# BARRIERS IMPACTING THE TRANSFER OF GENOMIC DATA BETWEEN THE U.S. AND THE U.K. FOR PRECISION ONCOLOGY RESEARCH

Brendan Cotta

## TABLE OF CONTENTS

## I. INTRODUCTION

Cancer treatments are getting increasingly more personalized, both to the individual and to the specific type of cancer being treated. No longer bound solely to a one-size-fits-all treatment approach, advancements in the field of precision oncology are allowing oncologists to fight cancer more safely and more effectively by utilizing information gained from a patient's own genomic data.[1]

Precision oncology is the cancer-focused subset of the larger precision medicine movement which is rapidly growing in popularity in the medical community. Precision medicine is defined by the National Cancer Institute (NCI) as "a form of medicine that uses information about a person's own genes or proteins to prevent, diagnose, or treat disease."[2] Cancers are "fundamentally diseases of the genome," and "understanding cancer begins by identifying the abnormal genes and proteins that confer the risk of developing cancer."[3] Vast amounts of genomic data are required in order to link specific genes and proteins to different cancers;[4] these links are then used to make precision oncology treatments as successful and personalized as possible. Pursuant to this goal, the National Cancer Institute has even been utilizing a portion of the funding provided by the Precision Medicine Initiative, a health initiative started by the Obama administration, to "[establish] a national database to house and integrate genomic information from tumors."[5]

The sheer amount of genomic data needed to conduct successful precision oncology research leads to issues when attempting to share information or conduct studies across international borders. This is due largely to significant differences in data protection laws between countries. This Note will look at what barriers arise when sharing information for research purposes between two countries on the forefront of precision oncology research: the U.S., operating under the Health Insurance Portability and Accountability Act (HIPAA), and the U.K., operating under the notably more protective General Data Protection Regulation (GDPR).[6]

To evaluate these barriers, this Note will begin by providing background information on the field of precision oncology and exploring the relevant differences in policy and structure between the HIPAA Privacy Rule and the GDPR, highlighting some of the fundamental differences which complicate and form barriers to the transfer of genomic data. It will then make a direct comparison between the HIPAA Privacy Rule and the GDPR, highlighting the different

---

1 *See NCI and the Precision Medicine Initiative*, NAT'L CANCER INST., https://www.cancer.gov/research/areas/treatment/pmi-oncology (last visited Oct. 17, 2021).

2 *Precision Medicine*, NCI DICTIONARY OF CANCER TERMS, https://www.cancer.gov/publications/dictionaries/cancer-terms/def/precision-medicine (last visited Oct. 15, 2021).

3 Harold Varmus, M.D., *Precision Medicine Initiative and Cancer Research*, NAT'L CANCER INST., https://www.cancer.gov/news-events/cancer-currents-blog/2015/precision-medicine-initiative-2016 (last visited Oct. 17, 2021).

4 *See NCI and the Precision Medicine Initiative*, *supra* note 1.

5 *NCI and the Precision Medicine Initiative*, *supra* note 1.

6 *See* Meg Leta Jones & Margot E. Kaminski, *An American's Guide to the GDPR*, 98 DENV. L. REV. 93 (2020).

components which form barriers when conducting precision medicine research and transferring genomic data. Finally, it will conclude with a look to the future, seeing what policy changes are already being made in the U.S., which are currently being considered, and what further changes could be made to improve the flow of genomic data and ease the conduct of research into this cutting edge and potentially life-saving field of medicine.

## II. BACKGROUND

### A. Precision Oncology

Developments in the field of precision oncology have revolutionized how we approach treating cancer. Precision oncology allows researchers to identify the "molecular fingerprints of various cancers and [use] them to divide [cancers] . . . into far more precise types and subtypes."[7] This enhanced understanding and classification of tumors allow physicians to tailor treatments "based on the DNA signature of an individual patient's tumor,"[8] with the overall goal of increasing treatment efficacy while reducing the occurrence of side effects and treatment resistance.

It's commonly said that the study of precision oncology originated in the late 1980s.[9] It was discovered that about a quarter of all breast cancer cases demonstrated an "amplification or overexpression of human epidermal growth factor-2 (HER2)"[10] and that "patients harboring such tumors had a poorer prognosis than those who did not."[11] This discovery, along with the realization that HER2 was a promising target for treatments, lead to the development of trastuzumab, a "critical, life-prolonging adjunct to chemotherapy in the metastatic, neoadjuvant, and adjuvant settings."[12] While trastuzumab was not a cure for breast cancer and did not, on its own, dramatically improve outcomes without chemotherapy, its life-prolonging impact sparked a movement in the medical community towards evaluating and tailoring treatments based on the genomic origins of a patient's cancer.[13] This interest has only grown since its origin, picking up speed in the last five to 10 years in response to improvements in molecular characterization technologies and increased evidence of "clinical benefits for many patients whose malignancies heretofore lacked effective therapy."[14] Multiple countries all around

---

7 *Precision Oncology*, NAT'L INST. OF HEALTH, https://www.nih.gov/about-nih/what-we-do/nih-turning-discovery-into-health/precision-oncology (last visited Apr. 12, 2022).

8 *Id.*

9 Deborah B. Doroshow & James H. Doroshow, *Genomics and the History of Precision Oncology*, 29 Surg. Oncol. Clin. N. Am. 1, 2 (Jan. 2020).

10 *Id.*

11 *Id.*

12 *Id.* at 3.

13 *See id.*

14 Doroshow & Doroshow, *supra* note 9, at 9.

the world have undertaken largescale genomic data accumulation projects and invested heavily in the development of large genomic databases, all for the purpose of advancing the field of precision medicine and providing their citizens with better, more personalized care.

1. Precision Oncology and Genomic Data

The development of newer and more personalized precision oncology treatments is dependent upon researchers accumulating and analyzing massive amounts of data to find links between genetic combinations, biological measurements, and cancer occurrences.[15] This data typically comes in one of three forms: the first is genomic information obtained via "genome sequence information and genetic analysis"[16] as well as other biological data such as "epigenetic and microbiome information."[17] The second form is data found in Electronic Health Records (EHR) such as "physical examinations, imaging studies, laboratory tests, pathology evaluations, and other measures."[18] This information is used to better understand "constituent elements of prior diagnoses, prognoses, and interventional strategies."[19] Finally, precision medicine also accumulates information from any source of data "with a possible connection to individual health" such as "mobile health apps, biometric measures captured from wearable devices, geolocation records, environmental exposure monitoring, and consumer and commercial information."[20]

The first kind of data, the genomic sequencing information, is particularly useful for the purposes of predicting disease and tailoring treatment. Genomic data is obtained from a subject's genome, which is "the complete set of genetic instructions"[21] from one's DNA, which can be found "in almost every cell."[22] Testing a subject's genome involves "collecting a sample of cells from a person — typically from hair, skin, blood, or saliva"[23] — and then extracting and testing the DNA in order to determine "the order and arrangement of the building blocks of the chemical bases" in the subject's genome.[24] This testing produces a massive amount of data considering one person has "6.4 billion building blocks, including around

15 *NCI and the Precision Medicine Initiative*, *supra* note 1.

16 Mark A. Rothstein, *Precision Medicine and the Risk to Privacy*, 15 SCITECH LAW 28 (2018).

17 *Id.*

18 *Id.*

19 *Id.*

20 *Id.*

21 Kristi Harbord, *Genetic Data Privacy Solutions in the GDPR*, 7 TEX. A&M L. REV. 269, 273 (2019).

22 *Id.*

23 *Id.* at 274.

24 *Id.*

20,000 protein-coding genes."[25] This information is highly valuable,[26] and the data contained in one's genome could provide potentially life-saving information regarding someone's "propensity for developing certain diseases"[27] as well as "their probability of having a child with certain conditions, or [receiving] a more accurate diagnosis."[28]

These genomic tests can have different purposes depending on the types of cells from which the genome is taken. Testing a genome taken from a healthy, noncancerous cell is known as genetic testing and can be done to "[look] for specific inherited changes (variants) in a person's gene"[29] for the purposes of finding out if someone has "inherited mutations that make them more likely to get cancer."[30] Genetic testing can provide subjects with some ability to manage their cancer risks and can help with decisions regarding treatment in the event that a cancer diagnosis occurs.[31] Testing a genome taken from a tumorous cell after a patient has been diagnosed with cancer is known as biomarker or tumor marker testing.[32] Biomarker testing looks for "genes, proteins, and other substances [biomarkers]"[33] which can provide information about a subject's specific cancer and can help a provider tailor a treatment based off the biomarkers that are identified.[34] Biomarker tests are an important component of precision oncology and can help link patients with treatments that might not otherwise have been available had their tumor's biomarkers not been identified.[35]

By sequencing and processing more genomes, researchers can find more patterns and links between biomarkers and treatments, thus improving precision oncology's reach, utility, and efficacy.[36] The sharing of genomic data between companies and countries further allows researchers to more easily "identify variations in genetic makeup and the significance of those variations more efficiently."[37]

---

25 *Id.* at 275.

26 Harbord, *supra* note 21, at 278.

27 *Id.* at 276.

28 *Id.*

29 *Genetic Testing for Inherited Cancer Susceptibility Syndromes*, NAT'L CANCER INST., https://www.cancer.gov/about-cancer/causes-prevention/genetics/genetic-testing-fact-sheet (last visited Apr. 12, 2022).

30 *Biomarker Testing for Cancer Treatment*, NAT'L CANCER INST., https://www.cancer.gov/about-cancer/treatment/types/biomarker-testing-cancer-treatment (last visited Apr. 12, 2022).

31 *Genetic Testing for Inherited Cancer Susceptibility Syndrome*, *supra* note 29.

32 *Biomarker Testing for Cancer Treatment*, *supra* note 30.

33 *Id.*

34 *Id.*

35 *Id.*

36 *See* Robert I. Field, Ethan Dombroski, Mary Kate McDevitt & Whitney A. Petrie, *Genetic Databases and the Future of Medicine: Can Law and Ethics Keep up? Perspectives and Analysis of a Conference*, 13 DREXEL L. REV. 321 (Feb. 11, 2021).

37 Harbord, *supra* note 21, at 277.

2. Risks Associated with Genomic Data Sharing

Such a tremendous accumulation of data, especially data so closely tied to the health and genetics of individuals, has important implications for privacy protection and data sharing. Because genomic data contains information related to our "physical and psychological traits and indicators of susceptibility to a range of diseases,"[38] as well as "information about our genetic heritage,"[39] the risk for discrimination by companies with access to that data is high.[40] A data breach or reidentification of one's genomic data may lead to social stigma and discrimination in areas such as "insurance, employment, and housing."[41] Though deidentification of all patient-related data is required before sharing in both the U.S. and the U.K. to varying degrees, much of this data, particularly genomic information, "can be reidentified with increasing ease."[42] Reidentification becomes even more likely and harmful if the party doing the reidentification has significant resources to put towards reidentification efforts. The HIPAA Privacy Rule provides some preventative measures to protect data subjects from inadvertent data breaches, but these measures only apply to "covered entities" and some of their "business associates," both of which are discussed in greater detail in Part II(B)(2). Notable organizations that are neither covered entities nor business associates, and thereby are not regulated by the HIPAA Privacy Rule, include social media companies, search engines, wearable device companies, employers, life insurance companies, and the general public.[43]

In the event of a genetic information data breach, HIPAA does not provide protections for the data subject against discrimination that may occur as a result of the data breach; these protections would be provided in the U.S. by the Genetic Information and Nondiscrimination Act (GINA).[44] GINA was instated to "prohibiting discrimination in health insurance and employment" based on genetic traits found through genetic testing.[45] GINA is divided into two Titles: Title I "prohibits genetic discrimination in health insurance,"[46] and Title II "prohibits genetic discrimination in employment."[47] GINA provides no protections against genetic discrimination in other potentially harmful areas such as housing. Additionally, GINA does not provide a full shield against genetic discrimination even if such discrimination can be proven and seemingly falls under the categories of either health insurance or employment.[48] For example, Title I protects against

38 Field et al., *supra* note 36, at 326.
39 *Id.*
40 *Id.* at 327.
41 *Id.*
42 *Id.* at 374.
43 Summary of the HIPAA Privacy Rule, HHS, https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html (last visited Apr. 15, 2022).
44 Field et al., *supra* note 36, at 357.
45 *Id.* at 361.
46 *Id.*
47 *Id.* at 362.
48 *Id.* at 361–362.

discrimination in health insurance, but "does not apply to other forms of health-related coverage, such as life, disability, or long-term care insurance." Similarly, Title II "bars employers from requesting, requiring, or purchasing genetic information about employees, applicants, or their family members."[49] However, several exceptions exist that could lead to employers acquiring and utilizing genetic information legitimately. These exceptions take effect when an employer 1) "acquires genetic information inadvertently;"[50] 2) is provided genetic information voluntarily by the employee as part of employer-sponsored services;[51] 3) "requests and receives genetic information in order to comply with the certification requirements of the FMLA, state leave laws, or certain employer leave policies;"[52] 4) when the genetic information "comes from sources that are commercially and publicly available;"[53] 5) "requests and receives genetic information as part of genetic monitoring required by law or conducted voluntarily under . . . defined conditions;"[54] and 6) "is engaged in conducting DNA tests for law enforcement purposes as a forensic laboratory or for identification of human remains."[55] To further complicate the protections that GINA attempts to provide, in the event that a violation is alleged to have occurred, the potential victim will "bear the burden of proving motive" of their employer or insurance provider.[56]

At this time, there is no equivalent protection against discrimination based on genetic information within the U.K. The closest applicable law is the Equality Act of 2010 which "legally protects people from discrimination in the workplace and in wider society."[57] This Act protects U.K. citizens from discrimination based on "protected characteristics" in a variety of areas including employment, education, buying or renting property, and several others.[58] The protected characteristics covered by the Equality Act include: age, gender reassignment, marriage or civil partnership, pregnancy or use of maternity leave, disability, race/nationality/ethnic or national origin, religion or belief, sex, and sexual orientation; additionally, protections apply to those who are "associated with someone who has a protected characteristic"[59] and have "complained about discrimination or supported someone else's claim."[60] Notably absent from this otherwise strong list is protection against any kind of genetic discrimination.

---

49 Field et al., *supra* note 36, at 362.

50 John D. Shyer & Kevin Kay, *Employer's Guide to GINA*, 19 Emp't Law Strategist 5, 3 (Sept. 2011).

51 *Id.*

52 *Id.*

53 *Id.*

54 *Id.*

55 Shyer & Kay, *supra* note 50.

56 Field et al., *supra* note 36, at 363.

57 *Equality Act 2010: Guidance*, GOVERNMENT EQUALITIES OFFICE, https://www.gov.uk/guidance/equality-act-2010-guidance (last visited Apr. 13, 2022).

58 *Discrimination: Your Rights*, EQUALITY ADVISORY SUPPORT SERVICE, https://www.gov.uk/discrimination-your-rights (last visited Apr. 13, 2022).

59 *Id.*

60 *Id.*

Citizens of the U.K. were protected against genetic discrimination prior to its departure from the E.U. through Article 21 of the EU Charter of Fundamental Rights.[61] Unlike the Equality Act of 2010, the Charter specifically prohibits any discrimination based on "genetic features."[62] Unfortunately, the Charter no longer applies to the U.K. because it was "not included in law as part of the European Union (Withdrawal) Act 2018."[63] It is possible that U.K. courts and legislators have not yet needed to address the issue of genetic discrimination in the event of a data breach, and that protections will be strengthened once they do need to address it. However, at present, no form of specific governmental protection against genetic discrimination exists in U.K. law.

Ultimately, both the U.S. and the U.K. could have more in place to protect their citizens from genomic discrimination. As technology improves, it's conceivable that reidentification will continue to get easier and require less of the genome to be successful; and because more and more people's genomic data are being stored and transferred each year, lawmakers should try and stay ahead of any discriminatory uses of deidentified genomic data. These enhanced protections could take a variety of forms but a strengthening of GINA within the U.S. and an adoption of a charter of fundamental rights within the U.K. would be good places to start.[64]

## B. The HIPAA Privacy Rule vs. The GDPR

In the United States, the transfer of genomic data, which falls under the classification of Protected Health Information (PHI), is governed predominantly by the Privacy Rule section of HIPAA. In the United Kingdom, as well as the European Union, to which the U.K. used to belong, the transfer of genomic data, and all personal data, is governed by the GDPR.

### 1. Origins

Though today, the HIPAA Privacy Rule and the GDPR differ in many significant ways, particularly surrounding the protection and sharing of genomic data, the two systems have largely the same origin. In the 1960s, the desire for a data protection system grew, stemming from concerns about the "accumulation of digital dossiers" of data.[65] These concerns related not just to the harm that could

---

61 EU Charter of Fundamental Rights, art. 21 (Dec. 12, 2007).

62 *Id.*

63 *What is the Charter of Fundamental Rights of the European Union?*, EQUALITY AND HUMAN RIGHTS COMMISSION, https://www.equalityhumanrights.com/en/what-are-human-rights/how-are-your-rights-protected/what-charter-fundamental-rights-european-union (last visited Apr. 13, 2022).

64 *See infra* Table 1 for a comparison of precision oncology in the United States and United Kingdom.

65 Jones & Kaminski, *supra* note 6, at 98.

result from the disclosure of information, but also to systemic implications about "power, fairness, accuracy, security, and accountability when governments and companies hold large amounts of information about individuals."[66] In response to this growing concern, the Fair Information Practices (FIPs) was implemented in multiple nations across the world, including the U.S. and in Europe.[67] The FIPs were "a set of principles for mass data collection, handling, and processing"[68] which included "rights of access, correction, and erasure and affirmative obligations for data handlers."[69] Though the FIPs were implemented differently in each country, both HIPAA and the GDPR were "ostensibly founded on the FIPs."[70]

HIPAA was signed into law by President Clinton on August 21, 1996.[71] It has been expanded upon several times since its passing.[72] In 2000, the Department of Health and Human Services (HHS) issued the Privacy Rule, an important strengthening of the Act which regulated "'covered entities' uses and disclosures of PHI."[73] The goal of the HIPAA Privacy Rule was to "balance the interest of individuals in maintaining the confidentiality of their health information with the interests of society in obtaining, using, and disclosing health information to carry out a variety of public and private activities."[74] Another notable enhancement of HIPAA occurred in 2009, when the Obama administration implemented the Health Information Technology for Economic and Clinical Health (HITECH) Act.[75] The goal of enacting the HITECH Act was to "promote the adoption and meaningful use of health information technology"[76] and "address privacy and security concerns associated with the electronic transmission of health information, in part, through several provisions that strengthen the civil and criminal enforcement of the HIPAA rules."[77] In addition to enhancing the protections imparted by HIPAA, the HITECH Act also strengthened the civil monetary penalties that may be imposed upon covered entities who fail to maintain the confidentiality of PHI.[78]

The GDPR was formally published on May 4, 2016, and went into force in the EU on May 25, 2018.[79] Although the U.K. voted to leave the European Union

---

66 *Id.*

67 *Id.* at 99.

68 *Id.*

69 *Id.*

70 Jones & Kaminski, *supra* note 6, at 99.

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

72 *See id.*

73 *Id.* at 976.

74 *Id.*

75 *Id.* at 973–74.

76 *HITECH Act Enforcement Interim Final Rule*, HHS, https://www.hhs.gov/hipaa/for-professionals/special-topics/hitech-act-enforcement-interim-final-rule/index.html (last visited Oct. 15, 2021).

77 *Id.*

78 Tovino, *supra* note 71, at 978.

79 DAVID ZETOONY, THE EU GENERAL DATA PROTECTION REGULATION (GDPR): ANSWERS TO THE MOST FREQUENTLY ASKED QUESTIONS, 11 (2018).

in 2016, it decided to retain the GDPR in its domestic law as the UK GDPR.[80] These regulations were enacted to "[lay] down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data."[81] Under the GDPR, data subjects have the right to "access, correct, and have deleted upon request any personal information" with limited exceptions.[82] The GDPR is still in its early stages and "[f]ew cases have been decided since the GDPR went into effect."[83] However, its international significance and the length of its reach have been demonstrated by "a number of recent, high-profile cases [which] reveal the complicated nature of EU law." [84]

2. Scope

The HIPAA Privacy Rule "applies only to covered entities; it does not apply to all persons or institutions that collect individually identifiable health information."[85] The covered entities are as follows: "(1) health plans, (2) health care clearinghouses, and (3) health care providers who electronically transmit any health information in connection with transactions for which HHS has adopted standards."[86] The Rule may also affect "other types of entities that are not directly regulated by the Rule" such as Business Associates.[87] Business Associates are people or entities "who, on behalf of a covered entity, [perform] or [assist] in performance of a function or activity involving the use or disclosure of individually identifiable health information."[88]

The GDPR has a much broader scope, applying to all companies that process personal data "in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not."[89] Not only does the GDPR regulate businesses that have employees and offices within Europe, it also regulates almost any company that interacts with European citizens.[90] Per Article 3, the GDPR applies to any company that "[offer] goods or services . . . to such data subjects in the Union,"[91] or any

---

80 *The UK GDPR*, INFORMATION COMMISSIONER'S OFFICE, https://ico.org.uk/for-organisations/dp-at-the-end-of-the-transition-period/data-protection-and-the-eu-in-detail/the-uk-gdpr/ (last visited Oct. 17, 2021).

81 GDPR, art. 1 (2018).

82 Field et al., *supra* note 36, at 364.

83 Jones & Kaminski, *supra* note 6, at 125.

84 *Id.*

85 *To Whom Does the Privacy Rule Apply and Whom Will It Affect?*, NAT'L INST. OF HEALTH, https://privacyruleandresearch.nih.gov/pr_06.asp (last visited Oct. 17, 2021).

86 *Id.*

87 *Id.*

88 *Id.*

89 GDPR, art. 3(1) (2018).

90 ZETOONY, *supra* note 79, at 7.

91 GDPR, art. 3(2)(a)–(b).

company that monitors European citizens' "behaviour as far as their behaviour takes place within the Union."[92]

3. Rules for Data Disclosure

Per the HIPAA Privacy Rule, in order for a covered entity to disclose PHI, they must adhere to one of 3 rules "depending on the purpose of the information use or disclosure."[93] The first rule permits certain PHI disclosures without prior permission from the PHI subject "in order to carry out [the covered entity's] own treatment, payment, and health care operations activities."[94] This includes the disclosure of PHI when a provider is consulting a specialist or when a covered entity sends a bill to a patient's insurer.[95] The second rule, also called the "oral permission rule,"[96] permits certain PHI disclosures to family members and loved ones only if "the individual is informed in advance of the use or disclosure and has the opportunity to agree to, prohibit, or restrict the use or disclosure."[97] This rule attempts to weigh the patient's interest in maintaining confidentiality against their interest in being visited in the hospital or receiving assistance, financial or otherwise, when needed.[98] The third and final rule is the default rule, and it covers the disclosure of all PHI that is not already covered by Rules 1 and 2 or any other exception found in the HIPAA Privacy Rule.[99] To disclose information that falls under the third rule, a covered entity must first obtain "written authorization from the individual who is the subject of the information."[100]

If a company within Europe would like to transfer data outside of the European Economic Area, they are permitted to do so; however, they must ensure that "they have put in place a mechanism that imposes many of the substantive provisions found within the GDPR upon the data once it leaves the . . . Area."[101] There are some countries (e.g. Canada, Israel, Argentina, etc.) that have been "recognized by the European Commission as ensuring an adequate level of protection;" therefore, these measures and mechanisms are not required for data transfer.[102] Unfortunately, the United States is not one of these recognized countries.[103] The measures that must be taken before transferring personal data outside of the European Economic Area are all based around ensuring that "the

92 GDPR, art. 3(2)(a)–(b).
93 Tovino, s*upra* note 71, at 980.
94 *Id.* at 980–81.
95 *Id.* at 981.
96 *Id.* at 982.
97 Tovino, *supra* note 71, at 982.
98 *Id.* at 983.
99 *Id.*
100 *Id.*
101 ZETOONY, *supra* note 79, at 103.
102 *Id.*
103 *See id.*

recipient has appropriate safeguards in place."[104] Appropriate safeguards, as detailed by the GDPR, include "Standard Contractual Clauses, certification to the Privacy Shield, and the implementation (and approval) of Binding Corporate Rules."[105] The Privacy Shield "refers to an agreement entered into between the U.S. Department of Commerce and the European Commission" which allows companies to self-certify that they will "abide by privacy principles that are similar . . . to those contained within the GDPR."[106] Binding Corporate Rules refers to "a set of internal policies, procedures, and protocols that are adopted between . . . a group of interrelated entities" which are then presented to and approved by a supervisory authority.[107]

4. Fines Incurred for Violations

Violations of the HIPAA Privacy Rule can incur both criminal and civil punishments, and these punishments are tiered based on the severity and nature of the violation.[108] For the purposes of this Note, only the civil violations will be discussed. The tiers are as follows: Category (A) covers instances in which the violating entity did not know they were in violation of a Privacy Rule; Category (B) covers instances in which the violating entity had a reasonable cause for the violation; Category (C)(i) covers instances of willful neglect which are subsequently corrected; and Category (C)(ii), the highest tier, covers instances of willful neglect which are not subsequently corrected.[109] The maximum fine for each tier is $50,000 per violation.[110] A penalty for violations "of the same requirement or prohibition under any of [the] categories may not exceed $1,500,000 in a calendar year."[111] Any decisions or determinations about the violations and what fines will be imposed upon a covered entity are made by the Secretary of HHS.[112]

The GDPR only has the authority to impose civil penalties and enforces its mandates regarding the protection of personal data via a two-tiered penalty structure.[113] Violations which meet the criteria to be penalized under the lower tier "are subject to an administrative fine that can be up to the greater of €10 million or

---

104 *Id.* at 105.

105 *Id.*

106 ZETOONY *supra* note 79, at 104.

107 *Id.*

108 *HIPAA violations & enforcement*, AMERICAN MEDICAL ASSOCIATION, https://www.ama-assn.org/practice-management/hipaa/hipaa-violations-enforcement (last visited Oct. 17, 2021).

109 Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules, 78 Fed. Reg. 17, 5583 (January 25, 2013) (to be codified at 45 C.F.F. pt. 160 and 164).

110 *Id.*

111 *Id.*

112 *Id.*

113 ZETOONY, *supra* note 79, at 145.

2% of a company's 'worldwide annual turnover.'"[114] Violations which are severe enough to meet the criteria for the higher tier are subject to an administrative fine that can be up to the greater of €20 million or four percent of a company's "'worldwide annual turnover.'"[115] These two tiers represent the maximum penalty that can be fined for certain violations; however, most violations that occur will be minor and not end up necessitating such drastic measures.[116] Authority for enforcing the GDPR and a Member State's domestic data privacy and security legislation is held by Data Protection Agencies (DPA) within the European Member States.[117] DPAs determine the extent of the fines imposed upon entities in violation of the GDPR.[118]

## III. COMPARISON

This section will analyze the policy differences between the HIPAA Privacy Rule and the GDPR which impact the sharing of genetic data between the U.S. and the U.K. for the purposes of precision oncology research.

### A. Classification as "Unsecure" Third Country

Perhaps the most significant barrier that U.S. and U.K. precision medicine researchers face with regards to transferring genomic data for the purposes of precision medicine research is that the United States is not one of the countries to which data transfer is expressly permitted by the GDPR.[119] The GDPR divides countries into "secure" and "unsecure" third countries for the purposes of data transfer; secure third countries are "those for which the European Commission has confirmed a suitable level of data protection on the basis of an adequacy decision."[120] The national laws in secure third countries "provide a level of protection for personal data which is comparable to those of EU law."[121] At this time, these countries include: "Andorra, Argentina, Canada (only commercial organizations), Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, Switzerland, Uruguay, Japan, the United Kingdom [following Brexit] and South Korea."[122] Despite the prominence of the U.S. in the field of precision oncology research, the lack of comprehensive personal data security provided by U.S. laws

---

114 *Id.*
115 *Id.*
116 *Id.*
117 *Id.*
118 ZETOONY, *supra* note 79, at 149; *See infra* Table 2.
119 *GDPR Third Countries*, INTERSOFT CONSULTING, https://gdpr-info.eu/issues/third-countries/ (last visited Apr. 13, 2022).
120 *Id.*
121 *Id.*
122 *Id.*

makes it an "unsecure" third country, thereby making data transfer notably more complicated.[123]

Fortunately, being classified as an "unsecure" third country "does not necessarily foreclose any data transfer to [the United States]."[124] Rather, prior to importing data from a country governed by the GDPR, a "mechanism that imposes many of the substantive provisions found within the GDPR upon the data" must be put in place by the data importer.[125] There are three mechanisms that are recognized by the GDPR as "imposing a sufficient measure of the GDPR provisions:"[126] (1) "Standard data protection clauses;"[127] (2) "Binding Corporate Rules" (BCRs);[128] and (3) "Privacy Shield."[129] Within the United States, the most popular method by which companies transfer data from the European Economic Area (EEA) to the U.S. is via Standard Contractual Clauses.[130] These are contractual agreements that have been reviewed and preapproved by the European Commission as sufficient to permit personal data held within the European Economic Area to be transmitted to a country that does not have the same level of data privacy and security laws.[131] While these contracts are helpful in providing an "additional layer of protection"[132] which "lowers . . . risks [to data subjects] posed by inconsistent law,"[133] they cannot entirely eliminate that risk[134] because data importers are only bound by the substantive protections provided by the GDPR, not the entirety of the GDPR itself.

Conversely, through Standard Contractual Clauses, U.S.-based organizations conducting precision oncology research across international borders can import permitted data from the U.K. However, in doing so, these organizations agree to take on far more regulations and protections on that data than they would otherwise be subjected to just following U.S. law. Additionally, they risk incurring penalties if they violate the new provisions they agreed to via their Standard Contractual Clauses.

## B. Transfer of Deidentified Data

Another major complication that can arise when attempting to transfer genomic data between the U.S. and the U.K. stems from differences in

123 *Id.*
124 *GDPR Third Countries*, *supra* note 119.
125 ZETOONY, *supra* note 79, at 103.
126 *Id.* at 104.
127 *Id.*
128 *Id.*
129 *Id.*
130 ZETOONY, *supra* note 79, at 110.
131 *Id.* at 104.
132 Laura Bradford, Mateo Aboy & Kathleen Liddell, *Standard Contractual Clauses for Cross-Border Transfer of Health Data after Schrems II*, 8 J.L. & BIOSCIENCES 1, 34 (2021).
133 *Id.*
134 *Id.*

deidentification and anonymization requirements as well as differences in what data is believed to be "deidentifiable" by each system.

When processing personal data, the GDPR differentiates between anonymization and pseudonymization.[135] Under the GDPR, anonymization is defined as "information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable."[136] Notably, the GDPR does not apply to fully anonymized information, thereby making the information easier for companies to use and transfer.[137] In order for personal data to be completely anonymized, all direct and indirect personal identifiers that may lead to an individual being identified must be removed.[138] This process differs from pseudonymization, which is defined in Article 4(3b) of the GDPR as "the processing of personal data in such a way that the data can no longer be attributed to a specific data subject without the use of additional information, as long as such additional information is kept separately and subject to technical and organizational measures to ensure non-attribution to an identified or identifiable individual."[139] Appropriate safeguards are required to ensure that the information that could be used to identify an individual using pseudonymized data is adequately protected.[140] This includes taking into account the time, cost, and technology that may be required to identify a subject from their pseudonymized personal data.[141] Because with pseudonymized data, there's still a risk that the data subject could be reidentified given the right information, it falls under the scope of the GDPR and, therefore, increased limitations are placed on the data and sufficient safeguards are required in any organization to which the data is transferred.[142]

This difference in how data is regulated under the GDPR is relevant to precision oncology research because the GDPR is currently undecided as to where the line is between anonymization and pseudonymization when it comes to data as sensitive, personal, and increasingly re-identifiable as genomic data. Some studies have shown that "fewer than 100 single nucleotide polymorphisms (SNP) are sufficient to distinguish an individual's DNA record."[143] Additionally, the "likelihood and severity of . . . re-identification" increases when genomic data

---

135 *Anonymisation and Pseudonymisation*, UNIV. COLL. LONDON, https://www.ucl.ac.uk/data-protection/guidance-staff-students-and-researchers/practical-data-protection-guidance-notices/anonymisation-and (last visited Jan. 31, 2022).

136 *Id.*

137 *Id.*

138 *Id.*

139 *Id.*

140 *Anonymisation and Pseudonymisation*, *Anonymisation and Pseudonymisation*, s*upra* note 174.

141 *Id.*

142 *Id.*

143 Mahsa Shabani & Luca Marelli, *Re-identifiability of Genomic Data and the GDPR*, EMBO REPORTS, May 24, 2019, at 2, 20: e48316.

includes peculiar characteristics such as rare genetic variants, exactly the type of data most likely to be transferred and utilized for precision medicine research.[144]

The relative ease with which genomic data may be re-identified and the amount that needs to be transferred for the purposes of precision oncology research means that it's unlikely this data will ever be considered anonymized. Therefore, the GDPR will likely always apply to such transfers. Additionally, the required safeguards for the transfer of pseudonymized data cause barriers in the form of potentially limiting how much genomic data can be sent at one time. Once again, this forms barriers in the performance of precision oncology research because not having the full genomic data slows down research and could lead to missed connections between genetic information and cancer treatments.

## C. Consenting to Data Usage

Though the HIPAA Privacy Rule does exist to provide protections for data subjects against data being used without their consent, these protections leave much to be desired in the modern age. It's discussed above that different standards exist for obtaining consent "depending on the purpose of the information use or disclosure."[145] The rule most applicable to the use and transference of genomic data for the purposes of precision oncology research is the default rule, which requires prior written authorization from the individual who is the subject of the PHI before using or disclosing the individual's PHI.[146] While this rule is beneficial to data subjects, it leaves much to be desired both in terms of its scope and its many exceptions. The HIPAA Privacy Rule and its protections pertaining to patient consent only apply to three kinds of organizations and their business associates[147] (described in more detail in section II(B)(2)). Additionally, "several broadly worded exceptions"[148] exist in the form of "permitted information uses and disclosures"[149] which allow even those organizations bound by the HIPAA Privacy Rule to "disclose, without a patient's knowledge or consent, health information in individually identifiable form."[150] These permitted uses and disclosures state that a covered entity is "permitted, but not required"[151] to use and disclose PHI without the data subject's consent for the following six purposes: "(1) To the Individual . . . ; (2) Treatment, Payment, and Health Care Operations; (3) Opportunity to Agree or Object; (4) Incident to an otherwise permitted use and disclosure; (5) Public Interest and Benefit Activities; and (6) Limited Data Set for the purposes of

144 *Id.* at 3.
145 Tovino, *supra* note 71, at 980.
146 *Summary of the HIPAA Privacy Rule*, HHS, 9, https://www.hhs.gov/sites/default/files/privacysummary.pdf (last visited Apr. 13, 2022).
147 *To Whom Does the Privacy Rule Apply and Whom Will it Affect?*, *supra* note 85.
148 Field et al., *supra* note 36, at 360.
149 *See* Tovino, *supra* note 71, at 982.
150 Field et al., *supra* note 36, at 360.
151 *Summary of the HIPAA Privacy Rule*, *supra* note 146, at 4.

research, public health or health care operations."[152] Additionally, "[t]here are no restrictions on the use or disclosure of de-identified health information,"[153] which is defined as "health information [which] neither identifies nor provides a reasonable basis to identify an individual."[154] However, as has already been made evident, reidentifying genomic data is becoming increasingly easier and more accessible, especially to companies with significant resources to put towards the reidentification efforts. It's evident from these significant gaps in scope and major exceptions, particularly in the field of research, that the consent requirement is nowhere near providing extensive data protection to patients looking to control the use and transference of their data via providing consent.

Under the GDPR, organizations processing personal health data must obtain "explicit consent . . . from the individuals" before collecting or using that data for almost any purpose unless a GDPR exception applies.[155] Per Article 6(1)(b) – (f), there are 5 exceptions that could allow companies to process personal data without first obtaining express consent from the data subject.[156] These apply if processing the data is necessary: (1) to perform a contract; (2) to comply with a legal obligation; (3) to protect the vital interests of a natural person; (4) to perform a task carried out in the public interest; and (5) for a legitimate interest pursued by a controller or a third party.[157] In the absence of one of these exceptions, the GDPR requires a "clear affirmative act" to demonstrate consent; a prechecked box, silence, and inactivity are insufficient for providing consent.[158]

There's currently some uncertainty surrounding an institution's ability to use a single "broad consent"[159] to allow them to utilize a subject's data for not only the consented use, but also for any subsequent uses for which the institution might require the data.[160] The legitimacy of such "broad consents" seems to be supported by the text of the GDPR, but "guidance from the regulatory body that interprets the law" does not support the use of broad consents.[161]

## D. Subject's Interest in Protecting Personal Data

Perhaps the most fundamental difference between the two policies lies in how they weigh the subject's interest in the protection of their personal data against other parties' private interests in that data. While the HIPAA Privacy Rule

---

152 *Id.*

153 *Id.*

154 *Id.*

155 Mabel Crescioni & Tara Sklar, *The Research Exemption Carve Out: Understanding Research Participants Rights Under GDPR and U.S. Data Privacy Laws*, Ariz. Legal Studies Disc. Paper No. 20-11, 128 (Apr. 2020).

156 ZETOONY, *supra* note 79, at 23

157 *Id.* at 23-24

158 *Id.* at 29

159 Field et al., *supra* note 36, at 365.

160 *Id.*

161 *Id.*

recognizes an "individual's interest in maintaining the confidentiality of [their] PHI,"[162] one of the Privacy Rule's stated goals, as implemented by the HITECH Act, is "to balance the interest of individuals in maintaining the confidentiality of their health information and the interest of society in obtaining, using, and disclosing health information to carry out a variety of public and private activities."[163] The GDPR, on the other hand, sees the protection of personal data as a "fundamental right and [a freedom] of natural persons."[164] Though this fundamental right is not absolute and, much like the Privacy Rule, is balanced against other private and governmental interests,[165] its classification as a fundamental right entitles citizens to different protections. Rather than just imposing "restrictions on the state," the GDPR places the onus of protection upon the government and the private sector by imposing protections which are actively "provided by the state."[166] This difference is significant because an "individual's interest" is not going to carry the same weight as a "fundamental right" when both are balanced against private and governmental interests.

In both the U.S. and the U.K., there are strong private and governmental interests in allowing precision oncology research to take place, and a recognition of the importance of accumulating and sharing genomic data to facilitate that research. However, the details of how information is shared, and what information is shared, creates barriers due to the differences in how each place sees the rights of the individual to the protection of their personal data.

## E. The Right to Be Forgotten

One of the most important of the rights granted by the GDPR in the modern age, the right to be forgotten, also called the right to erasure, refers to "the ability of a person to request that a company erase all of the personal data that it keeps about the person."[167] Article 17 of the GDPR states that a data subject "shall have the right to obtain from the controller the erasure of personal data concerning him or her . . . and the controller shall have the obligation to erase personal data."[168] The GDPR then goes on to detail when companies are and are not required to honor a request to be forgotten.[169] Companies under the GDPR are absolutely required to honor a request to be forgotten under the following circumstances: the data is no longer necessary; the data was processed based solely on consent; the controller's legitimate interest is outweighed by the data subject's rights; data is being processed unlawfully; erasure of data is controlled by law; or the data was collected from a

---

162 Tovino, *supra* note 71, at 984.

163 Stacey A. Tovino, *Teaching the HIPAA Privacy Rule*, 61 St. Louis U. L.J. 469, 475 (2017).

164 GDPR, Art. 1 (2018).

165 Jones & Kaminski, *supra* note 6, at 100.

166 *Id.* at 96-97.

167 *Id.*

168 GDPR, Art. 17(1) (2018).

169 ZETOONY, *supra* note 79, at 40.

child as part of offering an information society service.[170] This right, however, is not without exception; under the GDPR, a request for erasure does not have to be honored under the following circumstances: "(1) necessary to comply with a legal obligation under Union or Member State law; (2) desirable for public health reasons; or (3) desirable for scientific archiving reasons."[171] Data from clinical trials is generally "protected from a data subject's right to erasure, or portability,"[172] so long as the subject's consent has not been revoked because it has been deemed "necessary for scientific or research purposes."[173]

As is stated above, no analogous law relating to the right to be forgotten exists in the HIPAA Privacy Rule or in the majority of individual states.[174] There is a similar regulation included in the Children's Online Privacy Protection Act (COPPA) which permits parents to review and have deleted the online collection of information related to children under thirteen years of age.[175] The only policies in HIPAA analogous with the GDPR's right to be forgotten are those requiring covered entities to "maintain documentation required by the Privacy Rule" for a certain number of years following the document's last use.[176] These HIPAA policies, much like the exceptions in the GDPR's, recognize the potential benefits of maintaining health records. However, there's a significant difference between "the Privacy Rule [requiring] the maintenance of medical records . . . for a certain period of time"[177] and "The GDPR [requiring] erasure except when an exception applies."[178]

The ways that the transfer of genomic data can be impacted by the right to be forgotten are related to the scope of the GDPR versus the HIPAA Privacy Policy. If a valid request for erasure is made by a subject in the U.K., that request applies to all data kept by any company doing business within the U.K., regardless of whether they are a healthcare company.[179] This ensures complete erasure, meaning that, so long as the request doesn't push against any exceptions, the citizen's data cannot be used for the purposes of precision oncology research.[180] The HIPAA Privacy Rule, however, has no laws related to the mandatory erasure of personal data upon the request of the subject, and even if such a policy existed it would only be enforceable against covered entities and their business associates.[181] As it stands

---

170 *Id.* at 49-51.

171 Tovino, *supra* note 71, at 991.

172 Mabel Crescioni & Tara Sklar, *The Research Exemption Carve out: Understanding Research Participants Rights under GDPR and U.S. Data Privacy Laws*, Ariz. Legal Studies, Disc. Paper No. 20-11, 125, 128 (Apr. 2020).

173 *Id.*

174 *Id.*

175 *Id.*

176 Tovino, *supra* note 71, at 991.

177 *Id.*

178 *Id.*

179 ZETOONY, *supra* note 79, at 40.

180 *Id.*

181 *To Whom Does the Privacy Rule Apply and Whom Will it Affect?*, *supra* note 85; *See infra* Table 3.

now, there is no way for HIPAA to guarantee a subject's ability to be forgotten.[182] This is beneficial for the purposes of obtaining vast quantities of data in order to conduct precision oncology research, but it can also be seen as a violation of a subject's right to control their own personal data and how it's used.

In addition to the Right to be Forgotten, the GDPR provides a number of other notable rights to citizens that are either not found in U.S. Privacy Laws or present in U.S. laws but with a significantly more limited scope.[183]

## F. Violation Penalty Severity

As is discussed above, though both the HIPAA Privacy Rule and the GDPR can impose steep fines upon companies in violation of their respective privacy protection laws, it's worth noting how much more severe the GDPR's punishments can be. Because of HIPAA's relatively low maximum penalty per violation category per year, and because it can only assign fines that are strict dollar amounts rather than percentages, it's much more limited in the fines it can impose.[184] These limitations lead to the HIPAA Privacy Rule being a less effective deterrent to bigger companies who are willing and financially able to risk a multimillion-dollar penalty. To date, the largest penalty ever imposed for HIPAA Violations was a $16,000,000 penalty imposed upon Anthem, "an independent licensee of the Blue Cross and Blue Shield Association [and] America's second largest health insurer,"[185] along with an agreement to "take substantial corrective action to settle potential [HIPAA] violations."[186] This penalty was incurred following "a series of cyberattacks [that] led to the largest health data breach in history and exposed the electronic Protected Health Information of almost 79,000,000 people."[187] This corrective action, though sizeable, is nothing compared to what can be imposed upon a similarly violating company operating under the GDPR.

The penalty structure of the GDPR allows for much greater flexibility, not only in the amount that can be fined, but also in the type of entity upon which the fines can be imposed. Because the GDPR sees the protection of personal data as a fundamental right, and because its stated goals are less concerned with a balancing of private and public interests, the fines that can be imposed for violations are much

---

182 ZETOONY, *supra* note 79, at 52.

183 *See id.*

184 ZETOONY, *supra* note 89, at 145.

185 Steve Adler, *$16 Million Anthem HIPAA Breach Settlement Takes OCR HIPAA Penalties Past $100 Million Mark*, https://www.hipaajournal.com/16-million-anthem-hipaa-breach-settlement-takes-ocr-hipaa-penalties-past-100-million-mark/ (last visited Apr. 14, 2022).

186 *Anthem pays OCR $16 Million in record HIPAA settlement following largest health data breach in history*, HHS, https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/anthem/index.html (Oct. 15, 2018) (last visited Apr. 14, 2022).

187 *Id.*

higher. Consequentially, GDPR is a much more effective deterrent against large companies, particularly when the fines imposed involve not just a set dollar amount, but rather a percentage of a company's worldwide annual turnover. To date, the highest fine imposed by the United Kingdom for violations of the GDPR is a £22,046,000 fine against British Airways for "insufficient technical and organizational measures to ensure information security."[188] The highest total fine imposed by a country under the GDPR was a £746,000,000 penalty against Amazon for non-compliance with general data processing principles.[189]

As has been stated multiple times, genomic data is a highly valuable commodity for a company to possess. An inflexible penalty structure with relatively low maximum penalties, such as is found in the HIPAA Privacy Rule, simply does not provide an effective deterrent to the misuse of data when the accumulation of data is so profitable.

## IV. TRENDS IN U.S. PRIVACY LAWS AND LOOKING AHEAD

As should now be evident, significant policy differences between the HIPAA Privacy Rule and the GDPR lead to many of the barriers which impact how data can be transferred for the purposes of clinical oncology research.

When compared to the GDPR, the protections provided to data subjects by the HIPAA Privacy Rule are significantly more limited and place less importance on the subject's interest in their data privacy. In response to the significant gaps in protection left in the HIPAA Privacy Rule, several states have formed their own, more thorough personal data privacy laws more closely resembling the GDPR in order to provide their citizens with a level of protection not found under HIPAA alone.[190]

### A. State Driven Changes

The following sections are descriptions of policies enacted by U.S. states which expand upon HIPAA and more closely resemble the GDPR.

#### 1. The California Consumer Privacy Act

The California Consumer Privacy Act (CCPA) went into effect on January 1, 2020.[191] This law seeks to regulate "the collection, use, disclosure, and security

---

188 *GDPR Enforcement Tracker*, https://www.enforcementtracker.com (last visited Apr. 14, 2022).

189 *Id.*

190 *See* Sarah A. Sargent & Justin P. Webb, *California Consumer Privacy Act: A Practice Overview, 34 Corp. Counsel 25 (2020).*

191 *Id.*

of personal information" and expand the rights that data subjects have over their personal data.[192] Some of the most notable new privacy protections provided to California citizens by the CCPA include: (1) "[t]he right to know about the personal information a business collects about them how it is used and shared;"[193] (2) "[t]he right to delete personal information collected from them;"[194] (3) "[t]he right to opt-out of the sale of their personal information; and"[195] (4) protection from discrimination in the event that they exercise their CCPA rights.[196] This law is applicable only to California residents, which are defined by the CCPA as "a natural person (as opposed to a corporation or other business entity) who resides in California, even if the person is temporarily outside of the state."[197] The term "personal information" is defined within the CCPA as "information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household."[198] Excluded from this definition is aggregate and deidentified data.[199] These two terms "remain subject to interpretation by the California Attorney General."[200]

In addition to expanding data subject's rights, the CCPA also significantly expands upon HIPAA's scope. No longer only applying data privacy protection laws to specific types of healthcare companies and their business associates as is the case with the Privacy Rule, the CCPA's scope bears a much closer resemblance to that of the GDPR. The protections guaranteed by the CCPA apply to all businesses that meet one or more of the following criteria: (1) "Have a gross annual revenue of over $25,000,000;"[201] (2) "Buy, receive, or sell the personal information of 50,000 or more California residents, households, or devices; or"[202] (3) "Derive fifty-percent or more of their annual revenue from selling California residents' personal information."[203]

One important area in which the CCPA falls short of both the HIPAA Privacy Policy and the GDPR is in its ability to penalize companies for violations of the CCPA. The California attorney general's office "can seek civil penalties of $2,500 for each violation, or $7,500 for each intentional violation after notice."[204]

---

192 *Id.*

193 California Consumer Privacy Act (CCPA), CAL. DEP'T OF JUSTICE OFFICE OF THE ATT'Y GEN., https://oag.ca.gov/privacy/ccpa (last visited Apr. 14, 2022).

194 *Id.*

195 *Id.*

196 *Id.*

197 *Id.*

198 *Privacy Framework Comparison*, Center for Democracy & Technology, https://cdt.org/wp-content/uploads/2018/12/2018-12-12-CDT-CCPA-GDPR-Chart-FINAL.pdf (last visited Apr. 14, 2022).

199 *Id.*

200 *Id.*

201 CCPA, *supra* note 193.

202 *Id.*

203 *Id.*

204 The California Consumer Privacy Act: Frequently Asked Questions, 5, https://www.bakerlaw.com/webfiles/Privacy/2019/Briefs/California-Consumer-Privacy-Act-FAQs.pdf (last visited Apr. 14, 2022).

Additionally, "a 30-day opportunity to cure [has] been provided."[205] Additionally, private plaintiffs are permitted to bring "civil actions against a business in the event of a data security breach that results in unauthorized access and exfiltration, theft, or disclosure of the individual's personal information."[206] While these penalties become increasingly more severe depending on the number of violations found and citizens affected, those penalty caps make it unlikely that a company in violation will be paying anything near what they would be paying for a severe HIPAA or GDPR violation.

Though the CCPA was passed to provide California citizens with data protection similar to that provided by the GDPR, there remain some important distinctions between the two policies.[207] One of the most prominent differences is that of scope.[208] While the CCPA undoubtedly expands upon HIPAA's narrow scope, it still falls short of the broad-reaching GDPR which is applicable to all businesses, nonprofits, and government entities that process personal data within the EU, regardless of revenue, revenue source, or amount of personal information stored.[209] Not only must businesses operating in California meet certain criteria to fall under CCPA authority, but it also "does not apply to nonprofit organizations or government agencies."[210] There are also a variety of differences with regard to the rights offered by the two policies.[211]

Much like the GDPR, the CCPA is still new and developing. The specifics about its scope and how it will be enforced will develop over time. Additionally, it's uncertain how CCPA and the GDPR will interact and whether the protections provided by the CCPA will impact the ease of genomic data transfer between California and the U.K. Though California is a prominent location for medical research, and though the CCPA more closely resembles laws found in the GDPR's "secure" countries, it's unclear whether it's position as a state within an "unsecure" country will negate any changes in California's data transfer interactions with the U.K.

### 2. The Virginia Consumer Data Protection Act (VCDPA) and the Colorado Privacy Act (CPA)

Two other states, Colorado and Virginia, have followed California's lead and increased the data protection offered to their citizens beyond what is required by the HIPAA Privacy Rule and closer to the GDPR.[212]

---

205 *Id.*
206 *Id.* at 6.
207 *Privacy Framework Comparison*, *supra* note 198.
208 *Id.*
209 *Id.*
210 CCPA, *supra* note 193.
211 *Privacy Framework Comparison*, *supra* note 198.
212 *See infra* Table 4.

## V. CONCLUSION

As evidenced by the California, Colorado, and Virginia privacy protection law changes, there's a desire among certain states to enhance the data privacy protections beyond what's provided by the HIPAA Privacy Rule. It's possible that this signifies an upcoming push towards expanding the HIPAA Privacy Rule and increasing the protections provided on a federal level. States are often referred to as Laboratories of Democracy, a term stemming from a quote by Justice Brandeis in the *New State Ice Co. v. Liebmann* ruling.[213] As such, we could see more states and, eventually, the federal government following California, Colorado, and Virginia's lead should their new policies prove successful in the coming years.

However, it would be disingenuous to imply that all changes being proposed to HIPAA are attempting to elevate U.S. privacy laws all the way to the high standard of the GDPR. Most of the current popular proposals seek to add some consumer protections but fall well short of the privacy rights implemented by the CCPA or other, similar legislation. The most prominent potential HIPAA change right now is the modification proposed by the Office of Civil Rights (OCR) within the Department of Health and Human Services (HHS) on January 21, 2021 which seeks to "[reduce] administrative burdens on HIPAA covered health care providers and health plans, while continuing to protect individuals' health information privacy interests."[214] Some components of this proposition enhance HIPAA privacy protections, such as "strengthening individuals' rights to access their own health information, including electronic information."[215] Other components of the proposal could end up weakening protections depending on how they're enacted, such as the goal of "improving information sharing for care coordination and case management for individuals."[216] Regardless of whether or not protections are weakened by this proposed modification, it's notable that, at this time, it fails to address some significant holes in the HIPAA Privacy Rule such as the limited scope and the lack of guaranteed rights such as the right to be forgotten.[217] If the HIPAA Privacy Rule is changed in the next few years, it's most likely that change will be some form of the HHS's proposal. This indicates that a larger change expanding the scope and guaranteed rights is still a number of years away, even if the new state legislation proves successful.

Though a drastic change to federal data privacy laws is a lofty goal at this time, a strengthening of the HIPAA Privacy Rule seems to be the best way to eliminate many of the barriers that exist between the U.S. and the U.K. for the purposes of genomic data transfer. As is discussed in Section III(A), U.S.-based companies that are performing research and transferring data into and out of the

---

213 New State Ice Co. v. Liebmann, 285 U.S. 262, 310 (1932).

214 *Extension of the Public Comment Period for Proposed Modifications to the HIPAA Privacy Rule*, HHS, https://www.hhs.gov/about/news/2021/03/09/extension-public-comment-period-proposed-modifications-hipaa-privacy-rule.html (last visited Apr. 14, 2022).

215 *Id.*

216 *Id.*

217 *See id.*

U.K. are already binding themselves to substantial GDPR policies. These measures would be unnecessary if the U.S. were to model the changes to their privacy laws off of one of the "secure" third countries. Doing so would help to eliminate data transfer barriers and ease the difficulties associated with operating research under two different policies. Becoming a "secure" third country wouldn't require the U.S. to match the GDPR's level of protection exactly; it would only require that the U.S. "provide a level of protection for personal data which is comparable to those of EU law."[218] Considering the impact this would make on data sharing between the U.S. and the U.K., it could be worthwhile for legislatures to start proposing and advocating for at least the minimum requirements for obtaining "secure" third country status.

Finally, though this Note focuses on the impact that expanding the HIPAA Privacy Rule would have on the transfer of genomic data for the purposes of precision oncology research, it's very much worth noting the positive impact that such a change would likely have on U.S. citizens. In an increasingly data-driven world, ensuring data security as a right for your citizens and putting the onus on the government and private companies to proactively protect that right is quickly becoming essential. The GDPR is leading the way in providing protections for personal data for its citizens, and the HIPAA Privacy Rule will need to change soon or be replaced so as not to allow companies unchecked access to and use of potentially harmful data on U.S. citizens.

---

218 *GDPR Third Countries*, *supra* note 119.

## VI. APPENDIX

**Table 1: Precision Oncology in the U.S. vs. U.K.**

| United States | United Kingdom |
|---|---|
| <u>The Precision Medicine Initiative (PMI)</u><br>- President Obama launched the PMI on January 20, 2015[219]<br>- The PMI is a $215 million investment in the National Institute of Health and other partners to "accelerate biomedical research and provide clinicians with new tools to select the therapies that can be used in a more individualized approach with patients."[220]<br>- The PMI initiative has two main components:<br>1. "A near-term focus on cancers"[221]<br>2. "A longer-term aim to generate knowledge applicable to the whole range of health and disease."[222]<br><u>Genome Centers and Genomic Data</u><br>- In September 2018, "the National Institutes of Health ('NIH') provided $28.6 million in funding to establish three large-scale genome centers, | <u>The 10,000 Genomes Project</u><br>- In 2012, "Prime Minister David Cameron announced the 100,000 Genomes Project," a project which sought to "sequence 100,000 whole genomes from NHS (National Health Service) patients."[226]<br>- The project was successfully completed in 2018. It was reported that "actionable findings have been found for 1 in 4 / 1 in 5 rare disease patients, and around 50% of cancer cases contain the potential for a therapy or a clinical trial."[227]<br><u>Programme Coordination Group</u><br>- The Programme Coordination Group "brings together representatives from UK government, funding bodies, charities and a learned society"[228] with the goal of "ensuring that . . . the UK has the right environment to capture the patient and economic benefits offered by precision medicine."[229] |

219 Francis S. Collins & Harold Varmus, *A New Initiative on Precision Medicine*, 372 NEW ENG. J. MED. 793 (Feb. 26, 2015).
220 NCI, *supra* note 1.
221 Collins, *supra* note 219.
222 *Id.*
226 *100,000 Genomes Project*, GENOMICS ENGLAND, https://www.genomicsengland.co.uk/about-genomics-england/the-100000-genomes-project/ (last visited Apr. 13, 2022).
227 *Id.*
228 Mapping the UK Precision Medicine Landscape, INNOVATE UK, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/483560/Precision_Medicines_Booklet_Final_Web__002_.pdf (last visited Apr. 13, 2022).
229 *Id.*

| | |
|---|---|
| focused on generating genomic data"[223]<br>- The NIH also awarded "a $7 million contract to a software company that builds big-data platforms"[224] with the goal "[creating] a database of more than one million biosamples and associated health information." [225] | |

223 Harbord, *supra* note 21, at 270.
224 *Id.*
225 *Id.*

**Table 2: HIPAA Privacy Rule vs. The GDPR**

| | HIPAA Privacy Rule | The GDPR |
|---|---|---|
| Origins | - Founded on the Fair Information Practices (FIPS)[230]<br>- First signed into law on August 21, 1996[231]<br>- Privacy Rule was added in 2000 to regulate uses and disclosures of Protected Health Information[232]<br>- Protections were notably expanded in 2009 by the HITECH Act[233] | - Founded on the Fair Information Practices (FIPS)[234]<br>- Formally published on May 4, 2016[235]<br>- Went into force in the EU on May 25, 2018[236]<br>- U.K. decided to retain the GDPR after leaving the EU[237] |
| Scope | - Only applies to covered entities, a category which includes:[238]<br>1. Health plans[239]<br>2. Healthcare clearinghouses[240]<br>3. Health care providers who electronically transmit any health information in connection with transactions for which HHS has adopted standards[241] | - Significantly broader scope. Applies to all companies that process personal data within the EU[243]<br>1. Regulates businesses that have employees and offices within the EU[244]<br>2. Regulates businesses that interact with European citizens[245] |

230 Jones & Kaminski, *supra* note 6, at 98.
231 Tovino, *supra* note 71.
232 *Id.* at 976.
233 *Id.* at 973–74.
234 *Id.*
235 ZETOONY, *supra* note 79.
236 *Id.*
237 *The UK GDPR*, s*upra* note 80.
238 NAT'L INST. OF HEALTH, *supra* note 85.
239 *Id.*
240 *Id.*
241 *Id.*
243 GDPR, *supra* note 89.
244 GDPR, *supra* note 91.
245 GDPR, *supra* note 92.

| | | |
|---|---|---|
| | 4. other types of entities that are not directly regulated such as **business associates**[242] | |
| Rules for Data Disclosure | - Can disclose some PHI <u>without</u> permission from the subject to carry out subject treatment, payment, and health care operations activities[246]<br>- Can disclose some PHI to family members and loved ones if subject gives <u>oral consent</u>[247]<br>- All disclosures to which no exception applies require <u>written authorization</u> from the subject before disclosure[248] | - Prior to disclosure, appropriate safeguards must be in place that imposes the substantive GDPR provisions upon the data[249]<br>1. Appropriate safeguards include Standard Contractual Clauses, certification to the Privacy Shield, and the implementation (and approval) of Binding Corporate Rules[250]<br>- Some countries have been recognized as providing adequate data protection following transfer. The U.S. is not one of these countries[251] |
| Fines and Penalties | - Both civil and criminal penalties can be imposed[252]<br>- Penalties are tiered based on the violator's knowledge of the violation and the | - Only civil penalties can be imposed[255]<br>- Two-tiered system based on the nature of the violation[256]<br>1. Lower tier violations may incur a |

242 *Id.*
246 Tovino, s*upra* note 71, at 980–81.
247 *Id.* at 982.
248 *Id.* at 983.
249 ZETOONY, *supra* note 79, at 103.
250 *Id.* at 104.
251 *Id.* at 103.
252 *HIPAA violations & enforcement*, *supra* note 108.
255 ZETOONY, *supra* note 79, at 145.
256 *Id.*

| | | |
|---|---|---|
| | severity of negligence involved in the violation[253]<br>- A penalty for violations may not exceed $1,500,000 in a calendar year[254] | maximum fine of €10 million or two percent of a company's 'worldwide annual turnover, whichever is greater[257]<br>2. Higher tier violations may incur a maximum fine of €20 million or four percent of a company's 'worldwide annual turnover, whichever is greater'[258] |

253 *Id.*

254 Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules, *supra* note 109.

257 *Id.*

258 *Id.*

**Table 3: Rights Provided by the GDPR**

| | The GDPR | The HIPPA Privacy Rule |
|---|---|---|
| The Right to be Forgotten | - Data subjects have the right to obtain from the controller the erasure of personal data and the controller shall have the **obligation** to erase personal data[259]<br>- Companies are absolutely required to honor a request to be forgotten under the following circumstances:<br>1. The data is no longer necessary[260]<br>2. The data was processed based solely on consent[261]<br>3. The controller's legitimate interest is outweighed by the data subject's rights[262]<br>4. Data is being processed unlawfully[263]<br>5. Erasure of data is controlled by law;[264] or<br>6. The data was collected from a child as part of offering an | - **No analogous law** relating to the right to be forgotten exists in the HIPAA Privacy Rule.[270]<br>- Similar regulation is found in the Children's Online Privacy Protection Act (COPPA) which permits parents to review and have deleted the online collection of information related to children below 13 years old.[271]<br>- Covered entities are required to maintain documentation required by the Privacy Rule.[272] |

259 GDPR, Art. 17(1) (2018).
260 ZETOONY, *supra* note 79, at 49.
261 *Id.*
262 *Id.* at 50.
263 *Id.*
264 ZETOONY, *supra* note 79, at 49.
270 *Id.* at 52.
271 *Id.*
272 Tovino, *supra* note 71, at 991.

| | | |
|---|---|---|
| | information society service[265]<br>- Exceptions to the Right to be Forgotten Rule:<br>1. Data is necessary to comply with a legal obligation under Union or Member State law;[266]<br>2. Data is desirable for public health reasons;[267] or<br>3. Data is desirable for scientific archiving reasons.[268]<br>- Data from clinical trials is generally protected by the right to erasure or portability[269] | |
| Individual's Right to Access Their Information | - Data subject can request:<br>1. That a company confirm whether it has personal data about the individual;[273] and<br>2. That a company provide that information to the individual[274]<br>- Companies are required to respond to a requestor within one month.[275] | - Analogous policies can be found in HIPAA and FERPA but are not found in the majority of U.S. data privacy laws.[276] |
| Right to Receive | - When this right is triggered, a company is | - No analogous policies are found in the HIPAA Privacy Rule[282] |

265 *Id.* at 51.
266 Tovino, *supra* note 71, at 991
267 *Id.*
268 *Id.*
269 *Id.*
273 ZETOONY, *supra* note 79, at 55.
274 *Id.*
275 *Id.* at 59.
276 *Id.* at 60.
282 *Id.*

| | | |
|---|---|---|
| Information on a Portable Device | obligated to provide the data in a structured, commonly used, and machine-readable format per Article 20(1)[277]<br>1. Additionally, the format should be interoperable between different controllers and must capture relevant metadata[278]<br>- Only applies when a company's processing is based on the fact that either the data subject provided their consent for the processing or the data subject entered into a contract with the company[279]<br>1. If processing is <u>not</u> based on this consent, companies are not required to provide subjects access to data in a portable format[280]<br>- Request must be responded to within 1 month. 2 additional months can be added if needed due to complexity or number of requests.[281] | |
| Individual's Right to Fix | - Refers to the ability of a person to request that a company fix any | - No analogous policies exist in the HIPAA Privacy Rule[286] |

277 GDPR, Art. 20(1) (2018).
278 *Id.* at 63.
279 *Id.*
280 *Id.* at 61-62.
281 GDPR, *supra* note 277, at 64.
286 *Id.*

| | | |
|---|---|---|
| Their Information | inaccuracies in the personal data that it holds about them[283]<br>- A.K.A. The Right of Rectification<br>- Controllers are **obligated** to keep information up to date and as accurate as possible[284]<br>- Controllers have one month to respond to requests to fix data about an individual[285] | |

283 *Id.* at 67.
284 *Id.* at 67.
285 *Id.* at 68.

**Table 4: The VCDPA and the CPA**

| | **The VCDPA** | **The CPA** |
|---|---|---|
| Enacted | March 2, 2021<br>(Goes into effect January 1, 2023)[287] | July 8, 2021<br>(Goes into effect July 1, 2023)[288] |
| Scope | - "Imposes obligations on entities that conduct business in Virginia or produce products or services targeted to residents of Virginia, and control or process personal data of at least:[289]<br>1. 100,000 consumers during the calendar year, or[290]<br>2. 25,000 consumers and derive over fifty-percent of gross revenue from the sale of personal data."[291]<br>- Does NOT include any revenue thresholds (unlike CCPA)[292]<br>- Defines "personal data" as "any information that is linked or reasonably | - "Applies to any controller that:<br>1. Conducts business in Colorado, or produces or delivers commercial products or services that are intentionally targeted to residents of Colorado; and[300]<br>▪ Controls or processes the personal data of at least **100,000 consumers or more** during a calendar year; or[301]<br>▪ Derives revenue or receives a discount on the price of goods or services from the sale of personal data and processes or controls the personal data of **25,000 consumers or more**."[302]<br>- Does NOT include any revenue thresholds (unlike CCPA)[303] |

287 Lars Lindgren, *Virginia's New Consumer Data Protection Act: Will Others Follow?*, JOLT DIG. (Mar. 16, 2021), https://jolt.law.harvard.edu/digest/virginias-new-consumer-data-protection-act-will-others-follow.

288 Sarah Rippy, *Colorado Privacy Act Becomes Law*, Int'l Ass'n of Privacy Prof'ls (Jul. 8, 2021), https://iapp.org/news/a/colorado-privacy-act-becomes-law/.

289 Lindgren, *supra* note 287.

290 *Id.*

291 *Id.*

292 *Id.*

300 Rippy, *supra* note 288.

301 *Id.*

302 *Id.*

303 *Id.*

| | | |
|---|---|---|
| | linkable to an identified or identifiable natural person."[293]<br>- Further defines "sensitive data," a 2nd category within personal data. Covered entities must obtain consumer consent before processing sensitive data. This category includes:[294]<br>1. "Personal data revealing racial or ethnic origin, religious beliefs, mental or physical health diagnosis, sexual orientation, or citizenship or immigration status;[295]<br>2. The processing of genetic or biometric data for the purpose of uniquely identifying a natural person;[296]<br>3. The personal data collected from a known child; or[297]<br>4. Precise geolocation data"[298]<br>- The term "sale" explicitly excludes other types of | - "Is applicable even when a company derives less than fifty-percent of its gross annual revenue from selling data" (Unlike CCPA)[304]<br>- The term "sale" explicitly excludes other types of disclosure such as disclosures to a third party that will process the personal data on the controller's behalf.[305] |

293 Lindgren, *supra* note 287.
294 *Id.*
295 *Id.*
296 *Id.*
297 *Id.*
298 Lindgren, *supra* note 287.
304 *Id.*
305 *Id.*

| | | |
|---|---|---|
| | disclosure such as disclosures to processors or disclosures as part of a merger or acquisition.[299] | |
| Rights Granted | - Right of Access[306]<br>- Right to Correction[307]<br>- Right to Delete[308]<br>- Right to Data Portability[309]<br>- Right to Opt Out[310]<br>- Right to Appeal[311] | - Right of Access[312]<br>- Right to Correction[313]<br>- Right to Delete[314]<br>- Right to Data Portability[315]<br>- Right to Opt Out[316]<br>- Right to Appeal[317] |
| Obligations on Controllers | - Limits on Collection[318]<br>- Limits on Use[319]<br>- Technical Safeguards[320]<br>- Privacy Policy[321] | - Duty of Transparency[322]<br>- Duty of Purpose Specification[323]<br>- Duty of Data Minimization[324]<br>- Duty to Avoid Secondary Use[325]<br>- Duty of Care[326]<br>- Duty to Avoid Unlawful Discrimination[327]<br>- Duty Regarding Sensitive Data[328] |

299 Sarah Rippy, *Virginia Passes the Consumer Data Protection Act*, Int'l Ass'n of Privacy Prof'ls (Mar. 3, 2021), https://iapp.org/news/a/virginia-passes-the-consumer-data-protection-act/.

306 Rippy, *supra* note 299.

307 *Id.*

308 *Id.*

309 *Id.*

310 *Id.*

311 Rippy, *supra* note 299.

312 Rippy, *supra* note 288.

313 *Id.*

314 *Id.*

315 *Id.*

316 *Id.*

317 Rippy, *supra* note 288.

318 Rippy, *supra* note 299.

319 Rippy, *supra* note 288.

320 *Id.*

321 Rippy, *supra* note 299.

322 Rippy, *supra* note 288.

323 *Id.*

324 *Id.*

325 *Id.*

326 *Id.*

327 Rippy, *supra* note 288.

328 *Id.*

| | | |
|---|---|---|
| | | - Data Protection Assessments[329]<br>- Data Processing Contracts[330] |
| Enforcement | - Once the attorney general or district attorney initiates the action, notice must be provided to the controller.[331]<br>1. Controller has thirty **days** to cure the violation AND provide to the attorney general an "express written statement that the alleged violations have been cured and that no further violations shall occur."[332]<br>- "If the controller fails to cure the violation, the attorney general may fine them up to $7,500 per violation."[333] | - Once the attorney general or district attorney initiates the action, notice must be provided to the controller[334]<br>1. The controller then has sixty **days** to cure the violation (Unlike CCPA and VCDPA's 30 days)[335]<br>2. Right to cure will cease to exist on January 1, 2025, after which controllers will no longer be entitled to cure prior to attorney general action[336]<br>- "[A] non-compliant entity may be fined up to $20,000 per violation."[337] |

329 *Id.*
330 *Id.*
331 Rippy, *supra* note 299.
332 *Id.*
333 *Id.*
334 Rippy, *supra* note 288.
335 *Id.*
336 *Id.*
337 *Id.*