2020

HIPAA Reform or a Patchwork Scheme: A Look at Preemption, Scope, and the Inclusion of a Private Right of Action in a New Federal Data Privacy Law

David Cohen
American University Washington College of Law

HIPAA REFORM OR A PATCHWORK SCHEME: A LOOK AT PREEMPTION, SCOPE AND THE INCLUSION OF A PRIVATE RIGHT OF ACTION IN A NEW FEDERAL DATA PRIVACY LAW

David Cohen[*]

* * *

Table of Contents

[*] The author's biographical information can be found on LinkedIn at: https://www.linkedin.com/in/david-cohen-173b686b.

I. INTRODUCTION

The importance of data privacy is growing as there is a global movement towards enacting new legislation to protect personal data. The European Union has passed the General Data Protection Regulation (GDPR),[1] California has passed the California Consumer Privacy Act (CCPA),[2] and other states are currently looking at enacting their own privacy laws.[3] This would inevitably lead to a patchwork of different state privacy laws which could create a litany of problems for businesses and consumers alike.

The CCPA is already illustrative of many problems that state by state regulation would lead to. Mere Initial compliance with the CCPA has been estimated to cost as much as $55 billion total, costing the smallest of businesses around $50,000 each and the largest around $2 million each.[4] Other annual costs associated with the CCPA are estimated to reach about $75,000 per business.[5] These compliance costs will rise as each state passes its own unique privacy law. The public might vary on their sympathy towards the plight of businesses, but they are overwhelmingly in favor of policy changes that would promote medical research.[6] Lifesaving clinical studies that rely on various forms of data might get bogged down in red tape under a patchwork scheme.[7] Various members of Congress have drawn attention to these issues and some have proposed legislation to create a national privacy act,[8] but wait, doesn't the U.S. already have one?

---

[1] E.U. General Data Protection Regulation (GDPR): Regulation (E.U.) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2009 O.J. (L 119).

[2] *California Consumer Privacy Act (CCPA)*, CA. DEP'T JUSTICE: OFFICE OF ATTORNEY GEN., https://www.oag.ca.gov/privacy/ccpa (last visited Mar. 5, 2020).

[3] Liisa Thomas, *3 Privacy Law Predictions for the New Year*, LAW360 (Jan. 1, 2020), https://www.law360.com/articles/1229279/3-privacy-law-predictions-for-the-new-year.

[4] Aly McDevitt, *CCPA Compliance Costs Projected to Reach $55B*, COMPLIANCE WEEK (Oct. 8, 2019), https://www.complianceweek.com/data-privacy/ccpa-compliance-costs-projected-to-reach-55b/27847.article.

[5] *Id.*

[6] Robert Shalett, *Overwhelming Majority of Americans Say Discussions About Clinical Trials Should be a Part of Standard of Care*, RESEARCH AMERICA (July 25, 2019), https://www.researchamerica.org/news-events/news/overwhelming-majority-americans-say-discussions-about-clinical-trials-should-be.

[7] Jeannie Baumann**,** *Patchwork of Privacy Laws Muzzle Medical Studies Across States*, BLOOMBERG (May 28, 2019), https://www.bloomberglaw.com/document/X9SU9LM4000000?bna_news_filter=pharma-and-life-sciences&jcsearch=BNA%25200000 016ae652df18a36 be7d 7ec3e0002#jcite.

[8] David Ruiz, *US Congress Proposes Comprehensive Federal Data Privacy Legislation—Finally*, MALWAREBYTES (Mar. 26, 2019), https://blog.malwarebytes.com/security-world/privacy-security-world/2019/03/what-congress-means-when-it-talks-about-data-privacy-legislation/.

II. HIPAA BACKGROUND

This section will give a brief explanation of the history of America's primary federal health data privacy law and how it works. This will highlight the laws shortcomings and the reason why states are pushing for their own data privacy statutes. These state privacy laws are intended to regulate data generally, but I will focus on their effect on health data.

A. SECTORAL COVERAGE

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) is a unique statute in that its statutory language has almost nothing to do with what it is known for today.[9] The statute is largely known today for its privacy and security rules relating to health data, but many don't know that the law originally had almost nothing to do with data privacy.

As the name might suggest, the statutory language focused almost exclusively on healthcare portability and administrative simplification. The portability provisions were intended to combat an issue which some referred to as "job lock," an artificial barrier to employment based on health insurance.[10] The "job lock" phenomenon of the 90s led to scenarios where employees would pass up on better job opportunities because they feared losing their health benefits under their current job. HIPAA attempted to fix this by allowing employees to take their old health benefits with them to their new job if they met certain requirements.[11] The other focus of HIPAA was to simplify and standardize electronic claims forms to lower the administrative burden in healthcare billing.[12] Congress realized it needed to work some privacy provisions into the law to protect the health records being dealt with, but they couldn't reach a decision in time.[13] Instead, Congress did what it usually does and chose to punt the question to the agencies. HIPAA required the Secretary of Health and Human Services (HHS) to enact privacy regulations if Congress failed to do this, so HHS created basically all the privacy rules under HIPAA through notice and comment rulemaking.[14] These privacy regulations could have been broad in scope and applied to any party that dealt with any health information generally, but this is not the case

---

[9] Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub. L. No.104-191, 110 Stat. 1936 (1996).

[10] Ellyn E. Spragins, How to Beat Job Lock, NEWSWEEK, Dec. 14, 1998, at 98.

[11] John Graham**,** *Employer-Based Health Insurance: "Job Lock" is Not the Problem, "Insurance Lock" is*, THE BEACON, (Apr. 2, 2014), https://blog.independent.org/2014/04/02/employer-based-health-insurance-job-lock-is-not-the-problem-insurance-lock-is/.

[12] *Summary of the HIPAA Privacy Rule*, U.S. DEP'T HEALTH & HUM. SERVS. (July 26, 2013), https ://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html.

[13] *Id.*

[14] *Id.*

because the statute constrained HHS's authority by focusing on portability and electronic claims forms.

The privacy regulations clarify who and what the law applies to. The rules do not cover all health information; instead they only cover "protected health information (PHI)," which is individually identifiable health information held or transmitted by covered entities (CEs) or their business associates (BAs).[15] A CE includes the major industries in the healthcare sphere, such as health plans, most healthcare providers, and healthcare clearinghouses (companies that offer certain administrative services to healthcare entities).[16] A BA can refer to a vendor that performs work on behalf of the CE when the work involves the use or disclosure of the individually identifiable health information.[17]

Health plans and healthcare providers are the most important entities under the CE definition. The statutes focus on electronic claims forms narrowed the CE definition to include only those providers and plans that electronically transmit health information.[18] Additionally, the statute's focus on health coverage portability limited the privacy rules to only cover entities that directly deal with regular health insurance. This results in illogical scenarios where a person or business that should be covered by HIPAA, isn't. A healthcare provider like a doctor who provides services and bills electronically is covered by HIPAA, while a doctor that provides services and bills through physical paperwork is not. A hospital that uses its patients' health data which constitutes PHI is covered by the HIPAA rules because they bill health insurance programs directly. Drug companies and other healthcare businesses that do not directly bill health insurance programs may not be covered by the privacy rules, even if those businesses have the same PHI data that the hospital has.

These coverages gaps are why HIPAA is currently lacking in many regards. The 1996 statutory framework leads to illogical scenarios where a party who has PHI may or may not be regulated by HIPAA based on non-privacy related factors like electronic health records and portability. The industry specific or sectoral approach that HIPAA uses needs to be amended so that HIPAA can cover all data or all health data regardless of whose hands the PHI is currently in. There have been repeated calls to reform HIPAA in this manner, but how else should HIPAA be reformed? We now have the benefit of looking at and contrasting HIPAA with the CCPA and other data privacy laws to see what works and what doesn't.

---

[15] 45 C.F.R. § 160.103.
[16] *Id.* (defining "covered entity" under HIPAA).
[17] *Id.* (defining "business associate" under HIPAA).
[18] *Id.*

B. NOT ALL DATA IS CREATED EQUALLY AND WHY WE SHOULD FOCUS ON HEALTH DATA

Reforming the regulation of health information should be a massive priority for our government right now. Health information is easily the most important form of data that exists today. The average life expectancy has risen sharply since the 1900s, largely because of advances in medicine resulting from data-based research.[19] New drugs and lifesaving treatments, which were few and far between for most of human history, now regularly make headline news as the pace of innovation gets faster and faster. Health data is the most important form of data for improving life, but it is also the most valuable information in the hands of hackers and other criminals. Stolen healthcare data has been estimated to be worth 10 to 50 times more than credit card data when sold on the black market.[20] Hackers can use your health data to buy prescription drugs, hack your cell phone, create fake IDs, and even claim your social security benefits.[21] Some hackers have even engaged in ransomware attacks, where they demand millions of dollars from medical providers in exchange for returning the provider's ability to access their patient records.[22]

Health data can be used for the greater good, but it can also be abused to the detriment of society. Therefore, we need to strike a balance between protecting data and allowing access to it. HIPAA might not protect this data enough, but the CCPA is overprotective in many regards. Some health data are protected by HIPAA while other health data are covered by state law. What do these laws do right and what do they do wrong, and how should HIPAA be amended or left alone to compensate for these risks?

III. STATE AND FEDERAL CONFLICT AND CONFUSION

This section will give a brief explanation of some of the confusion and conflicts that exist between HIPAA and the CCPA. These problems would increase exponentially as each state creates its own unique data privacy law. The solution to this would be crafting a new federal health data privacy law that preempts state law. This section looks at what a federal law would need

---

[19] CDC, *Achievements in Public Health, 1900-1999: Control of Infectious Diseases*, (July 30, 1999), https://www.cdc.gov/mmwr/preview/mmwrhtml/mm4829a1.htm/.

[20] Byron Acohido, *Why Medical Records Are Easy to Hack*, INSURANCE THOUGHT LEADERSHIP (Feb. 25, 2015), https://www.insurancethoughtleadership.com/medical-records-easy-hack/.

[21] Meera Jagannathan, *Buying Prescription Drugs, Hijacking Your Cell Phone — and Other Sinister Things Hackers can do with your Data*, MARKETWATCH (Aug. 11, 2019), https://www.marketwatch.com/story/after-capital-ones-hack-here-are-all-the-crazy-things-bad-actors-can-do-if-they-steal-your-personal-data-2019-07-31.

[22] *Hackers Demand US$14M in Ransom to Unlock Systems in U.S. Nursing Homes*, CISOMAG (Nov. 27, 2019), https://www.cisomag.com/hackers-demand-us14m-in-ransom-to-unlock-systems-in-u-s-nursing-homes/.

to have in it to preempt state law and cover all health data. The surprising result is that a national data privacy law that regulates data generally is what is required if regulators wish to avoid a patchwork scheme of state regulation of health data. This is because traditional notions of what constitutes health data under HIPAA are no longer viable in today's age.

I will address the conflicts between state and federal law in this section, and the need for an amended HIPAA to cover all data generally in the next section.

A. WHICH LAW APPLIES? SIMILAR PROVISIONS HAVE DIFFERENT STANDARDS

The CCPA contains a provision that says that it largely steps back to the extent that HIPAA covers health data.[23] This means that PHI held by CEs and BAs will remain regulated by HIPAA only. HIPAA's sectoral coverage means that health data that fall outside of this specific category, will likely be regulated by the CCPA. Therefore, the CCPA might regulate other healthcare businesses such as joint ventures, unlicensed wellness providers, mobile health applications, hybrid entities, and many more.[24] This can confuse parties that handle health information especially in areas where HIPAA and the CCPA overlap.

The rights and responsibilities of the parties involved will vary drastically based on which law they are covered by. A party may attempt in good faith to abide by the law but end up violating nonetheless because it accidentally followed the rules of the incorrect law. One example involves de-identification. Under both laws, de-identification is essentially the process by which you remove various identifiers from health data until the data can no longer be reasonably linked to the individual it came from. HIPAA and the CCPA only cover data that have sufficient identifiers that they can be linked to some degree to a person, whereas data that are sufficiently anonymous can avoid regulation. A party wanting to use certain health data might go about de-identifying the data so that it is no longer regulated but it might accidentally de-identify under HIPAA's standard which might not sufficiently de-identify the data under the CCPA.

Under HIPAA, this list of identifiers includes names, certain geographic subdivisions (i.e. street address and/or county), all elements of dates (except the year), certain contact information, and various identification codes (i.e.

---

[23] Cal. Civ. Code § 1798.145(c)(1)(B).

[24] Andrea Musker & Anne Brendel, *The California Consumer Privacy Act's Applicability to the Health Care Industry*, BUCHALTER (Nov. 11, 2019), https://23ic801dv4zv2euw993mgvv9-wpengine.netdna-ssl.com/wp-content/uploads/2019/11/CCPA-Applicability-Healthcare.Musker.Brendel.pdf.

Social Security number).[25] You can also de-identify data by having an expert-de-identifier review and determine that it is very unlikely that the PHI could be linked to an individual.[26] The CCPA does not provide a list of identifiers to remove, but instead provides general criteria that must be met. A CCPA regulated party must ensure that the information cannot reasonably identify a particular customer and the business cannot try to re-identify the data.[27] That party must additionally ensure that it has sufficient safeguards which stop the data from being reidentified and the business must also prevent data breaches.[28] Unlike HIPAA, the CCPA does not have a similar expert de-identification standard.

Even California realized the confusion that would arise under the different di-identification standards. Some state legislators are now working to pass a new bill that would exempt from the CCPA data that are correctly de-identified under the HIPAA standard.[29] This is merely one example of the confusion that arises from the differences between HIPAA and the CCPA, but the issues don't end there.

B. WHICH LAW APPLIES? MULTIPLE STATE LAWS TO CONSIDER

Our inquiry doesn't end there. Before we even consider what the different standards are between a state privacy law and a federal privacy law, we need to know what state law applies. Some states have multiple data privacy laws which further complicates the matter. As stated before, the CCPA will generally step aside from the information that HIPAA already covers, but the CCPA also steps back from regulating data that is already regulated by California's Confidentiality of Medical Information Act (CMIA).[30] The CMIA regulates "medical information" which includes:

> any individually identifiable information, in electronic or physical form, in possession of or derived from a provider of health care, health care service plan, pharmaceutical company, or contractor regarding a patient's medical history, mental or physical condition, or treatment. Individually identifiable means that the medical information includes or contains any element of personal identifying information sufficient to allow identification of the

[25] 45 C.F.R. § 164.514(b).
[26] *Id.*
[27] Cal. Civ. Code § 1798.140(h).
[28] *Id.*
[29] Daniel Gottlieb & Deepali Doddi, *California Bill Proposes CCPA Exceptions For HIPAA De-Identified Information*, Other Health Data, MONDAQ (Jan. 20, 2020), https://www.mondaq.com/unitedstates/Privacy/885288/California-Bill-Proposes-CCPA-Exceptions-For-HIPAA-De-Identified-Information-Other-Health-Data.
[30] Cal. Civ. Code § 1798.145(c)(1)(A).

> individual, such as the patient's name, address, electronic mail address, telephone number, or social security number, or other information that, alone or in combination with other publicly available information, reveals the individual's identity.[31]

The medical information definition is very similar to the PHI definition but the CMIA adds additional protection in certain areas. As stated before, HIPAA does not preempt where states add additional protections which means that HIPAA will not preempt areas where the CMIA regulates more rigorously.

The end result is that health data coming from California could be regulated by either the CCPA, CMIA, HIPAA, or no laws. These four possibilities create a very complicated analysis for a party that deals with health information in California. The number of possible state laws that one could be subject to could increase exponentially if other states enact their own versions of the CMIA and/or CCPA. Healthcare entities attempting to comply with the law may be met with insurmountable compliance costs by having to hire a small army of lawyers to come to terms with what they can and cannot do with the data they hold.

C. PREEMPTION

As stated before, the patchwork scheme can be prevented by Congress. This can be done either by amending HIPAA directly or through the passage of a separate national data privacy law that works alongside HIPAA. Current proposals by Congress go with the latter option, but it would be preferable for Congress to amend HIPAA so that we have one data privacy law that regulates general data and health data. Having two separate federal laws on data would result in some health data being regulated by HIPAA and other health data being regulated by the new federal data privacy law.

HIPAA does not regulate a lot of data which would constitute health data and it cannot preempt what it does not cover. Even for the data that it does cover, HIPAA does not preempt state law to the extent that state law provides stronger protections.[32] Preemption occurs when state law provides for something that is directly contrary to something that HIPAA regulates, but HIPAAs sectoral coverage means that this conflict will not occur for a large amount of health data.[33]

Increasing what data HIPAA covers and how strongly that data is protected would then lead to a preemption of state privacy law. Congress can

---

[31] Cal. Civ. Code § 56.05(j).
[32] 45 C.F.R. § 160.202.
[33] *Id.*

preempt by way of conflict, express, or field preemption,[34] and Congress can be clear in the statute if they expressly want to preempt state law on the issue and to what extent.[35] An amended HIPAA should try to preempt on most or all issues so that businesses will usually only need to follow one uniform law. Amending HIPAA now would cool the data privacy issue and likely cause states that are in the process of drafting their own state data privacy law to drop the issue entirely. State legislators would not feel the need to act knowing that the gap has been filled by Congress. Privacy law is one of the few areas on capitol hill that garners bipartisan support, and with the rush by states to pass their own data privacy law, the time to amend HIPAA is now.[36]

It is not enough to call for the passage of a new federal law without discussing what should be in it. For the sake of brevity, I will only focus on the two main issues that are preventing a federal data privacy law from being passed. The first issue is what data should be covered and how far should a federal data privacy law preempt state law, and the other issue is whether there should be a private right of action in such an amended law.

IV. HIPAA DOES NOT COVER ALL HEALTH DATA

HIPAA needs an extensive overhaul and this paper will not be able to cover all of the reforms needed. This section will focus on reforming the scope of data that HIPAA should cover. As stated before, the current federal proposals would leave HIPAA unaffected and act as separate data privacy law. As seen with the confusion between the CCPA, HIPAA, and CMIA, the preferable option would be for Congress to amend HIPAA directly so that the nation would have one federal law to comply with. Broadening HIPAA's coverage to cover all sensitive data generally would make compliance easier and destroy the confusing sectoral coverage regime. As I will discuss below, this is also the only effective means of regulating all health data because data science is constantly redefining and broadening the scope of what qualifies as health data.

A. A UNIFORM HEALTH DATA SCHEME MUST COVER DATA BROADLY TO COVER ALL HEALTH DATA

[34] Murphy v. Natl. Collegiate Athletic Ass'n, 138 S. Ct. 1461, 1480 (2018).

[35] CONG. RESEARCH SERV., LSB10213, CALIFORNIA DREAMIN' OF PRIVACY REGULATION: THE CALIFORNIA CONSUMER PRIVACY ACT AND CONGRESS, (Nov. 2018).

[36] Jessica Davis, *Senators Push for Bipartisan Federal Privacy Law, But Still Divided*, HEALTH IT SECURITY (Dec. 6, 2019), https://healthitsecurity.com/news/senators-push-for-bipartisan-federal-privacy-law-but-still-divided.

HIPAA should cover all health data regardless of whose hands it's in, but it is insufficient to merely move away from the sectoral approach. Legislators will additionally need to redefine what health information is because researchers are currently learning that nearly all information about an individual could qualify as data that relates to an individual's health.

As explained before, HIPAA only covers PHI. PHI's definition contributes to HIPAAs sectoral coverage as explained earlier, but another issue with PHI's definition is that it does not cover all data which relates to health. With the sectoral parts of the definition aside, the regulations further clarify that PHI covers "individually identifiable health information" which is a subset of health information which includes:

> "the individual's past, present or future physical or mental health or condition, the provision of health care to the individual, or the past, present, or future payment for the provision of health care to the individual, and that identifies the individual or for which there is a reasonable basis to believe it can be used to identify the individual. Individually identifiable health information includes many common identifiers (e.g., name, address, birth date, Social Security Number) …The Privacy Rule excludes from protected health information…certain other records"[37]

In other words, HIPAA generally protects information which: 1) has not been de-identified because identifiers like your name or Social Security Number have not been removed, and 2) relates to physical and/or mental health information which is created or received by a healthcare entity, and 3) is not expressly excluded by the law. For example, the law expressly excludes individually identifiable health information that is already covered by the Family Education Rights and Privacy Act.[38] In practice, this means that HIPAA generally only protects your medical records and claims information that the hospital sends to bill for your procedure. This is what we may think of as traditional health data, but there is a growing use of non-traditional health data that might be just as important.

The biggest form of non-traditional health data are known as social determinants of health (SDOH) which broadly look at many social factors like wealth, education, workplace safety, etc. to make various determinations about your health.[39] SDOH show signs of great promise in helping understand

---

[37] 45 C.F.R. § 160.103.

[38] *Id.*

[39] *Social Determinants of Health: Know What Affects Health*, CDC, https://www.cdc.gov/socialdeterminants/index.htm.

and fix the various healthcare issues Americans are facing today.[40] For example, some studies[41] have shown strong links between SDOH and hospital readmissions, which hospitals are now taking seriously to reduce their readmission rates.[42] HIPAA does not cover SDOH or other non-traditional forms of health data, but the CCPA can.

The CCPA takes a broad approach to data privacy, regulating any "personal information" of "consumers" that is collected by a "business."[43] "Consumer" means a California resident and "business" includes certain companies based on their aggregate annual earnings or level of activity in California.[44] The CCPA will apply to most major businesses because the "business" definition includes companies that earn more than $25 million annually.[45] "Personal information" is extremely broad, and includes "information that identifies, relates to, describes, or is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household."[46] The CCPA does exempt some things such as data de-identified under the CCPA's de-identification standard.[47] However, the CCPA's broad definition will likely include many forms of SDOH that are not fully de-identified and therefore could be reasonably linked to a specific consumer or household. HIPAA largely provides a uniform national scheme for traditional health data (the CCPA steps back for data that HIPAA applies to)[48] but the CCPA and other state laws will lead to a patchwork scheme on the use of SDOH and other nontraditional forms of health data. The issue is that SDOH can seemingly include any data because studies have shown that everything from your TV habits to your online ordering history can have a calculable impact on your health.[49] This data can be used to improve health, but it can also be used to harm your health. Some

---

[40] Study: Social Risk Factors Linked to Hospital Readmissions, Penalties, AMERICAN HOSPITAL ASS'N (Mar. 12, 2019), https://www.aha.org/news/headline/2019-03-12-study-social-risk-factors-linked-hospital-readmissions-penalties.

[41] Jacqueline LaPointe, *Social Determinants of Health Impact Hospital Readmission Rates*, REVCYCLE INTELLIGENCE (Mar. 20, 2019), https://revcycleintelligence.com/news/social-determinants-of-health-impact-hospital-readmission-rates.

[42] Maria Castellucci & Megan Caruso, *Hospitals Want Readmissions Program to Account for Social Determinants*, MODERN HEALTHCARE (May 25, 2019), https://www.modernhealthcare.com/safety-quality/hospitals-want-readmissions-program-account-social-determinants.

[43] CONG. RESEARCH SERV., LSB10213, CALIFORNIA DREAMIN' OF PRIVACY REGULATION: THE CALIFORNIA CONSUMER PRIVACY ACT AND CONGRESS, (Nov. 2018).

[44] *Id.*

[45] *Id.*

[46] *Id.*

[47] *Id.*

[48] Cal. Civ. Code § 1798.145(c)(1)(B).

[49] Marshall Allen, *Health Insurers Are Vacuuming Up Details About You — And It Could Raise Your Rates*, PROPUBLICA (July 17, 2018), https://www.propublica.org/article/health-insurers-are-vacuuming-up-details-about-you-and-it-could-raise-your-rates.

companies are looking at using SDOH to more accurately determine your insurance rates, which are expected to raise rates for low-income minority families.[50]

SDOH data and other non-traditional forms of health data should be covered and regulated by a federal law that applies broadly to all data, but the federal law should also preempt state law to avoid a patchwork data privacy regime. America needs a law that regulates negative uses of this data while also providing a single compliance pathway for researchers who desire to use SDOH to improve health. SDOH's breadth is so large that Congress will need to pass a general data privacy statute just to regulate health data. Luckily, Congress is currently looking at two general federal privacy statutes. Both would broadly regulate data to sufficiently cover SDOH, but only one of the bills largely preempts state law.

Senator Maria Cantwell introduced the Consumer Online Privacy Rights Act (COPRA), which would regulate data that is linked or reasonably linkable to an individual or consumer device.[51] COPRA acts similarly to HIPAA in terms of preemption in that it does not preempt state law that affords greater protection to consumers.[52] The alternative bill, introduced by Senator Roger Wicker, is the United States Consumer Data Privacy Act of 2019 (CDPA).[53] CDPA takes the correct approach by preempting many state laws on data privacy, creating a true national data privacy scheme.[54] Individuals and companies would need to only look at either this law or HIPAA to understand their rights and responsibilities. COPRA would incentivize states to continue passing new data privacy laws which would make compliance difficult and stifle research.

Opponents to the CDPA might argue that state laws like the CCPA already provide many exemptions to certain forms of data. The issue is that many of the available exemptions and right-to-deletion exceptions are highly limited. For example, a business can ignore a consumer's deletion request and retain the personal information of a consumer, if the deletion would seriously impair research goals.[55] The issue is that this exception is highly limited and does not allow a business to refuse a deletion request if such research is to be used for any commercial purposes.[56] To return to the hospital readmission example, LexisNexis Risk Solutions is looking at various SDOH to reduce

---

[50] *Id*.

[51] Consumer Online Privacy Rights Act, S. 2968, 116 Cong. § 2(8)(A) (2019).

[52] *Id.* at § 302(c).

[53] United States Consumer Data Privacy Act of 2019, S. ___, 116th Cong. (Discussion Draft Nov. 27, 2019), *available at* https://aboutblaw.com/NaZ.

[54] *Id.* at § 404.

[55] Cal. Civ. Code § 1798.105(d)(6).

[56] *California Consumer Privacy Act: A Compliance Guide*, SKADDEN LLP (Mar. 2019), https://www.skadden.com/media/files/publications/2019/03/cybersecurity_california_privacy.pdf?la=en.

readmission rates to improve health but also to improve hospital reimbursement under the Hospital Readmissions Reduction Program.[57] Another researcher doing similar research in California and who is not covered by HIPAA might run into issues with the CCPA's stance on commercial use. Other research that happens to have a commercial purpose despite being in the best interest of the public, might fail under this right-to-delete exception.

Even if the CCPA and other state laws relaxed this and other exceptions, it would still be substantially more burdensome for a researcher to find out how to comply with fifty different state laws as opposed to one or two federal laws. Data based on a California resident would be regulated by the CCPA, data coming from a Washington resident would be subject to a Washington data privacy law, and so on. The CCPA does have a step back provision[58] on data that HIPAA applies to, but Congress will need to pass a federal law that covers all data that can be reasonably linked to a person if they want to cover health data regulated under one law.

V. PRIVATE RIGHT OF ACTION AND ENFORCEMENT

The other big barrier to passing a new federal data privacy law involves whether legislators should include a private right of action. A private right of action might ensure greater enforcement and therefore greater protection of health data and other sensitive information, but there are also substantial risks with including such a provision. This section will look at the pros and cons of including a private right of action under a new health data privacy scheme. This analysis can help one consider whether it would be wise to amend HIPAA to include a private right of action, or whether a new standalone federal data privacy law should include it. HIPAA technically lacks a private right of action which has led to enforcement issues, and this might lead some to demand that a new federal data law (either a standalone law or one that amends HIPAA) include one. The last subsection will show that HIPAA might indirectly have a private right of action because of how it works with other federal laws. This indirect private right of action might mean that HIPAA can now be effectively enforced through private lawsuits.

A. PRIVATE RIGHT OF ACTION PROS; A LOOK AT HIPAA'S WEAK PENALTIES AND POOR ENFORCEMENT HISTORY

[57] Mike Miliard, *LexisNexis Taps Social Determinants to Help Hospitals Predict Readmissions*, HEALTHCARE IT NEWS (Mar. 2, 2018), https://www.healthcareitnews.com/news/lexisnexis-taps-social-determinants-help-hospitals-predict-readmissions.

[58] Cal. Civ. Code § 1798.145(c)(1)(B).

HIPAA provides the public with a variety of rights, but a private right of action is not one of them. The law allows civil and criminal penalties to be enforced against violators, but these actions can only be brought by HHS or a state's attorney general.[59] Since the law's inception, private individuals have attempted to bring HIPAA claims, but courts have unanimously rejected them. The 8th Circuit,[60] 5th Circuit,[61] D.C. Circuit,[62] and other courts have consistently affirmed that no private right of action exists. This line of case law was recently confirmed by the D.C. District Court which found that courts were in agreement that the law contained no such right.[63] An individual is left only with the ability to submit a complaint to the government and hope that the government proceeds to enforce the claim.[64] This has caught many off guard because many members of the public assumed that they could sue for a HIPAA violation since the violation involves their data.[65] So, a private right of action clearly does not exist, but is this a good thing?

HHS has been criticized in the past for failing to enforce the act in a satisfactory manner, but the office has recently made good faith attempts to take the law more seriously.[66] To date, HHS has settled or imposed penalties totaling around $112 million.[67] This number includes $6,193,000 in 2015, $23,504,800 in 2016, $20,393,200 in 2017, $28,683,400 in 2018 and $15,270,000 in 2019.[68] The office deserves commendation for ramping up enforcement but these numbers still leave a lot to be desired. The $112 million total seems a lot smaller when considering that the privacy rule went into effect in April of 2003, which was almost two decades ago.[69] Additionally, HHS has brought less than 100 cases total for all years that the law was in effect,[70] despite there being on average many millions of breached

---

[59] 42 U.S.C. §§ 1320d–5.

[60] Adams v. Eureka Fire Prot. Dist., 352 F. App'x 137, 138–39 (8th Cir. 2009).

[61] Acara v. Banks, 470 F.3d 569, 571–72 (5th Cir. 2006).

[62] Johnson v. Quander, 370 F.Supp.2d 79, 100 (D.D.C. 2005) (dismissing HIPAA claim because no private cause of action existed), *aff'd*, 440 F.3d 489 (D.C. Cir. 2006).

[63] Lee-Thomas v. LabCorp, 316 F. Supp. 3d 471, 474 (D.D.C. 2018).

[64] 45 C.F.R. § 160.306.

[65] *Federal Court Affirms No Private Right of Action*, RELIAS MEDIA (Sept. 1, 2018), https://www.reliasmedia.com/articles/143198-federal-court-affirms-no-private-right-of-action.

[66] Roger Grimes, *HIPAA has no Teeth*, CSO (June 5, 2006), https://www.csoonline.com/article/2641625/hipaa-has-no-teeth.html.

[67] *Enforcement Highlights: Enforcement Results as of February 29, 2020*, U.S. DEP'T HEALTH & HUM. SERVS. (Mar. 5, 2020), https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/data/enforcement-highlights/index.html.

[68] *HIPAA Fines Listed by Year*, COMPLIANCY GROUP, https://compliancy-group.com/hipaa-fines-directory-year/.

[69] *Enforcement Highlights: Enforcement Results as of February 29, 2020*, U.S. DEP'T HEALTH & HUM. SERVS. (Mar. 5, 2020), https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/data/enforcement-highlights/index.html.

[70] *Id.*

healthcare records every year.[71] Enforcement actions by various state attorney generals have occurred, but they are similarly limited in the number of actions brought and dollar amounts obtained.[72]

These government enforcement statistics also pale in comparison to amounts won through private actions under other data privacy laws. While it is not perfectly comparable to HIPAA, Illinois does have a biometric data protection law called the Biometric Information Privacy Act (BIPA) which has a private right of action[73] and has seen much greater enforcement. BIPA enforcement actions have greatly outpaced HHS HIPAA enforcement actions, with over 200 BIPA cases in 2018 and 2019 alone.[74] One BIPA case against Facebook has resulted in a massive $550 million settlement[75] (pending approval by the court) which would award some class members up to $200 each. This highlights another issue with HIPAA's current enforcement model because HIPAA does not reward money to any of the individuals harmed. All the money awarded under HIPAA goes to the government. A remedy that does not make the aggrieved party whole can be attacked as a poor one.

Regulated parties likely feel less urgency to comply with laws that have poor enforcement, and HIPAA non-compliance is at an all-time high. Individuals have a mandatory right of access under HIPAA to get a copy of their PHI in a designated record set.[76] This is a very clear right and is subject only to some minor exceptions, for example, one cannot get access to the information compiled in reasonable anticipation for use in certain trials.[77] Despite this fact, a study from medRxiv found that a majority of providers fail to completely comply with this access right.[78] Some outlets have reported people waiting many months to get their records, with some paying as much as $541.50 to get access.[79] The problem came to a boiling point when HHS

---

[71] *November 2019 Healthcare Data Breach Report*, HIPAA JOURNAL (Dec. 20, 2019), https://www.hipaajournal.com/november-2019-healthcare-data-breach-report/.

[72] Mary Chaput, *State Attorney General HIPAA Enforcement Ramps Up*, CLEARWATER COMPLIANCE (June 27, 2019), https://clearwatercompliance.com/blog/state-attorney-general-hipaa-enforcement-ramps-up/.

[73] 740 Ill. Comp. Stat. 14/20.

[74] Richard Winter et al., *BIPA Update: Class Actions on the Rise in Illinois Courts*, HOLLAND & KNIGHT (July 22, 2019), https://www.hklaw.com/en/insights/publications/2019/07/bipa-update-class-actions-on-the-rise-in-illinois-courts.

[75] Devin Coldewey, *Facebook Will Pay $550 Million to Settle Class Action Lawsuit Over Privacy Violations*, TECH CRUNCH (Jan. 29, 2020), https://techcrunch.com/2020/01/29/facebook-will-pay-550-million-to-settle-class-action-lawsuit-over-privacy-violations/.

[76] 45 C.F.R. § 164.524(a).

[77] *Id.*

[78] Jessica Davis, *Majority of Providers Fail to Fully Comply with HIPAA Right of Access*, HEALTH IT SECURITY (Aug. 16, 2019), https://healthitsecurity.com/news/majority-of-providers-fail-to-fully-comply-with-hipaa-right-of-access.

[79] Harlan Krumholz, *Opinion: It's Your Right To See Your Medical Records. It Shouldn't Be This Hard To Do*, NPR (Aug. 28, 2019), https://www.npr.org/sections/health-

Secretary Alex Azar stated that even he could not easily access his health records.[80] HHS's Office of Civil Rights (OCR) has stated that the patient record access issue ranks third in their most investigated HIPAA issues list, but only recently has OCR taken serious enforcement action against providers with record access issues.[81] OCR actions under HIPAA against one provider resulted in a negligible $85,000 fine, whereas a separate access suit brought by private plaintiffs under state law for similar issues came to a close with a massive $35.4 million settlement.[82]

The CCPA remedies these issues not only with a private right of action but by also having greater penalties. Under the CCPA, a data breach could allow for claims for damages between $100-$750 per violation which would be multiplied "per consumer per incident or actual damages, whichever is greater."[83] A class action would multiply the damages by each person affected by the breach, likely resulting in multi-million-dollar suits. Enforcement becomes even more severe if the California Attorney General sues, a scenario that would raise penalties up to $2,500 per violation or $7,500 per violation if the breach was intentional.[84]

HIPAA's civil penalties break down into four categories based on culpability. The penalties have been modified over the years and they carry the following monetary penalties:

> 1. Violations with no knowledge carry a penalty of $100-$50,000 per violation, up to a maximum of $25,000 annually.[85]
> 2. Violations due to reasonable cause carry a penalty of $1,000-$50,000 per violation, up to a maximum of $100,000 annually.[86]
> 3. Violations due to willful neglect which are then timely corrected, carry a penalty of $10,000-$50,000 per violation, up to a maximum of $250,000 annually.[87]
> 4. Violations due to willful neglect that are not timely corrected, carry a penalty of $50,000 per violation, up to a maximum of

shots/2019/08/28/754725843/opinion-its-your-right-to-see-your-medical-records-it-shouldn-t-be-this-hard-to-.

[80] Patrick Malone, *A Top U.S. Health Official can't get his. Which is why we Need Records Reforms*, PROTECT PATIENTS BLOG (Feb. 13, 2020), https://www.protectpatientsblog.com/a-top-u-s-health-official-cant-get-his-which-is-why-we-need-records-reforms/.

[81] *Beware: Charging Improper Fees for Patient Access to Records Can Cost Providers Big*, HALL RENDER (Sept. 13, 2019), https://www.hallrender.com/2019/09/13/beware-charging-improper-fees-for-patient-access-to-records-can-cost-providers-big/.

[82] *Id.*

[83] Cal. Civ. Code § 1798.150.

[84] Cal. Civ. Code § 1798.155.

[85] 45 C.F.R. § 160.404(b)(2)(i).

[86] *Id.* at (ii).

[87] *Id.* at (iii).

$1.5 million annually.[88]

Some maximum annual penalty amounts under HIPAA were reduced from what they previously were, with some penalty maximums being reduced as much as 6,000 percent.[89] Also note that the penalty amounts are adjusted for inflation. For example, the $25,000 cap increased to $28,526 in 2018.[90]

The annual penalty caps are significant because HIPAA violations, like most other data violations, usually concern hundreds or thousands of patient data breaches.[91] This often means that the penalties will rack up way past the point of the annual cap, making that annual cap the highest liability that violators face. The HIPAA penalty range for even the lowest violation (no knowledge) of $100-$50,000 per violation seems to greatly surpass the per violation penalties under the CCPA. But the CCPA will likely still result in much greater penalty awards because the CCPA does not have an annual cap.

These low annual caps largely explain why so many HIPAA settlements result in relatively low fines compared to the number of affected individuals. The largest HIPAA settlement in history involved a $16 million settlement with Anthem because of an ePHI (electronic PHI) breach which affected almost 79 million individuals[92], coming out to about $5 per breach. A CCPA violation involving the same number of individuals would result in much higher fines even in a worst-case scenario. If the suit was brought by a private party and the lowest penalty amount applied ($100 per violation), the award sought could reach $7.9 billion. A company facing that level of liability would obviously not settle unless opposing counsel was willing to settle for a fraction of that amount, but hypothetical settlement seeking a mere 1% of $7.9 billion would still greatly exceeds HHS's settlement with Anthem.

Some may argue that the monetary gap in HIPAA enforcement can be supplanted by the criminal penalties it carries, but this government tool has its own issues. There are criminal penalties under HIPAA for severe violations which could fill in the enforcement gap that the minimal fines provide.[93] The criminal penalties as applied to individuals are as follows:

---

[88] *Id.* at (iv).

[89] Adam Greene et al., *HHS Reinterprets (and Significantly Lowers) Annual Penalty Caps for HIPAA Violations*, DAVIS WRIGHT TREMAINE LLP (Apr. 30, 2019), https://www.dwt.com/insights/2019/04/hhs-reinterprets-and-significantly-lowers.

[90] *Id.*

[91] *November 2019 Healthcare Data Breach Report*, HIPAA JOURNAL (Dec. 20, 2019), https://www.hipaajournal.com/november-2019-healthcare-data-breach-report/.

[92] *Anthem Pays OCR $16 Million in Record HIPAA Settlement Following Largest U.S. Health Data Breach in History*, U.S. DEP'T HEALTH & HUM. SERVS. (Oct. 15, 2018), https://www.hhs.gov/about/news/2018/10/15/anthem-pays-ocr-16-million-record-hipaa-settlement-following-largest-health-data-breach-history.html.

[93] 42 U.S. Code § 1320d–6(b).

> 1. For individuals who violate unknowingly or with reasonable cause, a fine of no more than $50,000 and/or imprisonment for not more than 1 year.[94]
>
> 2. For individuals who committed the offense under false pretenses, a fine of no more than $100,000 and/or imprisonment for not more than 5 years.[95]
>
> 3. For individuals who committed the offense with intent to sell, transfer or use the individually identifiable health information for commercial advantage, personal gain, or malicious harm, a fine of no more than $250,000 and/or imprisonment for not more than 10 years.[96]

The government could use this tool to their advantage, but criminal enforcement of HIPAA is very rare.[97] This is because any criminal actions must be pursued by the Department of Justice (DOJ). The DOJ has complained that HIPAA actions take a significant amount of time and effort to investigate and prosecute.[98] This may explain why there have been few criminal enforcement actions despite the hundreds of criminal referrals that OCR has made to the DOJ.[99]

B. PRIVATE RIGHT OF ACTION CONS; A LOOK AT PRIVATE ENFORCEMENT OF OTHER PUBLIC PROTECTION STATUTES

Merely covering and protecting data is not enough. Data privacy laws also need to determine how protected that data is. The CCPA provides a private right of action[100] as does COPRA,[101] meaning that a private individual can sue to enforce a privacy violation. Some argue that a private right of action would improve the enforcement and protection of people's data because the government offices tasked with enforcement already have too much on their plate.[102] This sounds like a valid point, but what really happens

---

[94] *Id.* at (1).

[95] *Id.* at (2).

[96] *Id.* at (3).

[97] Marianne McGee, *Guilty Plea in Rare HIPAA Criminal Case*, BANK INFO SECURITY (Mar. 8, 2019), https://www.bankinfosecurity.com/hipaa-crimes-a-12150.

[98] *Id.*

[99] *Enforcement Highlights: Enforcement Results as of February 29, 2020*, U.S. DEP'T HEALTH & HUM. SERVS. (Mar. 5, 2020), https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/data/enforcement-highlights/index.html.

[100] Cal. Civ. Code § 1798.150(a)(1).

[101] Lauren Feiner, *Senate Democrats Reveal New Digital Privacy Bill that Would Strengthen the FTC's Enforcement Powers Over Tech Companies*, CNBC (Nov. 26, 2019), https://www.cnbc.com/2019/11/26/senate-democrats-reveal-new-copra-digital-privacy-bill.html.

[102] Adam Schwartz, *Sen. Cantwell Leads With New Consumer Data Privacy Bill*, EFF (Dec. 3, 2019), https://www.eff.org/deeplinks/2019/12/sen-cantwell-leads-new-consumer-data-privacy-bill.

when private parties are allowed to enforce public protection statutes? The CCPA is too new and doesn't have much relevant case law, but other California public health statutes and cases are illustrative.

California has other public health statutes that largely mirror or interact with a variety of federal health laws. These California laws often allow for a private plaintiff to sue for harm to the entire class, or the state of California, allowing plaintiffs to extort millions out of companies over nonsensical claims.

Some other states allow parties a private right of action under state disability laws and the Americans with Disabilities Act (ADA), but California's Unruh Civil Rights Act more effectively incentivizes lawyers to bring these claims because the Unruh Act provides for much heavier fines and attorneys' fees.[103] These suits target businesses over minor violations where a ramp is off by a few inches or where a sign is in the wrong spot.[104] Big business chains are seldom bothered by these types of suits because they are more likely to have scores of lawyers to ensure compliance with every public accommodations law, so it's the small businesses that take the hit.[105] These suits are so vexatious that they have been referred to as "drive-by lawsuits" and shakedowns.[106]

California also has the Sherman Food, Drug, and Cosmetics Law,[107] which largely mirrors the federal Food Drug and Cosmetics Act. The federal act does not provide a private right of action to bring a labeling suit, while the California act does provide one through other California laws such as the Consumer Legal Remedies Act, the California Unfair Competition Law, and the False Advertising Law.[108] California courts vary on whether certain suits are preempted under federal law, but these courts will often find that no preemption exists, allowing the state claims to proceed.[109] Many of these suits are clearly frivolous and only intended to net the plaintiffs' attorneys thousands or millions of dollars in settlement deals. Starbucks was sued over allegations that they sold candy with misleading information because the candy was represented as coming from natural sources.[110] The suit failed in

---

[103] Cal. Civ. Code § 52(a).

[104] *What's a "Drive-By Lawsuit"?,* CBS NEWS (Dec. 4, 2016), https://www.cbsnews.com/news/60-minutes-americans-with-disabilities-act-lawsuits-anderson-cooper/.

[105] *Id.*

[106] *Id.*

[107] Cal. Health & Safety Code § 110760.

[108] Brazil v. Dole Food Co., Inc., 935 F. Supp. 2d 947 (N.D. Cal. 2013).

[109] William Stern, *A 2019 Field Guide to Calif. Class Actions*, LAW360 (Jan. 17, 2019), https://www.law360.com/articles/1119650/a-2019-field-guide-to-calif-class-actions.

[110] Ryan Boysen, *Starbucks Evades Consumer Suit Over Labels on Gummies*, LAW360 (Mar. 4, 2019), https://www.law360.com/articles/1134583/starbucks-evades-consumer-suit-over-labels-on-gummies.

part because the packaging was partially transparent, and a customer could look in and see that the gummies were gelatinous and clearly not natural.[111] A beer company was sued and settled for $4.7 million to resolve mislabeling claims which alleged that the company misled consumers to believe that their beer was brewed in Hawaii.[112] Another company settled a mislabeling claim for $4 million over allegations that they improperly labeled their kombucha drinks as non-alcoholic.[113] These claims are flimsy and clearly not brought to protect the public health, but instead to line the pockets of class counsel who take the lion's share of these settlement deals. Frivolous food labeling suits are so common in California that they have been given the "food court" title by some lawyers.[114]

California has become the home of "drive-by lawsuits" and "food court" lawsuits, and they will soon likely be the home to frivolous data breach lawsuits. Private enforcement under the CCPA will likely be no different especially considering that many plaintiffs' personal injury firms are already advertising their specialization in suing for data breaches.[115] HIPAA does not contain a private right of action and maybe it should be kept this way. COPRA would enable the same lawsuits that will take place in California to be brought anywhere in the United States. The excessive amount of tort lawsuits brought in California has been estimated to result in around $11.6 billion in annual costs and nearly 200,000 in lost jobs, resulting in a cumulative "tort tax" of many hundreds of dollars per person in some California cities.[116] These suits increase costs on residents, make it harder to run a business, and make it more difficult for meritorious claims to get their day in court.

C. FINDING MIDDLE GROUND

The issues raised with other public protection statutes that contain a

---

[111] *Id.*

[112] Mike Curley, *Kona Beer Has $4.7M Deal On Tap To Settle False Ad Suit*, LAW360 (Apr. 25, 2019), https://www.law360.com/articles/1153459/kona-beer-has-4-7m-deal-on-tap-to-settle-false-ad-suit.

[113] Lauren Berg, *Whole Foods Customers Reach $4M Kombucha Labeling Deal*, LAW360 (Mar. 18, 2019), https://www.law360.com/articles/1140099/whole-foods-customers-reach-4m-kombucha-labeling-deal.

[114] Sarah Brew et al., *How Food Label Class Actions Fare In Calif. Vs. NY*, LAW360 (Nov. 13, 2019), https://www.law360.com/articles/1218132/how-food-label-class-actions-fare-in-calif-vs-ny.

[115] *Complying with the California Consumer Privacy Act (CCPA)*, SHULMAN ROGERS (Jan. 30, 2020), https://www.shulmanrogers.com/news-events/complying-with-the-california-consumer-privacy-act-ccpa/#_ftn7.

[116] *An Assessment of Excessive Tort Costs in the San Francisco-Oakland-Hayward MSA and California and Potential Economic Benefits of Reform*, PERRYMAN GROUP (Dec. 18, 2018), https://www.perrymangroup.com/publications/infographic/assessment-of-excessive-tort-costs-and-potential-economic-benefits-of-reform/.

private right of action are concerning, but this might not be the case under a new data protection law. Private and government actors in California have taken note of the abuses of some of the beforementioned public protection statutes and are now countering with their own legal theories.

A law firm known for filing hundreds of frivolous ADA lawsuits has been countersued by one of the small businesses that the firm targeted.[117] The business sued under the Racketeer Influenced and Corrupt Organizations Act (RICO) by arguing that the firms were filing fraudulent actions by suing for minor breaches in disability law. The judge in *Saniefar* denied the defendant's motion to dismiss[118] which later resulted in the parties settling.[119] Other businesses have taken note of the use of RICO in defending against bad faith filers, so RICO may serve as an adequate protection against frivolous data privacy suits.[120]

The facts of the *Saniefar* case were especially bad and involved other elements of fraud, so a RICO counterattack might not be a one size fit all defense. The use of RICO against abusive attorneys remains unclear as little case law exists on the topic. Therefore, businesses can instead turn to the government for intervention. The governments in California and Arizona have picked up on this lawsuit abuse and have gone after some of these serial ADA filers.[121]

It is still possible that a private right of action will be abused by greedy attorneys seeking to make a quick buck. To safeguard against this risk, a national health data privacy law could provide for a private right of action which only exists for so many years and then sunsets unless reauthorized. Congress will be able to gauge the effectiveness of the provision and whether it is subject to abuse during these years, allowing them to decide whether to reauthorize such a provision. Another solution is to simply leave out a private right of action and instead create a new office that would focus on bringing these actions. COPRA would give enforcement powers to a new Federal Trade Commission bureau which would focus their efforts on bringing enforcement actions.[122] OCR currently handles HIPAA violations but they already have a lot of other duties on their plate.[123] OCR is also responsible

---

[117] Saniefar v. Moore, 117CV00823LJOBAM, 2018 WL 1305710, at *9 (E.D. Cal. Mar. 13, 2018).

[118] *Id.*

[119] Joyce Hanson, *Ex-Restaurateur Settles RICO Suit Over ADA Claims*, LAW360 (Oct. 24, 2019), https://www.law360.com/articles/1213146/ex-restaurateur-settles-rico-suit-over-ada-claims.

[120] Hannah Albarazi, *LA Developer Accuses Rival Of Using CEQA For Extortion*, LAW360 (June 10, 2019), https://www.law360.com/articles/1167735/la-developer-accuses-rival-of-using-ceqa-for-extortion.

[121] Jim Butler et al., *ADA Defense Lawyer: DA sues to stop abusive ADA litigation*, HOTEL LAWYER (May 21, 2019), https://hotellaw.jmbm.com/riverside-country-da-sues-to-stop-abusive-ada-litigation.html.

[122] Consumer Online Privacy Rights Act, S. 2968, 116 Cong. § 301(a) (2019).

[123] *Office for Civil Rights (OCR) Home*, U.S. DEP'T HEALTH & HUM. SERVS.,

for handling conscience and religious freedom rules, civil rights laws, and different issues relating to the Opioid crisis.[124] Creating a new office and tasking them with the primary duty of handling data breach actions may resolve the current lack of enforcement.

D. A POSSIBLE PRIVATE RIGHT OF ACTION UNDER *ESCOBAR* AND ITS PROGENY

Congress has remained extremely gridlocked so expecting the passage of a new data privacy law to resolve the issues surrounding HIPAA may be unrealistically hopeful. Some data privacy experts may find that the only realistic option is for states to pass laws that regulate data generally, therefore regulating large swaths of health data that are not covered by HIPAA. Though HIPAA does not provide for a private right of action, there may be an indirect private right of action under the False Claims Act (FCA).[125]

The FCA allows the government to recover fraudulently obtained federal funds, which were given over to parties that contracted with and billed the government for any items or services.[126] The FCA allows for qui tam actions, which are actions where a private party brings an FCA claim on behalf of the government.[127] If the government intervenes (takes up the case and expends the energy and resources to win it), the individual who filed the suit is entitled to 15-25% of the proceeds of the action or settlement.[128] If the government does not intervene, the individual who filed the suit is now entitled to 25-30% of the proceeds of the action or settlement.[129] The FCA is now mainly used in the healthcare context where defendants defraud the government under federal healthcare programs in amounts reaching the millions and sometimes billions of dollars.[130] The qui tam provisions are generous and have awarded whistleblowers with hundreds of millions of dollars for reporting false claims.[131] This has ensured strong enforcement of the FCA thus far, and will likely ensure that whistleblowers will continue to come forward in the future. From 1986 to 2018, the government recovered around $59 billion under the FCA with whistleblower accounting for $42.5 billion or 72% of that total

https://www.hhs.gov/ocr/index.html.

[124] *Id.*

[125] 31 U.S.C. § 3729-33.

[126] *Id.*

[127] 31 U.S.C. § 3730(d)(1).

[128] *Id.*

[129] *Id.* at (2).

[130] Mary Jane, *Qui Tam Relators Key to Recovering Billions of Tax-Payer Dollars through FCA Lawsuits*, NATIONAL LAW REVIEW (Jan. 9, 2020), https://www.natlawreview.com/article/qui-tam-relators-key-to-recovering-billions-tax-payer-dollars-through-fca-lawsuits.

[131] *Id.*

amount.[132] To prove an FCA claim, a party must prove the following:

> "(1) that the defendant made a false statement or engaged in a fraudulent course of conduct; (2) such statement or conduct was made or carried out with the requisite scienter; (3) the statement or conduct was material; and (4) the statement or conduct caused the government to pay out money or to forfeit money due."[133]

The first element explains that there must be a false statement or fraudulent action, and liability under this first element can arise under several different theories of what the defendant did. The defendant may have knowingly presented a false claim,[134] and/or knowingly created a false claim,[135] and/or knowingly retained any overpayment[136] and so on. Courts also clarified the different ways in which a claim for payment could be false, finding that a claim's certification could be either legally false or factually false.[137] A factually false certification would involve an incorrect description of what goods or services were provided to the patient.[138] An example of this would be a doctor certifying on a billing form that they performed an expensive surgical operation on the patient when in reality the doctor either performed some other lesser procedure or maybe provided no service at all.

False legal certification breaks down into either express false legal certification or implied legal false certification. The former exists where a claim falsely certifies that it has complied with a particular law, regulation or contractual term, and where compliance with any of those rules exists as a prerequisite to receiving payment.[139] The latter is broader and is based on the notion that submitting a claim for reimbursement by itself implies compliance with any governing federal rules that are a precondition to payment.[140] In the past, there was disagreement between the Circuit Courts of Appeals over the existence and application of an implied false certification theory, but the Supreme Court resolved this circuit split in the *Escobar* case.[141]

The Supreme Court held that an implied false certification can be a basis for a false claim, and therefore an FCA action, but the plaintiff must prove

---

[132] Michael Volkov, *False Claims Act 2018 Year in Review – Making Sense of the DOJ Fraud Statistics*, VOLKOV LAW (Jan. 20, 2019), https://blog.volkovlaw.com/2019/01/false-claims-act-2018-year-in-review-making-sense-of-the-doj-fraud-statistics/.

[133] U.S. ex rel. Harrison v. Westinghouse Savannah River Co., 352 F.3d 908, 913 (4th Cir. 2003).

[134] 31 U.S.C. § 3729(a)(1)(A).

[135] *Id.* at (B).

[136] *Id.* at (G).

[137] U.S. ex rel. Mikes v. Straus, 274 F.3d 687, 697 (2d Cir. 2001).

[138] *Id.*

[139] *Id.* at 698.

[140] *Id.* at 699.

[141] Universal Health Servs. v. U.S. ex rel. Escobar, 136 S. Ct. 1989, 1999 (2016).

that two conditions exist:

> "First, the claim does not merely request payment, but also makes specific representations about the goods or services provided; and second, the defendant's failure to disclose noncompliance with material statutory, regulatory, or contractual requirements makes those representations misleading half-truths."[142]

The first element is relatively straightforward and usually not at issue in the healthcare context because insurance claims forms usually make specific representations about goods or services provided in order to secure proper reimbursement. For example, a doctor who performed knee surgery on a patient will need to select the correct billing code for that operation and/or otherwise affirm that they performed that specific type of surgery to get the corresponding reimbursement. The second element, or materiality element, is more at issue as courts vary on what legal violations are material to the government's decision to pay. Some courts have found that a minor violation of some condition of payment under a federal healthcare program cannot constitute a material violation when the plaintiff has shown no meaningful proof that the government would have not paid the claim had they known of the legal violation.[143] Courts have voided verdicts won by relators under an implied legal certification theory, where the legal violations involved minor legal violations.[144]

The implied legal certification test under the FCA can involve the violation of a wide range of healthcare statutes or regulations, including many of the HIPAA regulations. The real issue is whether a court will find a HIPAA violation to be "material" to the government's decision to pay a claim. Under any implied legal certification argument, the decision as to whether something was material will vary greatly from each case. This is because the facts and judge involved in each case will be different. Sometimes the facts in one defendant's case will show definitive proof that the government was aware of the legal violations but continued to pay claims, clearly showing that those legal violations were not considered material by the government.[145] Even when the defendant cannot show this, the plaintiff is still subject to the risk that different judges will have different opinions on what is material.

While the law is not perfectly clear in this area and every defendant will face different circumstances, it is clear that a HIPAA violation can sometimes underly a private suit under the FCA's implied legal certification test.[146] In

---

[142] *Id.* at 2001.
[143] United States ex rel. Petratos v. Genentech, Inc., 855 F.3d 481 (3d Cir. 2017).
[144] *Id.*
[145] U.S. v. Salus Rehab., LLC, 304 F. Supp. 3d 1258, 1270 (M.D. Fla. 2018).
[146] U.S. v. Am. at Home Healthcare and Nursing Serv., Ltd., 14-CV-1098, 2018 WL 319319, at

United States v. America at Home Healthcare and Nursing Services, Ltd., the plaintiffs alleged violations involving 42 U.S.C. § 1320d-6(a), a provision that criminalizes knowingly using or disclosing PHI without proper authorization.[147] The court realized that this was a case of first impression, and the judge added the following:

> "Second, at this stage of the case, Relator adequately pleads potential FCA liability stemming from the alleged HIPAA violations. Defendants correctly point out that no cases exist in which FCA liability arose from a HIPAA violation. The other side of that coin, however, is that no cases exist saying that FCA liability *cannot* arise from a HIPAA violation."[148]

The judge then found that these HIPAA violations were material because HIPAA violations go "to the very essence of the bargain" between the government and health care providers.[149] That said, the judge seemed to limit his decision by adding that the HIPAA violations, in this case, were uniquely severe. The defendants in this case improperly obtained PHI to use it to solicit patients for additional services that were unnecessary.[150] The court then analogized this practice to a violation of the Anti-Kickback Statute (another healthcare fraud law), by stating that:

> "Although no HIPAA-based FCA cases exist, this Court can analogize to other FCA cases. If "information that a hospital has purchased patients by paying kickbacks has a good probability" of affecting a payment decision, *id.*, then information that a home health agency has pilfered protected health data to solicit patients has a good probability of affecting a payment decision too."[151]

The court then largely rejected the defendant's motion to dismiss and allowed the FCA claims through. This ruling is not clear, and I have not been able to find any other courts which cite this case concerning the HIPAA issues. A plaintiff will likely take this language to mean that HIPAA is always essential to the government's agreement to pay, allowing most HIPAA violations to satisfy the materiality standard. Defense counsel will argue that this case stands for the proposition that the only HIPAA violations that are material are those that are so egregious that they can be compared violations

---

*8 (N.D. Ill. Jan. 8, 2018).

[147] *Id.* at *6.

[148] *Id.*

[149] *Id.* at *7.

[150] *Id.*

[151] *Am. Home Healthcare Nursing Serv.*, 2018 WL 319319, at *7.

of other healthcare fraud laws.

While this is only a District Court decision and therefore not binding on lower courts, it will still be substantially persuasive if any similar case is brought because it seems to be the only case of its kind.

VI. CONCLUSION

Congress needs to act quickly to avoid the looming patchwork threat that will take over. HIPAA is one of the few data privacy laws that currently exist in the United States, but its flaws have been made all too apparent to many state legislators. The CCPA was the first real state data privacy passed in the United States and it has set off a domino effect in all the other states. America has stood at the forefront of data-based medical innovation for a long time, but there is a real risk that this innovation will slow down as each state passes its own data privacy rules. Businesses and researchers will face greater restrictions on what the can and cannot do with data. These parties might have to set aside more of their funds to hire lawyers to ensure compliance with so many different laws, which means that there will be less money to invest in research and development. The public will similarly be harmed as they stand to benefit from more advancements in the field of medicine, not fewer. Around a fifth of the nation's states will likely soon have their own data privacy law which means that Congress is quickly running out of time.[152] Only time will tell whether Congress can muster a bipartisan majority in both chambers to get the job done.

[152] Gopal Ratnam & Dean DeChiaro, *As Congress Stalls on Data Privacy, Big Tech Tangles with States*, ROLLCALL (Feb. 19, 2020), https://www.rollcall.com/2020/02/19/as-congress-stalls-on-data-privacy-big-tech-tangles-with-states/.