of devices with daily access to personal data in the consumer market such as smartwatches, mobile phone health apps, and more.[15] The network of physical objects that connect and exchange data with each other and other systems over the internet create the Internet of Things

[9] "Big Data" is generally understood to mean analyzing particularly large volumes, variety, and velocity of data, or the three Vs as described by Doug Laney in 2001. *See* Doug Laney, *3D Data Management: Controlling Data Volume, Velocity, and Variety*, META GROUP INC. (Feb. 6, 2001).

[10] *See, e.g.*, STANFORD MED., STANFORD MEDICINE 2017 HEALTH TRENDS REPORT: HARNESSING THE POWER OF DATA IN HEALTH 14-15 (2017) [hereinafter HEALTH TRENDS REPORT].

[11] NATIONAL INSTITUTE OF HEALTH, ALL OF US RESEARCH PROGRAM OPERATIONAL PROTOCOL 5 (March 28, 2018), https://allofus.nih.gov/.

[12] Lothar Determann, *Healthy Data Protection*, 26 MICH. TELECOMM. & TECH. L. REV. 229, 234 (2020), https://repository.law.umich.edu/mtlr/vol26/iss2/3 [hereinafter Determann, *Healthy Data Protection*]

[13] For an overview of CIS, see Donte, What Is A Clinical Information System (CIS)?, BIOHEALTHMATICS (June 19, 2018), http://www.biohealthmatics.com/technologies/hospitalinformation-systems/clinical-information-systems.

[14] Determann, *Healthy Data Protection*, *supra* note 12, at 234–35; Oleg Bestsennyy, Greg Gilbert, Alex Harris, & Jennifer Rost, *Telehealth: A Quarter-Trillion-Dollar Post-COVID-19 Reality?*, MCKINSEY & CO. (July 9, 2021), https://www.mckinsey.com/industries/healthcare-systems-and-services/our-insights/telehealth-a-quarter-trillion-dollar-post-covid-19-reality (Telemedicine has increased about 38x compared to before the COVID-19 pandemic).

[15] *See, e.g.*, HEALTH TRENDS REPORT, *supra* note 10, at 5.

(IoT).[16] Healthcare uses IoT for everything from tracking patient outcomes to tracking physical assets such as wheelchairs within the hospital.[17]

All of this trends towards more personalized medicine and treatment plans that are tailored to the patient's specific life circumstances, environmental factors, and even their biological or genetic predispositions.[18] This increase in the collection of data offers the healthcare industry the opportunity to improve the analysis of disease factors, to improve diagnostic methods, and to increase the chances of finding cures. Furthermore, this increase in data could possibly reduce medical costs and increase the healthcare system's efficiency.[19] However, the increased value of this data comes with increased risk for the data processor due to the regulations regarding protected data, and increased risk for the individual that could result in identity theft, stigmatization, discrimination, or even blackmail.[20]

Though the global healthcare industry is estimated to reach over eleven trillion dollars by 2022,[21] the regulations on PHI or personal data and the risks associated with handling this data can disincentivize new players in the market and the technological innovation they can bring.[22] With regulations like the GDPR restricting data sharing, innovative start-ups or smaller research institutions cannot gain information from larger corporations that can bear the burden of compliance and potential fines.[23] Consequently, small tech start-ups and research institutions are limited to working within one country because of potentially exorbitant fines and difficulties inherent in complying with a wide variety of international regulations. Additionally, regulations prevent companies from sharing the wealth of data contained in biobanks, which are databases of

---

[16] *What is IoT?*, ORACLE, https://www.oracle.com/internet-of-things/what-is-iot/ (last visited Oct. 25, 2021).

[17] *Id.*

[18] Determann, *Healthy Data Protection*, *supra* note 12, at 234–35; Wullianallur Raghupathi & Viju Raghupathi, *Big Data Analytics in Healthcare: Promise and Potential*, 2 HEALTH INFO. SCI. & SYS. 1, 1–2 (2014).

[19] In 2011, a McKinsey Global Institute report estimated that big data in the U.S. healthcare system alone could provide over $100 billion per year just in cost reductions. *See* J. MANYIKA ET AL., BIG DATA: THE NEXT FRONTIER FOR INNOVATION, COMPETITION, AND PRODUCTIVITY 2, 7 (McKinsey Global Institute 2011).

[20] *See generally* Kat Jercich, *The Biggest Healthcare Data Breaches Reported in 2020*, HEALTHCARE IT NEWS (Dec. 30, 2020), https://www.healthcareitnews.com/news/biggest-healthcare-data-breaches-reported-2020. I elaborate on these risks in Part III of this Comment.

[21] Laura Wood, *The $11.9 Trillion Global Healthcare Market: Key Opportunities & Strategies (2014-2022) – ResearchAndMarkets.com*, BUSINESSWIRE (June 25, 2019, 01:35 PM), https://www.businesswire.com/news/home/20190625005862/en/The-11.9-Trillion-Global-Healthcare-Market-Key-Opportunities-Strategies-2014-2022—-ResearchAndMarkets.com.

[22] Determann, *Healthy Data Protection*, *supra* note 12, at 270.

[23] *Id.* at 270; Wolford, *What is GDPR*, *supra* note 7.

biological and genetic material.[24] Smaller companies, therefore, have little to no access to the existing anonymized data that could propel their research to new heights. For example, a company could not share its video footage of public roads with another company training autonomous vehicles without providing detailed privacy notices, seeking parental consent, and granting broad access and deletion rights under the EU's GDPR or the California Consumer Privacy Act (CCPA).[25]

In Part II, this Comment will discuss differences in the data protection regulations of various global healthcare industries by examining the policies of the United States, the European Union, the United Kingdom, Canada, and China.[26] Next, this Comment will discuss the benefits and detriments of these regulations on small healthcare companies and start-ups as they seek to provide business to these countries in accordance with individual regulations and the interactions between these countries. In Part III, this Comment will look at the risks to researchers, start-ups, medical professionals, and individuals posed by data breaches. Finally, this Comment will provide guidance on how to change data protection policies to encourage innovation within the global healthcare industry. This Comment will do so by calling for the reduction of penalties and fines, and the encouraging of data sharing; these reforms are meant to take the place of current regulations which have resulted in segmentation and high barriers to entry.

I. DATA PROTECTION REGULATION AND PATIENT PROTECTIONS

The protection of data and privacy is a global issue in our connected world. There are many international treaties and national constitutions that express or imply that privacy is a core principle or objective.[27] How the data is protected, however, greatly differs by country and region. These differences are most apparent in health data protections. In Europe, the processing of health data is regulated by general, omnibus data processing regulations such as the GDPR. The United States, on the other hand, uses sector- and harm-specific privacy

---

[24] Determann, *Healthy Data Protection*, *supra* note 12, at 234, 270.

[25] *Id.* at 270.

[26] *See* Smiljanic Stasha, *The State of the Healthcare Industry – Statistics for 2021*, POLICYADVICE (Aug. 6, 2021), https://policyadvice.net/insurance/insights/healthcare-statistics/ (North America and Western Europe have the highest healthcare industry revenue and China has the largest population using connected health devices in the world).

[27] *See* Lothar Determann, *Privacy and Data Protection*, MOSCOW J. INT'L L. 18, 20–21 (2019).

laws.[28] Also, many countries require patient confidentiality by law or regulation as further protection for health data.

A. The United States

1. HIPAA and Other Federal Policies

The United States does not have any comprehensive federal legislation on privacy or data protection that can be compared to other regulations explored by this Comment.[29] Courts have found that the U.S. Constitution covers and protects certain aspects of privacy in its Fourth Amendment even though the document never explicitly uses the term "privacy."[30] Instead, the United States addresses the risks and harms to privacy via sector- and harm-specific privacy laws that are tailored to specific industries and risks.[31]

Outside of the healthcare field, there are a variety of different laws that discuss data privacy by industry. These include the Fair Credit Reporting Act (FCRA) for consumer reporting agencies, the Family Educational Rights and Privacy Act (FERPA) for student education records, the Gramm-Leach-Bliley Act (GLBA) for financial institutions, the Electronic Communications Privacy Act (ECPA) for wiretaps of phone calls and electronic data transmissions involving computers, the Children's Online Privacy Protection Rule (COPPA) for all privacy requirements pertaining to children under thirteen years of age, the Video Privacy Protection Act (VPPA) for protecting video rental records, and more.[32] It is easy to see how difficult it can be to understand the different data privacy laws and to know which ones are relevant to a particular product or service.

For health data protection, the Health Insurance Portability and Accountability Act of 1996 (HIPAA) is the ruling regulation.[33] HIPAA requires healthcare sector organizations to implement detailed technical and organizational security measures, disclose data processing practices to patients,

---

[28] Determann, *Healthy Data Protection*, *supra* note 12, at 236.

[29] *See* Paul M. Schwartz, *Preemption and Privacy*, 118 YALE L. J. 902, 910–16 (2009).

[30] *See, e.g.*, Carpenter v. United States, 138 S. Ct. 2206 (2018); Lawrence v. Texas, 539 U.S. 558 (2003); Griswold v. Connecticut, 381 U.S. 479 (1965).

[31] *See* DANIEL J. SOLOVE & PAUL M. SCWARTZ, INFORMATION PRIVACY LAW 257, 349–61 (5th ed. 2014); ANDREW B. SERWIN, INFORMATION SECURITY AND PRIVACY: A GUIDE TO FEDERAL AND STATE LAW AND COMPLIANCE §§ 7.1, 28 (2014).

[32] Thorin Klosowski, *The State of Consumer Data Privacy Laws in the US (And Why It Matters)*, N.Y. TIMES (Sept. 6, 2021), https://www.nytimes.com/wirecutter/blog/state-of-privacy-laws-in-us/.

[33] OCR PRIVACY BRIEF, *supra* note 5.

and obtain consent in certain limited situations.[34] President Clinton, upon signing HIPAA into law, claimed the Act would "ensure the portability of health benefits when workers change or lose their jobs and [would] protect workers against discrimination by health plans based on their health status."[35] HIPAA defines covered entities as health plans, health care providers, and health care clearing houses.[36] Additionally, HIPAA requires specified written safeguards for a person or organization "that performs certain functions or activities on behalf of, or provides certain services to, a covered entity that involve the use or disclosure of individually identifiable health information."[37] These individuals or organizations are referred to as business associates and include any company that provides services such as electronic medical records (EMR) and electronic health records (EHR) such as EPIC, Cerner, and others.[38]

HIPAA defines protected health information (PHI) in its Privacy Rule from 45 C.F.R. § 160.103 as any information held by covered entities or business associates regarding health status, the provision of health care, or health care payments that can be linked to any individual.[39] The disclosure of such information is authorized by patients' express written authorization,[40] though there are some exceptions for specific circumstances such as a legally required disclosure.[41] Importantly, under HIPAA, patients have the right to access their health data at any time. However, unlike patients in some other countries, patients in the United States do not have the right to erasure.[42]

The Federal Policy for the Protection of Human Subjects, also known as the "Common Rule," supplements HIPAA.[43] This policy was published in 1991 and revised in 2017. It sets the standards for "all research involving human subjects conducted, supported, or otherwise subject to regulation by any Federal

---

[34] *Id.*

[35] William J. Clinton, *Statement on Signing the Health Insurance Portability and Accountability Act of 1996*, AMERICAN PRESIDENCY PROJECT (Aug. 21, 1996), www.presidency.ucsb.edu/documents/statement-signing-the-health-insurance-portability-and-accountability-act-1996.

[36] OCR PRIVACY BRIEF, *supra* note 5, at 2–3.

[37] *Id.* at 3.

[38] Marla Durben Hirsch, *Editor's Corner: HER Vendor Business Associate Agreements Still Skewed Against Providers*, FIERCE HEALTHCARE (Oct. 11, 2016), https://www.fiercehealthcare.com/it/ehr-vendor-business-associate-agreements-still-skewed-against-providers.

[39] 45 C.F.R. § 160.103 (2021).

[40] 45 C.F.R. § 164.508(a) (2021).

[41] 45 C.F.R. § 164.502(a)(2) (2021).

[42] Stacey A. Tovino, *The HIPAA Privacy Rule and the EU GDPR: Illustrative Comparisons*, 47 SETON HALL L. REV. 973, 990 (2017).

[43] 45 C.F.R. § 46.101(a) (2021).

department or agency."[44] Therefore, all companies whose research involves identifiable data about living individuals and is conducted, funded, or regulated by Common Rule departments or agencies must submit a written assurance of compliance with the Common Rule to the head of a department or agency.[45] The study has to also be reviewed by the Institutional Review Board (IRB)[46] at least once a year.[47] The IRB ensures that the data subjects' risks are minimized and researchers have obtained informed consent.[48] Should the IRB find non-compliance, the funding of a study or its approval may be terminated.[49] However, outside of terminating a study's funding or approval, the Common Rule does not grant any legal remedies to research participants who participate in the study.[50] Additionally, certain low-risk studies conducted by HIPAA-covered entities are exempted from the Common Rule.[51]

2. State Regulations

In addition to HIPAA, the Common Rule, and other industry-specific privacy laws at the federal level, there are numerous state laws in the United States. In particular, California has led the way in data privacy legislation and regulation.[52] For health data, the Confidentiality of Medical Information Act (CMIA), issued by California, categorizes providers of software, hardware, and online services as "providers of healthcare," rather than just business associates as HIPAA does.[53] The CMIA also provides that "a provider of health care, health care service plan, or contractor" is not allowed to "disclose medical information regarding a patient," unless the disclosure is authorized by the patient.[54]

In addition to the CMIA, California passed the CCPA on June 28, 2018, and it came into effect on January 1, 2020.[55] The CCPA affects most businesses in

---

[44] *Id.*

[45] 45 C.F.R. § 46.103(a) (2021).

[46] 45 C.F.R. § 46.107 (2021). An IRB has to have at least five members of varying backgrounds, at least one scientific and non-scientific member and at least one nonaffiliated with the institution. *See id.*

[47] The definitions of "research" and "human subject" are available in 45 C.F.R. § 46.102(1) (2021) and 45 C.F.R. § 46.102(e)(1) (2021), respectively.

[48] 45 C.F.R. § 46 (2021).

[49] 45 C.F.R. §§ 46.123, 46.113 (2021).

[50] Jessica L Roberts & Valerie Gutmann Koch, *Law vs. Regulations in the Common Rule*, YALE J. L. & TECH. BLOG (Jan. 6, 2016), https://yjolt.org/blog/law-vs-regulations-common-rule.

[51] 45 C.F.R. § 46.104(d)(4) (2021).

[52] CAL. CIV. CODE § 56 (West 2021); California Consumer Privacy Act, CAL. CIV. CODE § 1798 (West 2021).

[53] CAL. CIV. CODE § 56 (West 2021).

[54] CAL. CIV. CODE § 56.10(a) (West 2021).

[55] Lothar Determann, *New California Law Against Data Sharing*, 35 COMPUT. & INTERNET L. 1, 2 (2018).

the world because any business is covered if it does business remotely or physically in California, obtains any California resident's personal information, and exceeds one of the following three thresholds: (1) generates annual gross revenues of $25 million; (2) processes personal information of 50,000 or more California residents, households, or devices annually; or (3) generates fifty percent of annual revenue from selling California residents' personal information.[56] The CCPA defines "personal information" more broadly than any other U.S. regulation, as it includes any "information that . . . relates to . . . a particular consumer or household."[57] Further, the CCPA defines "selling" as any disclosure or provision of personal information for monetary or other valuable consideration.[58] "Consumer" under the CCPA refers to any resident, including employees, business representatives, students, or patients.[59] In order to comply with the CCPA, businesses must use precise language and organization as outlined in the statute for disclosures, implement an online opt-out link to enable consumers to prohibit the sale of their personal information,[60] and grant new data subject rights, including access, erasure, and portability.[61]

The CCPA continues to cover businesses or entities governed by HIPAA or CMIA even when they do not act as a "covered entity" or a "provider of healthcare," or when they process data that does not qualify as PHI under HIPAA or medical information under CMIA.[62] Consequently, healthcare providers and other businesses within the healthcare industry must comply with the CCPA and its data sharing restrictions in addition to the restrictions created by HIPAA and CMIA.

B. The European Union

Unlike the United States, European countries focus their data protection laws on protecting the individual from the potential adverse effects of automated data processing by generally prohibiting the processing of personal data and allowing data processing only within certain enumerated exceptions. In response to the need for modern data protections, the EU passed the General Data Protection

---

[56] *Id.*; California Consumer Privacy Act, CAL. CIV. CODE § 1798.140(c)(1) (West 2021).

[57] California Consumer Privacy Act, CAL. CIV. CODE § 1798.140(o)(1) (West 2021).

[58] CAL. CIV. CODE § 1798.140(t); Determann, *Healthy Data Protection*, *supra* note 12, at 243 ("This definition of selling thus covers most types of data exchanges in practice, given that businesses tend to share information only for consideration and consideration is a basic element of any contract").

[59] CAL. CIV. CODE §1798.140(g).

[60] CAL. CIV. CODE §1798.135(a)(1).

[61] CAL. CIV. CODE §1798.100, 105.

[62] CAL. CIV. CODE §1798.145(c).

Regulation 2016/679 (GDPR) which went into effect on May 25, 2018.[63] This regulation is applicable to member states of the European Economic Area (EEA) and generally applies to companies within and outside the EEA when the controller, processor, or data subject is based in the EU.[64]

According to the GDPR, organizations cannot process personal data unless they can provide a justification recognized by law.[65] This is the opposite of the general presumption of liberty in which everything is allowed if not prohibited.[66] The GDPR requires organizations to meet all regulation requirements and national laws and to claim one of the six "legal bases" for processing data: (a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes; (b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; (c) processing is necessary for compliance with a legal obligation of the data subject or of another natural person; (d) processing is necessary in order to protect the vital interests of the data subject or of another natural person; (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; or (f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.[67]

For consent to be valid according to the first legal basis, it must be a "freely given, specific, informed and unambiguous indication of the data subject's wishes" and she must signify agreement "by a statement or by a clear affirmative action . . . to the processing of personal data relating to him or her."[68] Article 7 of the GDPR notes additional requirements for consent. The most important ones require respective declarations to be unambiguous and based on clear and easily accessible requests for consent, and consent to be revocable at any time.[69]

---

[63] Wolford, *supra* note 7.

[64] A controller being a "natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data" and the processor is a "natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller." Council Regulation 2016/679, art. 44(7)-(8), 2016 O.J. (L 119/32–33).

[65] Wolford, *supra* note 7.

[66] *See* Jeremy Waldron, *The Rule of Law*, STAN. ENCYC. PHIL. (June 22, 2016), https://plato.stanford.edu/entries/rule-of-law/.

[67] Council Regulation 2016/679, art. 6(1), 2016 O.J. (L. 119/36).

[68] *Id.* art. 4(11).

[69] Determann, *Healthy Data Protection*, *supra* note 12, at 237.

"Personal data" under the GDPR includes any information related to an identified or identifiable data subject "who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person."[70] This definition means that data is covered by this regulation when it *can* be associated with an identifiable person even when the data itself does not to identify a data subject.[71] The Court of Justice of the European Union has affirmed this understanding, stating that data can be considered personal if the company or body collecting the data in question "has the legal means which enable it to identify the data subject with additional data which the [company or body] has about that person."[72] Data ceases to be personal only when it is appropriately anonymized or aggregated so that it can no longer be associated with an identifiable individual.[73]

The GDPR's definition of "processing of personal data" is broadly defined, much like its definition of personal data. Processing can mean "any operation . . . which is performed on personal data [. . .] , whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction."[74] Additionally, any data processing is subject to extensive restrictions because of GDPR's principles related to the processing of personal data, which are the principles of (a) lawfulness, fairness and transparency; (b) purpose limitation; (c) data minimisation; (d) accuracy; (e) storage limitation; and (f) integrity and confidentiality.[75] These principles taken together communicate that all data processing must be lawful and transparent, restricted to the express purpose, limited to only what is necessary for the purpose, accurate and up-to-date, kept in storage only as long as necessary for the purpose, and processed with appropriate security and protection.

However, the goals of "big data" are diametrically opposed by the GDPR principles. While "big data" relies upon large volumes of data to be frequently collected and then analyzed for new insights or connections *apart* from the original purpose, the GDPR principles require only the *minimum* amount of data

---

70 Council Regulation 2016/679, art. 4(1), 2016 O.J. (L. 119/36).

71 *Id.*

72 *See* Case C-582/14, Beyer v. Bundessrepublik Deutschland, 2016 E.C.J. I-779.

73 For more about anonymization and aggregation requirements, see *infra* Part III(A)(1) of this Comment.

74 Council Regulation 2016/679, art. 4(2), 2016 O.J. (L. 119/36).

75 *See* Council Regulation 2016/679, art. 5(1), 2016 O.J. (L. 119/36) (for specifics regarding the principles).

to be collected and analyzed *expressly* for the original purpose with which consent was gained.[76] For example, big data could be used to find a correlation between the location and development of certain diseases within a population, but the GDPR would prevent this discovery unless the data was originally collected for that specific purpose.[77]

In addition to increased restrictions on data processing, the GDPR differs from the U.S. regulations in that the GDPR grants more rights to data subjects affected by data processing.[78] The GDPR provides the right to disclosures and access, which means the data subjects must be informed if their data is processed, about which data in particular is being processed, about the purposes of the data processing, and about the recipients of the processed data.[79] Further, the GDPR provides the right of rectification, data portability, and erasure.[80] One of the most important differences between the rights provided under the GDPR and HIPAA is the right to erasure. EU law states that an entity, which relied upon patient consent to collect data, will lose the legal basis for retaining such data if the data subject withdraws his or her consent. EU law also entitles patients to withdraw consent at any time, though there are certain exceptions, such as for public health and scientific research.[81]

Perhaps most importantly for companies is the GDPR restrictions on the transfer of data abroad. Cross-border transfers of data can be of significant importance for global medical studies, international research projects, and international companies.[82] However, the cross-border transfer of data is generally prohibited by Chapter V of the GDPR, and this restriction is subject only to some complex and narrow exceptions.[83] Under these policies, the EU determines if the country that is not a part of the EU has an "adequate" level of data protection; in practice, the EU has only approved a limited selection of countries for data transfer.[84] So far, EU has only made positive adequacy decisions regarding Andorra, Argentina, Canada, Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland, the United

---

76 *See* Laney, *supra* note 9; Council Regulation 2016/679, art. 5(1), 2016 O.J. (L.119/36).
77 Council Regulation 2016/679, art. 5(1), 2016 O.J. (L. 119/36).
78 *Id.* art. 15(1).
79 *Id.*
80 *Id.* arts. 16–17, 20.
81 Council Regulation 2016/679, 2016 O.J. (L. 119/36).
82 *See id.*
83 *Id.*
84 Determann, *supra* note 12, at 239.

Kingdom, and Uruguay.[85] The United States' regulations do not meet the EU's adequacy requirements. Instead, companies based in the United States can voluntarily register under the EU-U.S. Privacy Shield program.[86] However, the Privacy Shield has limited usefulness for many exchanges of healthcare data between the United States and the European Union because many U.S. health care providers and payors are excluded from its terms.[87] The Privacy Shield is only an option for those organizations subject to the jurisdiction of the Federal Trade Commission (FTC) or the Department of Transportation.[88] Generally, insurance companies in the United States are regulated primarily by state insurance commissioners, and not the FTC.[89] Further, the FTC's jurisdiction does not generally cover nonprofit entities. Consequently, health care providers, hospitals, and other care organizations that operate as non-profits or through insurance companies regulated by state insurance commissioners may be excluded from the Privacy Shield's framework.[90]

The Privacy Shield also places asymmetric burdens on controllers in the United States when compared to those expected of controllers native to the EU. Under the GDPR, EU controllers can process health data under an independent lawful basis for the purposes of treatment, social care, public health, or medical research.[91] In contrast, U.S. controllers must comply, under the Privacy Shield, with detailed and untested requirements regarding the explicit consent of data subjects, even for public health and medical research purposes.[92] The Privacy Shield does offer very narrow exceptions pertaining to the processing of data for direct "medical care and diagnosis" or research done specifically by "non-profit entities."[93] The practical impact of this asymmetric burden is that U.S. research entities must bear the brunt of compliance burdens that are heavier than those borne by their EU counterparts, thereby hindering cross-border research and

---

[85] *Adequacy Decisions: How The EU Determines if a Non-EU Country has an Adequate Level of Data Protection*, EURO. COMM'N [hereinafter *Adequacy Decisions*], https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en (the United Kingdom is considered adequate under the GDPR and Law Enforcement Directive).

[86] Determann, *Healthy Data Protection*, *supra* note 12, at 239.

[87] Laura Bradford, *International Transfers of Health Data Between the EU and USA: A Sector-Specific Approach for the USA to Ensure an 'Adequate' Level of Protection*, 7 J. L. & BIOSCIENCES 1, 19 (2020).

[88] *Id.*; European Commission, Commission Implementing Decision (EU) 2016/1250 of July 2016, 2016 O.J. (L 207) 11.

[89] Bradford, *supra* note 87, at 19.

[90] *Id.*

[91] Council Regulation 2016/679, 2016 O.J. (L. 119/36).

[92] Bradford, *supra* note 87, at 19.

[93] UNITED STATES DEPARTMENT OF COMMERCE, EU-U.S. PRIVACY SHIELD FRAMEWORK PRINCIPLES ISSUED BY THE U.S. DEPARTMENT OF COMMERCE 14, https://www.privacyshield.gov/article?id=14-Pharmaceutical-and-Medical-Product; Council Regulation 2016/679, 2016 O.J. (L. 119/36).

innovation.[94] However, the Privacy Shield also lacks the organizational and technological safeguards set out in the GDPR, so it creates undue burdens on U.S. health research, while remaining unduly lenient on actual patient protections involving the use of health data.[95]

Also, the GDPR considers health data to be a "special category" that includes all "personal data related to the physical or mental health of a natural person, including the provision of health care services which reveal information about his or her health status."[96] The processing of health data is prohibited unless the processing is necessary for health or medical purposes, or if explicit consent is given for one or more specified purposes.[97] However, the GDPR does not differentiate between severity within the health data category; a bandage visible on security footage is treated identically to more specific health data such as treatment plans or diagnoses.[98] However, the GDPR allows some leeway for EU Member States to legislate derogations from the GDPR; this policy creates a legal patchwork that makes it more difficult for research institutions and companies to conduct international studies or exchange data across borders.[99] Additionally, treating physicians and researchers have to comply with EU regulations on Clinical Trials on Medicinal Products for Human Use, which standardizes authorization procedures, safety necessities, and requirements for consent to participate in clinical trials, thereby further complicating requirements related to the use and sharing of data from clinical trials.[100]

Violations of the GDPR cause devastating fines and can apply to companies outside of the EU as long as the company either processes the personal data of EU citizens or residents, or offers goods or services to such people.[101] There are two tiers of penalties, which max out at twenty million euros or four percent of the company's global revenue (whichever is higher); also, data subjects have the right to seek compensation for damages beyond the fine.[102]

---

94 *Id.* (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 scientic research subject to safeguard).

95 Bradford, *supra* note 87, at 20.

96 *See Guidelines 2/2018 on Derogations of Article 49 Under Regulation 2016/679*, EUR. DATA PROT. BD. (May 25, 2018), http://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_2_2018_derogations_en.pdf; Council Regulation 2016/679, 2016 O.J. (L. 119/36).

97 *Id.*

98 Council Regulation 2016/679, 2016 O.J. (L. 119/36).

99 Determann, *supra* note 12, at 241.

100 Council Regulation 536/2014, 2014 O.J. (L. 158).

101 *See generally* Wolford, *supra* note 7.

102 *Id.*

C. The United Kingdom

Prior to Brexit on January 31, 2020, the United Kingdom was a part of the EU and followed the GDPR.[103] The United Kingdom implemented EU regulations through its own legislation and incorporated the GDPR as the Data Protection Act (DPA) of 2018.[104] The DPA continues to be the data protection law of the United Kingdom, even though it has key differences from the EU's GDPR. The significant differences between the GDPR and DPA are that the DPA: (1) lowers the data processing age of consent from sixteen to thirteen; (2) changes the definition of "identifier" to be much more limited when compared to the GDPR's definition; (3) does not require the processor to have official authority; (4) allows the organization to potentially ignore the rights of the data subjects if these rights would "seriously impact an organisation's ability to carry out their functions when processing data for scientific, historical, statistical and archiving purposes."[105] Generally, the DPA is wider in scope than the GDPR, but is considered "adequate" by the EU Commission.[106]

D. Canada

Canada's main data privacy regulation is called the Personal Information Protection and Electronic Documents Act (PIPEDA), and it applies to all personal data, including health data.[107] PIPEDA, however, is not necessarily the only law to consider when conducting data processing. PIPEDA allows each Canadian province to have different laws as long as the provincial laws are "substantially similar" to PIPEDA.[108] Currently, Alberta, British Columbia, Nova Scotia, and Quebec have established their own data privacy laws.[109] However, regardless of whether a province has its own law, all personal information that crosses international borders is subject to PIPEDA.[110] PIPEDA further complicates efforts to transfer health data across borders, because PIPEDA does not define health data in any way; instead, it is only differentiated

---

[103] *Data Protection*, GOV.UK, https://www.gov.uk/data-protection; *Brexit: What You Need to Know About the UK Leaving the EU*, BBC (Dec. 30, 2020), https://www.bbc.com/news/uk-politics-32810887.

[104] *Data Protection*, *supra* note 103.

[105] *What is the Difference Between the DPA 2018 and the GDPR? (and Why Does It Matter?)*, DPO CENTRE (Dec. 7, 2018), https://www.dpocentre.com/difference-dpa-2018-and-gdpr/.

[106] *Adequacy Decisions*, *supra* note *85*.

[107] *PIPEDA in Brief*, OFF. PRIV. COMM'R CANADA (May 2019), https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda_brief/.

[108] *Id.*

[109] *Id.*

[110] *Id.*

by provincial health privacy laws.[111] British Columbia's and Nova Scotia's provincial laws do not allow their residents' health data to be stored in the United States, even if the data is encrypted and otherwise compliant with PIPEDA.[112] The combination of PIPEDA and provincial data protection laws makes cross-border data transfer with Canada either complicated or impossible, thereby restricting the innovations that can be brought to Canada in their early stages.

E. China

In China, data protection and data privacy laws are relatively new, following a period of technological growth. The personal data of more than a billion citizens was available for collection and processing by Chinese researchers and businesses without any restrictions, unlike in Europe or the United States.[113] While western governments focused on individual privacy and regulations, the Chinese government encouraged the growth of domestic technology companies to advance and lead the technology market.[114] However, by 2017, China changed its focus to data privacy and protection by bringing the Chinese Cybersecurity Law (CSL) into effect, and this law was followed by the Personal Information Security Specification (PI Security Specification).[115]

The standing committee passed a brand-new regulation on August 20, 2021, and it went into effect on November 1, 2021. The regulation is called the Personal Information Protection Law (PIPL), and it is meant to replace the CSL.[116] The PIPL focuses on the entities that process personal identifiable information (PII) and is similar in scope to the GDPR.[117] The PIPL adds additional rights to individuals in China that were not present under the CSL, including the right to edit, remove, restrict use, or withdraw consent given previously.[118] Like the GDPR and the CCPA, the PIPL exerts extraterritorial jurisdiction over data processing activities outside China when the purpose of these activities is to provide products or services to individuals located in China,

---

111 *Id.*

112 *What You Need to Know About HIPAA and Canada Health Information Privacy*, VSEE (Jan. 20, 2017), https://vsee.com/blog/hipaa-canada-health-information-privacy/.

113 *See* Luxia Zhang et al., *Big Data and Medical Research in China*, BMJ 3 (Feb. 5, 2018).

114 Meng Jing & Sarah Dai, *China Recruits Baidu, Alibaba and Tencent to AI "National Team,"* S. CHINA MORNING POST (Nov. 21, 2017), https://www.scmp.com/tech/chinatech/article/2120913/china-recruits-baidu-alibaba-and-tencent-ai-national-team.

115 Determann, *Healthy Data Protection*, *supra* note 12, at 245.

116 *See generally* Liao, *supra* note 8.

117 DELOITTE, CHINA DRAFT PERSONAL INFORMATION PROTECTION LAW (PIPL): GENERAL INTRODUCTION AND IMPACT ANALYSIS 1 (2021).

118 *Id.*

or to analyze or assess the behaviors of individuals located in China.[119] Prior to the PIPL, extraterritorial jurisdiction was only provided in draft regulations or national guidelines that had no binding effect.[120]

Similarly to the GDPR, the PIPL specifies additional lawful bases as binding law and provides that consent is not required for: (1) performing a contract where the data subject is a party to that contract or where necessary for the implementation of human resources management; (2) fulfilling statutory duties or obligations; (3) responding to sudden public health incidents or protecting individuals' lives, health, or properties under emergency conditions; (4) acting in the public interest for news reporting and media supervision within a reasonable scope; or (5) processing personal information disclosed by data subjects or other legally disclosed personal information within a reasonable scope.[121]

For cross-border data transfer, the PIPL actually creates an option for certain companies that allows them to be exempted from the onerous procedure of conducting government security assessments. They can obtain this exemption by either obtaining a personal information protection certification awarded by a professional institution or by signing a standard contract formulated by the Cyberspace Administration of China (CAC).[122] The PIPL also enhances the informed consent requirements for cross-border data transfers by requiring data controllers to inform data subjects of the overseas recipient's name, their contact information, the processing purpose and method, the types of personal information to be disclosed, and the ways and procedures with which data subjects can exercise their rights under the PIPL with the recipient overseas.[123]

Finally, the PIPL increases penalties for noncompliance like the GDPR. Previously, under the CSL, the capped penalty was approximately $149,000; the PIPL increases the maximum penalty to approximately $7,456,000 or five percent of the company's turnover in the last year.[124]

---

119 *See generally* Liao, *supra* note 8.
120 *Id.*
121 *Id.*
122 *Id.*
123 *Id.*
124 *Id.*

II. BENEFITS AND RISKS OF DATA PROCESSING AND SHARING

A. Benefits and Risks for Researchers, Start-Ups, and Medical Professionals

Researchers, medical professionals, and start-up employees face numerous risks when processing patient or health data. Modern medicine requires large amounts of data for treatment, prevention, and medical research. Increasing available data can lead to more effective treatment and prevention options.[125] Without access to data, medical professionals may have to rerun tests or delay treatment until the data is acquired directly from the patient and not from the vast amount of patient data that has already been collected. By restricting data sharing in the healthcare industry, global regulations slow down potential medical and scientific progress, because scientists and medical professionals have to repeat tests that have already been performed by others in another country. If health data could be shared internationally, then these consolidated data sets could be used to better understand diseases and determine common health factors, in ways that smaller data sets cannot accomplish effectively. One of the greatest examples of this involves genetics or genome mapping. Scientists, physicians, and even technology start-ups could find, diagnose, and treat genetic diseases more effectively by accessing genomic data globally.[126]

The recent COVID-19 pandemic, which began in 2019, is another example of how access to health data could be beneficial to international healthcare. While many countries were willing to send COVID-19 case data to the World Health Organization (WHO), each government authority could determine which data it sent and when this data was released.[127] If there were already channels for health information that allowed it to be sent throughout the globe to hospitals and national laboratories, then there might have been a quicker and more coordinated global response to COVID-19.

Additionally, by allowing the better sharing of health information, treating physicians can better tailor their treatments to patients by having access to their entire medical histories.[128] If a physician is seeing a new patient, he cannot

---

[125] *See* Nicholas J. Schork, Comment, *Time for OnePerson Trials*, 520 NATURE 609, 609 (2015) (noting that there are a significant amount of people who take medication that does not benefit them).

[126] Determann, *Healthy Data Protection*, *supra* note 12, at 235.

[127] Erwin Calgua, *COVID-19: Data collection and transparency among countries*, COVID-19 PANDEMIC, 163, 164 (2022).

[128] Nir Menachemi and Taleah H. Collum name several benefits of electronic health records, e.g., improved legal and regulatory compliance, improved ability to conduct research and increased job satisfaction among physicians. *See* Nir Menachemi & Taleah H. Collum, *Benefits and Drawbacks of Electronic Health Record Systems*, 4 RISK MGMT. & HEALTHCARE POL'Y 47, 47, 50 (2011).

assume that the new patient will reliably transmit all the necessary or helpful details of his habits, symptoms, prior treatments, test results, and other relevant subjects.[129] Many patients might conceal negative habits, such as drinking or eating habits, exaggerate exercise habits, or simply forget details that would be included in their medical histories.[130]

Attempting to do business in multiple countries opens healthcare companies up to additional risks, because their operations now require knowledge of each additional country's data privacy regulations and other pertinent details such as requirements for specific informed consent.[131] With the possibility of heavy fines or other legal complications resulting from noncompliance, small companies or start-ups must invest more heavily in legal counsel or designate a Data Protection Officer to assist in compliance.[132] These regulations inhibit the global reach of medical researchers and start-ups that cannot afford to take these additional steps.

Even if researchers, start-ups, or medical professionals have the resources to invest in global data processing, the risk of inadvertent disclosure is still very relevant. An inadvertent disclosure could be something as simple as accidentally revealing the email addresses of data subjects by using To or CC instead of BCC when sending an email.[133] Using internet or cloud storage creates additional access points for data, unlike relying on hardcopies that can be physically locked away.[134] As mentioned in Part II(B), certain research exemptions do not include U.S. entities unless they fall under the Privacy Shield.[135]

B. Risk Prevention for Researchers, Start-Ups, and Medical Professionals

Across the globe, healthcare providers and researchers rely on three measures to protect patient privacy: (1) limiting the use of health data to what is necessary to treat the patient; (2) redacting or aggregating information so that the individual cannot be identified or associated with the data; and (3) obtaining patient consent for additional data usages.[136] While patients and their privacy

---

[129] Determann, *Healthy Data Protection*, *supra* note 12, at 263.

[130] *Id.*

[131] Bradford, *supra* note 87, at 9.

[132] *See generally* Wolford, *What is GDPR*, *supra* note 7.

[133] Complaint, Eli Lilly & Co., C-4047, at ¶ 6 (Fed. Trade Comm'n May 8, 2002).

[134] Maria Eduarda Conçalves, *Over Troubled Water: E-Health Platforms and the Protection of Personal Data: The Case of Portugal*, 35 PORT. J. PUB. HEALTH 52, 58 (2017).

[135] Bradford, *supra* note 87, at 11.

[136] *See* Naya Sethi & Graeme T. Laurie, *Delivering Proportionate Governance in the Era of eHealth: Making Linkage and Privacy Work Together*, 13 MED. L. INT. 168 (2013).

can be protected by any combination of these methods, there have been questions regarding the efficacy of anonymization and consent as a result of the acquisition and processing of ever-larger amounts of health data in the age of modern medicine.[137]

1. Anonymization

Anonymizing data means to "remove identifying information from (something, such as computer data) so that the original source cannot be known."[138] Anonymization is a common way to gather data without the same risks associated with identifiable data; it is frequently referenced in privacy policies and consent forms, and yet anonymization is rarely included in statutes.[139] Depending on the regulation, other terms may be used for a similar concept. In the GDPR, the term used is "pseudonymization," and it is defined as:

> "the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person."[140]

The GDPR refers to pseudonymization throughout as a recommended data security measure.[141]

The CCPA does not use the term "anonymization" either; instead, it uses the terms "deidentification" and "aggregation."[142] Aggregation of consumer information refers to another system of anonymizing information that "relates to a group or category of consumers, from which individual consumer identities have been removed, that is not linked or reasonable linkable to any consumer or household, including via a device;" this definition does not necessarily mean "one or more individual consumer records that have been deidentified," as it requires a definable group or category of consumers.[143] Generally, aggregate

---

137 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 (2016).

138 *Anonymize*, MERRIAM-WEBSTER, https://www.merriam-webster.com/dictionary/anonymize (last visited October 25, 2021).

139 Determann, *Healthy Data Protection*, *supra* note 12, at 247.

140 Council Regulation 2016/679, 2016 O.J. (L. 119/33-35).

141 Council Regulation 2016/679, 2016 O.J. (L. 119/33-35).

142 *See* CAL. CIV. CODE § 1798.140(o), (h).

143 *Id.*

information consists of statistical information regarding a large population of persons that does not provide or imply information on a specific individual.[144] Aggregate information and data generally fall outside the scope of the CCPA, GDPR, or other data privacy laws.

For many medical professionals, anonymization is not a valid option as it removes any personal connection by turning patients from individuals into data sets.[145] Additionally, laboratory values and test results only provide value to a diagnosis when they are connected to a patient, so anonymization of data is rarely possible when a medical diagnosis is necessary. However, lab reports or images often use partial redaction (e.g., replacing patient names with ID numbers), but there remains risk of identification using this process. There is always some trace of the deidentification process, as seen in the re-identification of the medical data of Massachusetts Governor William Weld in 1997.[146] Governor Weld collapsed during a public event and a researcher gained access to his medical records from a Massachusetts Group Insurance Commission database by using his zip code and birth date, two easily found data points.[147]

Medical research can have more use of aggregated or anonymized data by looking at general trends. However, even here the more individual data that can be provided leads to better value from the data. Each piece of information redacted can lessen the chance of finding the key factor linking the data sets, and redacting location may prevent researchers from finding that a specific area has a higher prevalence of a specific disease.

2. Consent

Consent-based data processing respects patient self-determination and autonomy and is based on the "underlying [] principle . . . that since individuals are rational moral agents, they should be in command of decisions that relate to *their* lives and bodies." [148] Historically, individual consent was primarily prevalent with respect to medical research and clinical trials, but, after significant medical advances, healthcare providers require significantly more

---

144 *E.g.*, X% of all citizens older than eighteen in country Y have been diagnosed with diabetes

145 Determann, *Healthy Data Protection*, *supra* note 12, at 248.

146 For a summary of the incident and critical view on the actual impact of the case on the anonymization debate, *see* Daniel C. Barth-Jones, The "Re-Identification" of Governor William Weld's Medical Information: A Critical Re-Examination of Health Data Identification Risks and Privacy Protections, Then and Now (2012) (unpublished manuscript) (available at SSRN: https://ssrn.com/abstract=2076397).

147 *Id.*

148 Gil Siegal, *Enabling Globalization of Health Care in the Information Technology Era: Telemedicine and the Medical World Wide Web*, 17 VA. J. L. & TECH. 1, 23–24 (2012).

data processing that require patient consent.[149] With the development of medical technology allowing for more interaction with patient or consumer data through developments such as fitness apps or telemedicine, legal consent is a vital concept for both physicians and healthcare business to understand.[150] Informed consent varies depending on the situation. To truly have informed consent, the patient must be informed of all risks and any additional relevant information; simply providing details does not mean that the patient is informed if they do not have the expertise, whereas they might understand more from a broader, more generalized explanation.[151] This type of fully informed consent, one that goes beyond simply giving detailed information to the data subject, is required by regulations such as the GDPR, which requires consent to be "freely given, specific, informed and unambiguous."[152]

Both telemedicine and conventional medicine utilize consent throughout every aspect. However, the more that telemedicine grows, the more likely that there will be a failure in communication regarding how data is maintained, stored, or accessed.[153] Currently, many institutions and practitioners outsource certain diagnostic services (e.g., sending x-rays to a radiologist that does not work for the institution) out-of-state or even to foreign countries without sharing this fact with the patient.[154] Institutions may use this method to cut down on costs of maintaining certain departments in-house; they often hide this fact for prestige, so that it is not well known that a prestigious hospital system outsources its radiology work.[155] The outsourcing may even include sending data abroad, such as when an x-ray is taken late at night in the United States, after which the test might be sent to Australia to be read by a radiologist there, rather than by a local (or in-house) radiologist.[156] This can mean that a patient may not even understand that their data is being sent from the hospital to another state or even country.

Furthermore, while this is certainly helpful for the hospital and the physicians that no longer have to wake up in the middle of the night, this greatly complicates potential legal remedies. For example, if a radiologist in Australia

---

149 *Id.*

150 Determann, *Healthy Data Protection*, *supra* note 12, at 252.

151 *Id.* at 252–53.

152 Wolford, *What is GDPR*, *supra* note 7.

153 Siegal, *supra* note 148, at 26.

154 *Id.*

155 *Id.*

156 Marianne Matthews, *Day for Night: The Development of Long-Distance Reading*, AXIS IMAGING NEWS (Nov. 3, 2002), https://axisimagingnews.com/radiology-products/imaging-equipment/ct/day-for-night-the-development-of-long-distance-reading.

makes an error and the patient chooses to sue for malpractice, there are now many questions regarding the choice of law, appropriate forum, and many more potential problems.[157] This is just another risk to medical professionals that would be most easily addressed by informed consent and, perhaps, a contract clarifying the issues mentioned above.

C. Risks to Individuals

While sharing personal data can help individuals receive more personalized care, there are risks inherent in sharing personal data. These include identity theft, stigmatization, discrimination, and many others.[158] The most private information is often health information, and sharing health data leaves patients at risk more than other types of data sharing.

When a criminal has access to medical records, identity theft or fraud require little effort, as the records may include names, addresses, social security numbers, family history, demographic data, insurance information, medications, and more.[159] In 2019, $16.9 billion were lost to identity fraud from 5.1% of consumers in all industries.[160] Medical records are often targeted for their wealth of data, and in 2016, there were nine times more medical records breached than financial records: 27 million, representing nearly ten percent of the U.S. population.[161]

Even without identity theft or fraud, a breach of personal data could cause an individual to become stigmatized due to his or her health record. This is especially true in the case of infectious diseases such as HIV,[162] mental health conditions such as depression or schizophrenia, addictions, and even cancer.[163] This stigmatization can come in the form of embarrassment, shame, or more severe social ramifications such as exclusion should sensitive medical

---

157 Siegal, *supra* note 148, at 32.

158 Determann, *Healthy Data Protection*, *supra* note 12, at 256-57.

159 Robert Lord, *The Real Threat Of Identity Theft Is In Your Medical Records, Not Credit Cards*, FORBES (Dec. 15, 2017), https://www.forbes.com/sites/forbestechcouncil/2017/12/15/the-real-threat-of-identity-theft-is-in-your-medical-records-not-credit-cards/?sh=6398c8ce1b59.

160 Krista Tedder & John Buzzard, *2020 Identity Fraud Study: Genesis of the Identity Fraud Crisis*, JAVELIN (Apr. 7, 2020), https://www.javelinstrategy.com/coverage-area/2020-identity-fraud-study-genesis-identity-fraud-crisis.

161 *Id.*

162 In 2019, the names, addresses, and HIV status of 14,200 people in Singapore were leaked. *Fury at HIV Data Leak in Conservative Singapore*, MED. EXPRESS (Feb. 10, 2019), https://medicalxpress.com/news/2019-02-fury-hiv-leak-singapore.html.

163 *See* J. Ernst et al., *Perceived Stigmatization and Its Impact on Quality of Life – Results from a Large Register-Based Study Including Breast, Colon, Prostate and Lung Cancer Patients*, 17 BMC CANCER 741 (2017).

information become public. While identity theft or fraud can be rectified by blocking access to a bank account or canceling a credit card, the harm caused by the public disclosure of a person's disease cannot be undone so easily; this accidental release of information may lead to further health conditions, such as a variety of psychosomatic symptoms.[164] Stigmatization is not only limited to medical information but can also come from the disclosure of political opinions, religion, race, or sexual preferences and cause the same feelings of embarrassment, shame, or social exclusion.[165]

A more serious form of stigmatization can stem from data breaches as well: discrimination.[166] Most notable of these is the potential for insurance discrimination through higher rates for health, life, or disability insurance or even complete rejection of insurance benefits if health information were to become public.[167] Additionally, employers could use the information to make adverse decisions regarding hiring, retaining, or promoting job candidates.[168] Banks may only grant loans to healthier individuals or adjust the interest rates to ensure the individual's contractual obligations could be met and housing rates could be more expensive if a landlord believes the health information revealed could impact the tenant's ability to pay rent.[169]

There are various other risks as well. These risks include blackmail, where a criminal may threaten to release information about the individual unless they are paid. The individual may wish to avoid the previously mentioned stigmatization. Another risk is directed marketing, where companies can use personal information to personalize advertisements or send items directly to the individual. While not overly harmful, it can be a breach of privacy and could alert others to a disease or condition if enough information is sent directly to the consumer. Also, the patient might be made aware of medical information that they were not ready to disclose, and, in some cases, this kind of premature disclosure could be to the patient themself. For example, a patient might be prematurely informed of a predisposition to a chronic disease that has no clear

---

164 Determann, *Healthy Data Protection*, *supra* note 12, at 257; Michael Koller et al., *Symptom Reporting in Cancer Patients: The Role of Negative Affect and Experienced Social Stigma*, 77 CANCER 983, 994 (1996).

165 Determann, *Healthy Data Protection*, *supra* note 12, at 256.

166 Benjamin E. Berkman et al., *The Ethics of Large-Scale Genomic Research*, *in* ETHICAL REASONING IN BIG DATA: AN EXPLANATORY ANALYSIS 53, 59; *see also* Ribhi Hazin et al., *Ethical, Legal, and Social Implications of Incorporating Genomic Information into Electronic Health Records*, 15 GENETICS IN MED. 810, 810-15 (2013).

167 Hazin et al., *supra* note 166, at 814.

168 Determann, *Healthy Data Protection*, *supra* note 12, at 258.

169 *Id.*

therapeutic or adoption status, both of which may appear in certain genomic tests.[170]

These risks are just some of the more apparent and frequent concerns about digitizing and transferring personal data. Concerns regarding these risks drive many data protection laws, including the GDPR and potential reforms in the United States. However, the benefits that can be gained from more freely moving and storing personal information can outweigh the risks if done properly.

III. IMPROVING DATA ACCESS POLICIES FOR HEALTHCARE AND TECH START-UPS

Despite the various risks to researchers, start-ups, medical professionals, and individuals, there are a large number of benefits available to all through data processing across international borders. Currently, small start-ups have difficulty shouldering the burdens of international data processing laws and regulations and are kept a step behind large corporations that are already in the space and can afford the required protections and possible fines. This section will explore the policy changes that would enable small start-ups and research institutions to work internationally by reducing penalties and encouraging data sharing, while maintaining protections for individual data rights.

A. International Policy and Reduction of Penalties

The first step needed to encourage the growth of start-ups and small research institutions in global healthcare is to reconsider the penalties for data breaches. Under the' GDPR, the first tier of fines is for violations to the obligations of the data controller or process and can lead to fines up to ten million euros or two percent of the total worldwide annual sales of the preceding financial year, whichever is higher.[171] The GDPR also doubles the maximum fine to the second tier of fines if there is a violation of the data subject's rights or failure to comply with an order of a supervising authority, increasing up to twenty million euros or up to four percent, whichever is higher.[172] This fine structure allows the fines to vary based on the severity of the violation and the size of the violating company or institution. At first glance, this seems to be perfectly reasonable as

---

[170] Ellen Wright Clayton, *Incidental Findings in Genetics Research Using Archived DNA*, 36 J. L. MED. & ETHICS 286 (2008); Elle Hunt, *Your Father's Not Your Father*, GUARDIAN (Sep. 18, 2018), https://www.theguardian.com/lifeandstyle/2018/sep/18/your-fathers-not-your-father-when-dna-tests-reveal-more-than-you-bargained-for.

[171] Wolford, *GDPR Fines*, *supra* note 4.

[172] *Id.*

the data protection regulator of each EU country can choose the amount and can use a percentage. However, as both levels of fines take the higher number, it may not be worth investing into the European Union as a smaller company as the company could be fined much higher than four percent of the previous year's worldwide annual sales, as long as it remained below twenty million euros. Additionally, while healthcare has only made up 3.41% of the fines from May 2018 to March 2021, the technology and telecoms industry has made up 46.10% of GDPR fines in that same time period.[173] This poses a high risk to upcoming technology start-ups who are considering entering the European Union to do business, even if they also are part of the healthcare industry. Additionally, as each country's DPA can make its own decisions regarding the fines, including whether to fine at all or issue warnings, there is more pressure on small companies to research and understand each individual country within the European Union, defeating much of the purpose of having the GDPR at all.[174]

Many US officials and industry representatives prefer the U.S. approach to data privacy, claiming that it is "more nimble" than the "EU's 'one-size-fits-all' approach."[175] By allowing more specific regulations for different sectors, the U.S. approach is more amenable to small technology firms, unlike the blanket approach of the GDPR and China's PIPL, which "stifle technology firms."[176]

However, the U.S. approach can certainly be considered a messier option. With many separate and conflicting data privacy laws at the federal level and the possibility of further laws and regulations added at the state level, there is much to be desired when looking to comply from an industry standpoint. The adjusting thresholds based on sector can allow smaller companies to more easily enter the market.

In order to develop international laws to best provide data protection and allow new businesses to start data processing, the international community needs to consider international data protection laws that are flexible for different sectors or industries. While the international community is trending towards similar comprehensive data regulations, as can be seen in the most recent laws passed such as the GDPR, CMIA, and PIPL, these all share a broad one-size-fits-all approach to data processing. In these regulations, all data processing is considered equal, no matter the purpose or potential benefits to processing or

---

173 Estelle Massé, THREE YEARS UNDER THE EU GDPR: AN IMPLEMENTATION PROGRESS REPORT 7 (2021).

174 *Id.* at 8–9.

175 Martin A. Weiss & Kristin Archik, US-EU Data Privacy: From Safe Harbor to Privacy Shield, Congressional Research Service 7-5700 R442574, 4 (May 19, 2016).

176 Bradford, *supra* note 87, at 15–16.

sharing data. Additionally, as these regulations are enacted in separate countries, a company may face fines in both countries for a single incident.

Instead, the international community should take many of the requirements from the GDPR and similar regulations but apply them through a combination of industry regulations (as seen in the United States) and data regulations. The new data regulations would consider the nature of the data to be processed or held as well as the planned use of the data. As such, data like names or addresses would have less stringent protections even though this data is identifying information. In contrast, more sensitive data, such as social security numbers or medical records, would have more stringent protections. In making these decisions, policy makers could also consider whether the data is to be stored, accessed by physicians, used for research and development, or employed for some other purpose. This perspective would create a modular system that adjusts the requirements and penalties based on the sensitivity and potential benefit of the data processing.

The most difficult part of such a modular system would be to enact an international treaty that countries would sign onto. This treaty would bind them to the rules and regulations specified and would be overseen by a supranational organization or perhaps overseen by the United Nations. This would also simplify the requirements for cross-border transfer of data, as the theoretical United Nations Data Processing Agency (UNDPA) would have jurisdiction and have set standard regulations in place. However, as with all international treaties, great care would need to go into the specifics. If the treaty's requirements were too lenient, then the data would not be adequately protected; if they are too strict, many countries would be unwilling to join.

Finally, this international regulation would have a maximum fine amount set with specific exceptions for blatant or willful disregard of the law. This allows companies to know their exact risk for processing data internationally while still allowing the organization to severely punish companies or institutions that willfully ignore the regulations.

B. Encouraging Data Sharing

The second step in adjusting the international policy would be to encourage data sharing between companies and institutions, rather than discouraging it as is done now. The level of restrictions within the regulations, especially the GDPR, discourages or actively prohibits the sharing of personal information. As data cannot be shared, innovative start-ups or smaller research institutions cannot access important sources of data that would greatly accelerate the

development of products, treatments, services, and research. In contrast, large companies continue to accumulate market power under this system. They can also use data privacy laws as an excuse to deny other organizations access to their data regardless of any conflicting competition laws.[177]

By adjusting the data privacy laws to allow companies to share data, start-ups and research institutions can access large sources of data. This can be actively encouraged by the data privacy laws themselves by creating incentives for large companies to securely share data in the form of tax breaks or another format, or these incentives could be folded in with competition laws to prevent a company from maintaining a monopoly within an industry simply due to their data sources. Countries can also use these incentives to help invigorate commerce and growth. By encouraging data sharing, a country would increase the desirability of collecting, storing, or processing data within its borders, both for new companies looking to access data otherwise difficult to obtain and larger companies that can take advantage of the tax breaks.

Neither individuals nor businesses should be granted proprietary rights to health data in order to promote innovation. By allowing patients or businesses to own health information, individuals could claim data in the face of free speech, information freedom, science, commerce, and technological progress.[178] Allowing patients to restrict access to their medical data by requiring financial compensation would increase the costs for all involved with the research and would further complicate the use of data, as each individual could claim a different contract for the use of their data. Any attempt to allow the purchase or sale of individual data would drive up the costs to research, produce, and sell diagnostics, products, and services within the medical industry. While data rights should be protected, it should not be through the ownership of data.

C. Ensuring Protection of Individual Data Rights

Despite the policies recommended above, which generally encourage the sharing and use of data, there is still a need to protect privacy and access to certain data to defend against the many risks discussed earlier.[179] As such, the protections for storing data must be kept at a high level, such as that required by the GDPR. The data privacy regulations, at least for medical records, should also encourage encryption over anonymization. Once data is anonymized, it is much less useful in the medical field, but by focusing spending on encryption that had

---

177 Determann, *Healthy Data Protection*, *supra* note 12, at 270.

178 Lothar Determann, *No One Owns Data*, 70 HASTINGS L. J. 1 (2018).

179 *See supra*, Part III.

previously been spent on anonymizing, the data can retain its usefulness while remaining secure from those who should not have access to the sensitive information. By spending more time and money on encryption, the data can be protected against breaches more effectively.

Another benefit of using a supranational organization such as the fictional UNDPA would be housing consent forms in one electronic database. Consent can remain an essential part of data privacy but needs to be simplified. By having a centralized location to give consent, an individual could use the UNDPA website to determine how she would like her data to be used, such as for medical research, only in emergencies, or otherwise, without having to communicate consent each time a company or entity desires to use her data. This would streamline the consent process for both individuals and data processors.

The system could even be expanded to a general health record for citizens of participating countries housed within the UNDPA. Some Scandinavian countries have already established similar systems, allowing citizens to access their complete health records online.[180]

To maintain simplicity, the laws protecting data privacy should not require entities to go into excruciating detail for every request for consent. If this were not handled in a centralized location as suggested, the regulation should encourage simple, easy-to-understand short forms for consent. It is likely that many individuals would only care about having their information secured and used only for a specific purpose; these people would likely not need a form providing legally mandated specificity to feel secure. A research exemption already exists only under the GDPR should an individual EU state wish to exempt certain medical data processing from restrictions, but it would be helpful to reduce legally mandated details. Consent could instead be provided in certain tiers allowing for levels of consent based on the expected use. These levels could be "broad" for expansive consent to data usage, "narrow" for only limited uses, or "sector-specific" if someone wanted to allow data processing only for medical purposes. However, the levels of consent would need to be consistent across countries, as there is no such consistency at this time.

In addition, there should be extensive free resources for businesses to access, since start-ups and small research institutions struggle "'to even understand where to start.'"[181] Due to the skill required to understand and implement data

[180] Determann, *Healthy Data Protection*, *supra* note 12, at 271.

[181] Chris Norval, *Data protection and tech startups: The need for attention, support, and scrutiny*, 13 POL'Y & INTERNET 278, 285 (2021).

protections, there is a large barrier to entry, due to both financial and knowledge restrictions. By creating more resources aimed at start-ups and small research institutions, a new company could follow clear and actionable steps in the form of a checklist, rather than muddling through the legal jargon of the regulation itself.

Another option to allow for better understanding of data privacy would be to require certifications for data storage, at least for the more sensitive levels of data such as medical records. This model would allow companies to take educational courses to better understand the steps needed to meet regulatory requirements. This would be particularly helpful to start-ups and small research institutions in making sure they can comply with the security requirements without having to invest as much into private assistance. To further help the public trust companies and research institutions with their data, there could be different levels of certifications to show how secure the data is kept. This could then tie into consent by allowing the public to choose a minimum level of certification to give consent to their data.

While this policy would maintain and even improve many security efforts, the right to deletion as specified under current data privacy laws such as the GDPR would likely have no place in this updated international policy. With a lower level of proprietary rights to data, individuals would not be able to reclaim their data once consent had been given. However, consent could be revoked at a later point, but only new data points would be affected by this change.

CONCLUSION

The future of both medicine and technology will be shaped by who can access the right data. Allowing new, innovative companies to have the same access to data as established corporations would increase competition and creativity within the marketplace, bettering everyone over time. By creating and investing in an international system for data privacy protection, all can reap the benefits of a reinvigorated push for new technologies and innovative medicines.

Overly protective data privacy laws can be harmful to health by becoming an obstacle to the process of treating a disease. While fear of stigmatization, discrimination, blackmail, and the other risks has resulted in a public push for stricter data protections, data processing is inherently necessary to better medicine and the lives of people across the globe. Potential privacy risks do not justify a reflexive call for increased restrictions on data processing, especially when the opportunities of medical data exchange are so great. Just as a ban on

cars would not be appropriate to prevent an increase in road deaths, neither would a ban on data processing be appropriate to prevent the potential risks. Instead, just as cars have continued with improved safety features, so should data processing continue with improved security.

RYAN PRESTON