JOURNAL OF HEALTH CARE FINANCE

Winter 2019

HIPAA PRIVACY:
Liability Beyond Regulatory Enforcement

Erica Brinkman, MJ, CHPC

INTRODUCTION

In 1996, health care providers, plans and others in the United States invested about $10 to $15 billion on information technology to store and transmit health information.[1] Advances to information technology in the health care industry increased the ability of providers to identify and treat individuals "at risk for disease, conduct vital research, detect fraud and abuse, and measure and improve the quality of care delivered in the U.S."[2] However, the shift from paper medical records to electronic records also came with an increase in the flow of sensitive medical data, which ultimately heightened the need for legal protections for the privacy of this information.[3]

Due to the increase of information technology in all business sectors, came the development of numerous laws, regulations and legislative proposals ranging from financial privacy to safeguarding the privacy of children online.[4] The Congress addressed the opportunities and challenges created with the increase use of information technology in the health care industry in the Health Insurance Portability and Accountability Act of 1996 (HIPAA), Public Law 104-191.[5] Section 262(b) of the Administrative Simplification provision under HIPAA required the Department of Health and Human Services (HHS) to develop recommendations for privacy standards and submit to Congress.[6] The recommendations were to include: (1) the rights individuals should have in regards to their individually identifiable health information; (2) a process on how individuals can exercise these rights; and (3) what uses and disclosures of the information should be with authorization or required.[7] The HHS Secretary submitted the recommendations to Congress on September 11, 1997.[8]

Congress was also working on broad health privacy standards during this time and provided a three-year deadline for the issuance of this legislation under section 264(c)(1) of the Administrative Simplification provisions of HIPAA.[9] This section also directed the Secretary of HHS to publish the proposed rules if there were no privacy legislation enacted by Congress at the end of the three-year deadline.[10] Ultimately, Congress did not enact any federal privacy legislation within the required period.[11] Therefore, the Secretary of HHS published the proposed privacy regulations in 1999 and finalized the rules in December 2000, which required health care entities compliance by April 14, 2003.[12]

---

[1] Federal Register, Part II, Department of Health and Human Services; Office of the Secretary; 45 CFR Parts 160 and 164 Standards for Privacy of Individually Identifiable Health Information; Final Rule; December 28, 2000; page 82465
https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/privacyrule/prdecember2000all8parts.pdf
[2] *Id.*
[3] *Id.*
[4] *Id.* at 82469
[5] *Id.*
[6] *Id.*
[7] *Id.* and 82470
[8] *Id.* at 82470
[9] *Id.*
[10] *Id.* at 82469-82470
[11] *Id.*
[12] https://www.hhs.gov/hipaa/for-professionals

During this promulgation process, the Secretary of the Department of Health and Human Services (HHS) expressed concerns regarding a lack of private right of action under HIPAA.[13] Specifically, the Secretary stated that the lack of a private right of action in the HIPAA legislation would result in covered entities not taking their responsibilities to protect patient information seriously.[14] The HHS Secretary further stated that they would "continue to call upon Congress to pass comprehensive federal privacy legislation."[15] However, approximately 22 years later, there has been no such legislation passed.

While there is no private right of action under HIPAA, there have been cases brought under state law that create one and instances where HIPAA has been determined as a standard of care.[16] Class actions have also become essential for individuals to ensure relief and justice from data breaches.[17] Furthermore, there has been enhancements made to HIPAA with the passing of the Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH).[18]

Therefore, since the strengthening of the HIPAA privacy and security regulations with the implementation of provisions under HITECH and the ability for consumers to remedy HIPAA violations in other methods, a private right of action under HIPAA is not necessary.

This paper will review the enforcement abilities provided under HIPAA, while also comparing it to other federal agencies that have oversight of privacy regulations, or laws, and will explore the opportunities that exists for consumer redress. Part I of this paper will review the enforcement actions available under HIPAA and HITECH while Part II will delve into the enforcement actions to date by the Office for Civil Rights compared to other federal agencies. Part III will compare the different breach notification laws and Part IV will explore other methods of remedy available to consumers, such as state tort actions and class actions. These parts combined will explain why there should not be a private right of action under the HIPAA regulation.

Part I: HIPAA-HITECH: An In-Depth Review of Enforcement Abilities

The HHS published the interim final rule on enforcement, also known as the *Enforcement Regulations*, on April 7, 2003.[19] This interim final rule was the first installment of the Enforcement Regulations and was set to expire on September 16, 2004. [20] The purpose of the interim rule was to provide covered entities with the procedural approach the OCR would use for enforcement of

---

[13] https://www.hhs.gov/hipaa/for-professionals/privacy/index.html; Privacy Rule History, November 3, 1996, HIPAA Privacy Proposed Rule, page 59923

[14] Federal Register, Part IV, Department of Health and Human Services, Office of Secretary, 45 CFR Parts 160 through 164, Standards for Privacy of Individually Identifiable Health Information; Proposed Rule; November 3, 1999; page 59923; file:///C:/Users/erica/AppData/Local/Microsoft/Windows/INetCache/IE/AF2GMZOH/1999nprm.pdf

[15] *Id.* at 59924

[16] *Id.* at 6-76

[17] Article: Standing Together: An Analysis of the Injury Requirement in Data Breach Class Actions; 2016/1017; 52 Gonz. L. Rev. 59*; Daniel Bugni; page 3

[18] https://wayback.archive-it.org/3926/20131018161347/http://www.hhs.gov/news/press/2009pres/10/20091030a.html

[19] Federal Register, Department of Health and Human Services, Office of Secretary, 45 CFR Part 160, Civil Money Penalties: Procedures for Investigations, Impositions of Penalties and Hearings, April 7, 2003, Page 18895

[20] *Id.*

the HIPAA Regulations.[21] On September 15, 2004, HHS extended the rules expiration date by one year to provide more time to develop a more comprehensive set of enforcement rules. [22] The HHS extended the expiration date once again prior to finalizing it on February 16, 2006.[23]

By February 17, 2009, the HITECH Act was enacted as part of the American Recovery and Reinvestment Act of 2009, three years after the finalization of the HIPAA Enforcement Rule, to promote the adoption of meaningful use of health information technology.[24] Subtitle D of the HITECH Act addresses concerns with the privacy and security of electronically transmitted health information by expanding the criminal and civil enforcement abilities under HIPAA.[25] The Acting Director and Principal Deputy Director of OCR at the time, Robinsue Frahbrose, described the changes associated with the implementation of HITECH as a cornerstone for maintaining consumer trust as HHS and other government agencies move forward with meaningful use of electronic exchange of health information.[26]

The Office for Civil Rights (OCR), a department of HHS, is responsible for the implementation and enforcement of the HIPAA Privacy and Security Rule and Subtitle D of HITECH with respect to voluntary compliance activities and civil money penalties (CMP).[27] The Centers for Medicare & Medicaid Services (CMS) has enforcement authority over the other parts of the HIPAA regulations associated with the transactions and codes sets (TCS), the National Employment Identification Number (NPIN), the National Provider Identification (NPI), and the Operating Rules.[28]

With the implementation of provisions under HITECH came the requirement of the HHS-OCR to conduct a formal investigation into complaints when a preliminary review indicates potential willful neglect.[29] The HHS-OCR also can conduct compliance reviews, which is an investigation into alleged violations of HIPAA that is learned through methods other than a reported complaint, such as media accounts[30]. Moreover, with the expansions of enforcement provisions under HITECH, the HHS-OCR has transformed its approach and has increased the number of civil and criminal prosecutions.[31] HITECH also provided authority to the State Attorneys General to bring civil actions on behalf of state residents for violations of HIPAA Privacy and Security Rules.[32]

---

[21] *Id.*
[22] Federal Register, Department of Health and Human Services, Office of Secretary, 45 CFR Part 160, Civil Money Penalties: Procedures for Investigations, Impositions of Penalties and Hearings: Extension of Expiration Date, September 15, 2004, page 55515
[23] Federal Register, Department of Health and Human Services, Office of Secretary, Part III, 45 CFR 160, Civil Money Penalties: Procedures for Investigations, Impositions of Penalties and Hearings; Final Rule; February 16, 2006; page 8391
[24] https://www.hhs.gov/hipaa/for-professionals/special-topics/hitech-act-enforcement-interim-final-rule/index.html
[25] *Id.*
[26] https://www.hhs.gov/hipaa/for-professionals/breach-notification/laws-regulations/final-rule-update/hitech/index.html
[27] https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html?language=en
[28] https://www.gpo.gov/fdsys/pkg/FR-2013-01-25/pdf/2013-01073.pdf; page 14-15
[29] *Id.*
[30] *Id.*
[31] *Id.*
[32] https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/state-attorneys-general/index.html

The OCR does not investigate all complaints received, such as if a complaint alleges violations that occurred prior to the effective date of the rules or if the complaint is filed against an entity that is not required by the law to follow the rules.[33] Additionally, the complaint must allege an activity that violates HIPAA and the report must be within 180 days of knowing of the violation.[34]

The OCR notifies the covered entity and complainant of the acceptance of a complaint and may request additional information, or specific information, to assist in the investigation.[35] It is required under the law that covered entities cooperate with the requests for information.[36] If through the evidence submitted, the OCR determines that there was a violation of the Privacy or Security Rule, OCR will generally resolve the violations through voluntary compliance, corrective action, and/or a resolution agreement.[37] Although most complaints are resolved satisfactorily in one of these methods, those that are not can result in the imposition of civil money penalties (CMPs).[38] Covered entities can request a hearing with the HHS administrative law judge to determine if the evidence supports the penalties imposed.[39] HHS deposits the CMPs into the U.S. Treasury; currently the complainants do not receive any portion of it.[40] However, the HITECH regulations appointed the Comptroller General to issue a report recommending a methodology to determine a percentage of the civil money penalties or monetary settlements collected to share with the harmed individuals.[41] HHS published an advanced notice of proposed rulemaking (ANPRM) in the spring of 2018 to solicit the public's comment on establishing such methodology; however, there has been no further notifications on the ANPRM.[42] Complaints that describe a violation of the criminal provisions under HIPAA are submitted to the Department of Justice (DOJ) for investigation, which will be further explored in upcoming sections.[43]

The most favorable approach of enforcement by the OCR remains to be through the encouragement of voluntary compliance and informal resolutions. HHS-OCR will first attempt to informally resolve, such as through a corrective action plan, when a review indicates non-compliance and there is no evidence of willful neglect.[44] Some believe this approach is not very effective. For example, in the Final Enforcement Rules, under Section 160.304, "Principles for Achieving Compliance," there was one public comment criticizing the HHSs' approach on voluntary compliance with resolution agreements.[45] The commenter stated concerns that this approach has

---

[33] https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/examples/what-ocr-considers-during-intake-and-review/index.html
[34] *Id.*
[35] https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/examples/how-ocr-enforces-the-hipaa-privacy-and-security-rules/index.html
[36] *Id.*
[37] *Id.*
[38] *Id.*
[39] *Id.*
[40] *Id.*
[41] HIPAA Compliance Handbook 2018 page 6-20
[42] https://www.reginfo.gov/public/do/eAgendaViewRule?pubId=201804&RIN=0945-AA04
[43] HIPAA Compliance Handbook 2018; Patricia I. Carter; Wolters Kluwer; page 6-20
[44] *Id.* at page 6-22
[45] Federal Register, Department of Health and Human Services, Office of Secretary, Part III, 45 CFR 160, Civil Money Penalties: Procedures for Investigations, Impositions of Penalties and Hearings; Final Rule; February 16, 2006; page 8394

led to "lax enforcement" and was essentially a "flawed" approach for enforcement of the Privacy Rule.[46]

However, there have been meaningful results with the enforcement of the Privacy Rule that began for most covered entities in April 2003, such as the improvement of privacy practices in the health care industry by requiring covered entities to implement systemic changes.[47] One way this is achieved is through resolution agreements. The resolution agreements act as a contract between the covered entity and the HHS that obligate the covered entity to make reports to the HHS to show compliance with the HIPAA rules.[48] In 2017, there were eight instances of the OCR assigning a resolution agreement and 40 since 2008.[49] These agreements could be compared to the Office of Inspector General's (OIG) Corporate Integrity Agreements (CIA); however, HHS resolution agreements are typically for two to three years while the OIG CIAs are typically for five years.[50]

The requirements of the 2017 agreements included the implementation of more clear policy and procedures; training on policy and procedures; HHS approved security risk assessments and management plans; specific policy and procedures and training around business associates; and implementation of secure device and media controls.[51]

Moreover, the OCR is not the only government entity that uses the voluntary compliance approach. For example, the CMS enforces HIPAA Standards and Transaction under the Administrative Simplification Regulations through education and complaint-driven enforcement.[52] The Department of Labor (DOL) Employee Benefits Security Administration also encourages voluntary compliance with the Employee Retirement Income Security Act (ERISA) by self-correcting violations of the law through the Voluntary Fiduciary Correction Program (VFCP).[53]

Part II: Results of Enforcement Actions under HIPAA-HITECH and Other Federal Privacy Regulations, or Laws

The OCR is not the only federal agency that has oversight authority for consumer privacy. While the OCR provides oversight in relation to the privacy of protected health information (PHI), the Federal Trade Commission (FTC) - Division of Privacy and Identity Protection provides oversight on other types of data privacy, such as consumer financial information.[54] Some of the privacy

---

[46] *Id.*
[47] https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/index.html
[48] HIPAA Compliance Handbook 2018; Patricia I Carter; page 6-31
[49] HIPAA Compliance Handbook 2018; Patricia I Carter; page6-31 and 6-66 through 6-71
[50] Id and https://oig.hhs.gov/compliance/corporate-integrity-agreements/index.asp
[51] Id at 6-66 through 6-71
[52] https://www.cms.gov/Regulations-and-Guidance/Administr,ative-Simplification/Enforcements/index.html
[53] https://www.dol.gov/agencies/ebsa/employers-and-advisers/plan-administration-and-compliance/correction-programs
[54] https://www.ftc.gov/about-ftc/bureaus-offices/bureau-consumer-protection/our-divisions/division-privacy-and-identity

laws enforced by the FTC include section 5 of the FTC Act on unfair and deceptive practices, the Gramm-Leach-Bliley Act (GLBA) and the Children's Online Privacy Protection Act (COPPA).[55]

The GBLA mandates financial institutions, companies that offer consumers financial products or services such as loans, financial or investment advice, or insurance, to inform customers of how they share and how they safeguard sensitive data.[56] The FTC issued the Safeguards Rule as part of the implementation of GBLA.[57] This rule requires financial institutions under FTC jurisdiction to have measures in place to keep customers information secure.[58] Generally, courts have held that there is no private right of action provided to those affected by violations of the privacy provisions under this act.[59] There is also no private right of action available under COPPA.[60] COPPA was first enacted in 1998 and disallows websites and apps from collecting personal information from children under 13 without parents' consent.[61] Further, there is no private right of action under the FTC unfair and deceptive act; therefore, states have added their own consumer protection acts known as "little FTCs" for consumer redress of violations under this act.[62]

There are some differences in how these two agencies are able to enforce the regulations, or laws. For instance, the Secretary of HHS has the authority under section 13410(d) of the HITECH Act to impose civil money penalties that violate the regulation.[63] The Secretary has discretion on the amount of penalty to impose depending upon the nature and extent of the harm resulting from the violation.[64] In comparison, the FTC enforces consumer privacy law through administrative and judicial processes.[65] When the FTC determines during a litigated administrative adjudicatory proceeding that a violation has occurred and the issuance of a final cease, and desist order occurs, the FTC must seek the aid of a court for the issuance of civil penalties or consumer redress.[66]

As for enforcement activities by the FTC, the *Privacy & Data Security Update: 2017* reported there has been over 60 cases against companies for failure to adequately protect consumers' personal data in relation to unfair or deceptive practices since 2002.[67] The report also states there has been almost 30 cases since 2005 for violations of the Gram-Leach-Bliley Act (GLBA) and

---

[55] *Id.*
[56] https://www.ftc.gov/tips-advice/business-center/privacy-and-security/gramm-leach-bliley-act
[57] https://www.ftc.gov/tips-advice/business-center/guidance/financial-institutions-customers-information-complying
[58] *Id.*
[59] 1 Banking Manual Section 4.03 (2nd 2018); page
[60] Top Lessons learned from the Vtech children's privacy breach; Inside Counsel (formerly Corporate Legal Times); December 2015; page 1 and
[61] https://www.ftc.gov/reports/privacy-data-security-update-2017-overview-commissions-enforcement-policy-initiatives; https://www.ftc.gov/system/files/documents/reports/privacy-data-security-update-2017-overview-commissions-enforcement-policy-initiatives-consumer/privacy_and_data_security_update_2017.pdf
[62] Note: The FTC Won't Let Me Be: The Need For A Private Right Of Action Under Section 5 Of The FTC Act, 50 Val. U.L. Rev. 227, Page
[63] https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/enforcementrule/enfifr.pdf page 56124-56125
[64] *Id.*
[65] https://www.ftc.gov/about-ftc/what-we-do/enforcement-authority
[66] *Id.*
[67] https://www.ftc.gov/reports/privacy-data-security-update-2017-overview-commissions-enforcement-policy-initiatives; https://www.ftc.gov/system/files/documents/reports/privacy-data-security-update-2017-overview-commissions-enforcement-policy-initiatives-consumer/privacy_and_data_security_update_2017.pdf

over 100 cases against companies for violating the Fair Credit Reporting Act (FCRA), which resulted in over $30 million dollars in civil penalties.[68] There were over 20 cases reported related to violations under the COPPA that has resulted in millions of dollars in civil penalties.[69]

In comparison, the OCR's website reports that there has been 55 cases as of July 31, 2018 that resulted in CMPs equaling $78,829,182.00.[70] Additionally, it lists the overall number of complaints reported to the OCR by the public being 186,453 with more than 905 compliance reviews and 178,834 cases being resolved.[71] There has also been 26,152 cases requiring changes in privacy practices, corrective actions or technical assistance; 29,042 cases requiring technical assistance and no investigation due to early intervention by the OCR; 11,399 cases finding no violation of the HIPAA Privacy or Security Rule after an investigation; and 112,122 cases that were not eligible for OCR review.[72] Lastly, there has been 688 referrals made to the DOJ for criminal investigations that will be discussed in forthcoming sections.[73]

The annual percentage of increases of complaints to the OCR in the past three years has been 18%, 41%, and 6% for an average increase of nearly 22%. [74] The yearly increases are not expected to subside, which will significantly affect the OCR's ability to keep up.[75] The trend of the increasing caseloads can be attributed to OCR's expanded jurisdiction with Section 1557 and HITECH.[76] The OCR also attributed the increase to the attention on the work conducted through improved outreach and resolution of multiple high impact cases, which is expected to further increase the number of reports received.[77]

Although the Centers for Medicare and Medicaid Services (CMS) ("Centers") does not provide oversight for privacy regulations, or laws, it is worth mentioning the Centers enforcement activities associated with the oversight of the Administrative Simplification provisions under HIPAA. Under HIPAA, the HHS was mandated to establish standard transactions for covered entities to streamline the communications between providers and health plans.[78] Four standards were adopted, transactions for healthcare administration and pharmacy claims; operating rules that support the transactions; unique identifiers for providers, health plans, and employers; and code sets associated with diagnosis and procedures.[79] Similar to the OCR, the CMSs' enforcement approach is through voluntary compliance and complaints.[80] CMS publishes monthly reports on their website that describe the number of complaints received, type of complaint, and how many

---

[68] *Id.*
[69] *Id.*
[70] https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/data/enforcement-highlights/index.html
[71] https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/data/enforcement-highlights/index.html
[72] *Id.*
[73] *Id.*
[74] https://www.hhs.gov/sites/default/files/fy2017-budget-justification-ocr.pdf?language=es; page 22
[75] *Id.*
[76] *Id.*
[77] *Id.*
[78] https://www.cms.gov/Regulations-and-Guidance/Administrative-Simplification/HIPAA-ACA/Downloads/AboutAdminSimpFactSheet20171017.pdf
[79] *Id.*
[80] https://www.cms.gov/Regulations-and-Guidance/Administrative-Simplification/Enforcements/index.html

are closed or active.[81] For the months of January 2018-September 2018, the CMS has received on average 56 complaints a month.[82] Unlike the FTC and similar to HIPAA, individuals can file a complaint electronically on the agencies website.[83]

Referrals to the Department of Justice

As briefly discussed in previous sections, HIPAA complaints that describe an action that could be a violation of criminal provisions under HIPAA, are referred to the DOJ for review and action.[84] A criminal penalty of up to $50,000 and/or imprisonment for up to one year can occur when an individual knowingly and in violation of the HIPAA Administrative Simplification provisions either: "uses or causes to be used a unique health identifier; obtains individually identifiable health information relating to an individual; or discloses individually identifiable health information to another."[85] There have been several instances of the DOJ bringing suit against individuals for misuse of patient information. A recent case from August 1, 2017 charged a gynecologist, Rita Luthra, after she provided a pharmaceutical sales representative access to patient information, amongst other unlawful behavior.[86] In another case out of Tyler, Texas, a former hospital employee, Joshua Hippler, plead guilty on August 28, 2014 for the misuse of patient information and was sentenced to 18 months in federal prison, three years of probation and $12,000 in restitution.[87] In an earlier case from August 2012, convicted a medical equipment company owner for the misuse of patient information and healthcare fraud, which resulted in 12 years in federal prison and $1.3 million dollars seized.[88]

Enforcement by State Attorneys General

Under Section 13410(e) of the HITECH Act, State Attorneys General (SAG) was provided authority to obtain damages on behalf of state residents or to enjoin further violations of the HIPAA Privacy and Security Rules.[89] The SAG must have reason to believe that the states resident(s) has been or is threatened or adversely affected by an individual failure to abide by the HIPAA Privacy and Security Regulations.[90] To assist SAG's to use this authority the OCR has developed computer based training that is available on their website.[91] There is the general requirement that SAG's

[81] https://www.cms.gov/Regulations-and-Guidance/Administrative-Simplification/Enforcements/HIPAAEnforcementStatistics.html
[82] *Id.*
[83] https://asett.cms.gov/ASETT_HomePage
[84] https://www.hhs.gove/hipaa/for-professionals/compliance-enforcement/examples/how-ocr-enforces-the-hipaa-privacy-and-security-rules/index.html; 42 USC 1320d-6
[85] HIPAA Compliance Handbook 2018; Patricia I. Carter; Wolters Kluwer; page
[86] https://www.justice.gov/usao-ma/pr/springfield-doctor-sentenced-illegally-sharing-patient-medical-files
[87] 6:14cr18, USA v Hippler; US District Court Criminal Docket; US District Court for the Eastern District of Texas; (Tyler); Retrieved 04/11/2-18 and https://www.justice.gov/usao-edtx/pr/former-hospital-employee-sentenced-hipaa-violations
[88] https://www.justice.gov/usao-ma/pr/springfield-doctor-sentenced-illegally-sharing-patient-medical-files
[89] https//www.hhs.gov/for-progessionals/compliance-enforcement/state-attorneys-general/index.html
[90] HIPAA Compliance Handbook 2017; Patricia I. Carter; Wolters Kluwer; page 6-9
[91] https//www.hhs.gov/hipaa/for-professionals/compliance-enforcement/state-attorneys-general/index.html

report to the OCR when enforcing the HIPAA Privacy and Security Rule for collaboration.[92] The SAG can request ongoing and concluded investigation results to assist in enforcement activities.[93]

There have been several instances of SAG's using their authority under HITECH to enforce HIPAA Privacy and Security Regulations. The first SAG to enforce HIPAA was in Connecticut in January 2010.[94] Connecticut SAG sued Health Net, a health plan, after a portable computer disc that contained 1.5 million individuals went missing.[95] A settlement was reached in July 2010 for $250,000 to the state and a corrective action plan.[96] The Connecticut AG entered into a second settlement in November 2015 after Hartford Hospital and one of its business associates were involved in a HIPAA breach.[97] This particular breach occurred in 2012 and involved the theft of an unencrypted laptop from the home of the business associates employee.[98] This settlement was for $90,000 to the state and a corrective action plan.[99]

The most active SAG has been in Massachusetts with five cases with settlements ranging from $40,000 to $750,000.[100] In January 2012, a Minnesota Attorney General filed a lawsuit directly against a business associate, which was the first time this has ever occurred.[101] This case arose from the theft of a laptop that contained sensitive health information of 23,531 patients.[102] The business associate agreed to pay $2.5 million dollars to the state and ceased business operations for two years.[103] In Indiana, the SAG took action in 2015 after a dentist improperly disposed of records belonging to 5,600 patients.[104] This case settled with a $12,000 penalty.[105]

Part III: Enforcement of Privacy Laws through the Requirement(s) to Self-Report and Notify of a breach

This section will explore enforcement through the requirement of self- reporting and consumer notification under federal and state regulations, or laws.

Federal Breach Notification Requirements

On February 22, 2010, the FTC began enforcement of the Health Breach Notification Rule that requires certain businesses that are not covered under HIPAA regulations to notify customers and others of a breach of their unsecured, individually identifiable electronic health information occurs.[106] This includes "vendors of personal health information (PHR), PHR related entities, and

---

[92] *Id.*
[93] *Id.*
[94] HIPAA Compliance Handbook 2017; Patricia I. Carter; Wolters Kluwer; Page 6-10
[95] *Id.*
[96] *Id.*
[97] *Id.*
[98] *Id.*
[99] *Id.*
[100] HIPAA Compliance Handbook 2017; Patricia I. Carter; Wolters Kluwer; page 6-11 and 6-12
[101] *Id.* at 6-13
[102] *Id.*
[103] *Id.*
[104] *Id.* at 6-14
[105] *Id.*
[106] https://www.ftc.gov/tips-advice/business-center/guidance/complying-ftcs-health-breach-notification-rule

third party service providers for vendors of PHRs or PHR related entities."[107] Similar to HIPAA, companies are required to notify the FTC and, under certain circumstances, the media of a data breach.[108] Breaches that affect less than 500 consumers can be reported annually, within 60 days after the end of the calendar year in which the breach occurred.[109] However, when a data breach affects 500 or more individuals, they are required to notify the FTC within 10 business days after discovery while HIPAA allows 60 days after the discovery of a breach.[110] Making reports to the FTC is not easy, companies have to print and send the notification form to a designated FTC official by courier.[111] The FTC will not accept email submissions due to security concerns.[112] The FTC states they will periodically make public a list of breaches that affect 500 or more individuals, but only after the company has notified the consumer.[113] As of the date of this paper, there were two "Health Breach Notices Received by the FTC" found on their website that totaled ten submission of breaches that affected between three individuals up to 568,879 individuals. [114]

As for breaches reported by covered entities under HIPAA, the OCR's *FY2017 Budget Justification Report* stated there has been1,430 breaches affecting more than 500 individuals and 191,052 reports affecting fewer than 500 individuals self-reported to the OCR by covered entities since 2009.[115] When there is a breach that affects 500 or more individuals, the HHS Secretary is required to post them on a public website to comply with section 13402(e)(4) of the HITECH Act. This public site currently lists 2,101 cases that are completed and archived while 411 cases currently remain under review.[116]

Regardless of the repercussions on making reports to the OCR of breaches affecting 500 or more individuals, the number of reports received by the OCR has remained consistent. In the CY 2009 and 2010 Report to Congress, OCR reported they received 45 during the three-month reporting period in 2009 and 207 during the first full reporting year of 2010.[117] After the first full reporting year, the OCR has reported receiving 236 in 2011; 222 in 2012; 294 in 2013, and 277 in 2014.[118] Although the OCR has not published a report after the CY2013-2014, the numbers available on

---

[107] *Id.*
[108] *Id.*
[109] https://www.ftc.gov/system/files/documents/federal_register_notices/2009/08/healthbreachnotificationrulefinal.pdf; page 15
[110] https://www.ftc.gov/system/files/documents/plain-language/draft_breach_notices_received_by_ftc_2015.pdf and https://www.hhs.gov/hipaa/for-professionals/breach-notification/breach-reporting/index.html
[111] https://www.ftc.gov/system/files/documents/federal_register_notices/2009/08/healthbreachnotificationrulefinal.pdf; page 15
[112] *Id.*
[113] *Id.*
[114] https://www.ftc.gov/system/files/documents/rules/health-breach-notification-rule/draft_breach_notices_received_by_ftc_2014.pdf and https://www.ftc.gov/system/files/documents/plain-language/draft_breach_notices_received_by_ftc_2015.pdf
[115] https://www.hhs.gov/sites/default/files/fy2017-budget-justification-ocr.pdf?language=es; *Id.* at page 29
[116] https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf
[117] https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/breachnotificationrule/breachrept.pdf; page 4
[118] https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/breachnotificationrule/breachreport2011-2012.pdf page 4-5 and https://www.hhs.gov/sites/default/files/rtc-breach-20132014.pdf page 6

the OCRs public website suggest the trend has not declined, with approximately, 268 archived for 2015, 318 for 2016, and 231 for 2017.[119]

State Breach Notification Laws

As of March 2018, all 50 states, the District of Columbia, Guam, Puerto Rico and the Virgin Islands have enacted legislation requiring private or governmental entities to notify individuals of security breaches of information when it is personally identifiable.[120] The first state to implement a state level data breach notification law was California, sixteen years ago, in 2002.[121] As explored earlier in this paper, with there being no private right of action provided under the FTC's section 5 on unfair and deceptive acts, state level laws were implemented. The state level unfair and deceptive laws have been effective for all states for over 40 years and have been utilized by state attorney generals and consumers.[122] In the beginning, the state unfair and deceptive laws were slow to invoke; however, their enforcement is now at an impressive level of maturity and strength.[123] The same fate could be expected for the state level data breach notification laws.

The last two states, Alabama and South Dakota, recently implemented state level data breach notification acts earlier this year of 2018.[124] There has been trends in the newly enacted state breach notification laws that are indicative of broader social attitudes toward data breaches.[125] One trend relates to the amount of time an entity has to report a data breach.[126] While some of the older state data breach laws still require notification to occur "as soon as possible and without unreasonable delay," the most recent and revised laws are more specific with notification date ranges between 30 and 60 days after discovery.[127] The removal of the ambiguous phrase reflects a desire by states to limit the discretion allowed as to when they can make notification of the breach.[128] HIPAA requires notification within 60 days after discovery and without unreasonable delay; therefore, the states that require 30 days to make notification and those states that remove "as soon as possible and without unreasonable delay" would be more stringent than HIPAA.[129]

Another trend is with the expansion to the definition of personal information in the majority of the state data breach notification laws.[130] Categories of personal information, such as social security numbers and payment card information, has been consistent among the definitions.[131] One example of the expanded definition is with the Alabama breach notification law. Alabama is more expansive on the definition than other states and includes a resident's name in combination with

---

[119] https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf
[120] http://www.ncsl.org/research/telecommunciations-and-information-technology/security-breach-notification-laws.aspx; page 1
[121] https://fas.org/sgp/crs/misc/R42475.pdf ; page 3
[122] *Id.*
[123] *Id.*
[124] http://www.ncsl.org/research/telecommunciations-and-information-technology/security-breach-notification-laws.aspx; page 1
[125] Developments in State Data Breach Notification Laws; Law 360; July 23, 2018; page 1
[126] *Id.*
[127] *Id.*
[128] *Id.*
[129] https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html
[130] Developments in State Data Breach Notification Laws; Law 360; July 23, 2018; page 1
[131] *Id.*

"any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a healthcare professional."[132] The expansion of more broad definitions of personal information is indicative of changing views of personal information.[133]

A third trend among the state data breach notification laws relates to the requirement to report to state attorney general when a certain threshold of residents are affected.[134] The threshold to report varies between 250 residents up to 1,000 residents.[135] This requirement highlights the expanded roles SAG's have in regulating data security and predicts a more active role they will have in pursing claims of data breaches.[136]

Although not yet a trend, there has been some development in one state that creates a private right of action for consumers affected by a data breach.[137] On June 28, 2018, California passed the California Consumer Privacy Act (CaCPA) that creates a private right of action for any consumer that experience certain unauthorized access and exfiltration, theft, or disclosure of a consumer's non-encrypted or non-redacted private information.[138] The CaCPA has been compared to the European Union's General Data Protection Regulation (GDPR) and provides more than just a private right of action.[139] It also provides an individual the right to know "what information a company has on a data subject including how it is sourced and whether it is disclosed or sold; the right to deletion of personal information; and the right to receive equal service and pricing despite exercising personal rights."[140] Under the CaCPA, affected individuals can be awarded for statutory damages ranging from $100-$750 or for actual damages for unauthorized access and exfiltration, theft, or disclosure due to a business's violation of their duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information.[141]

Together, these trends in the state level data breach notification laws display the states greater involvement to ensure transparency and supervision of data breach actions.[142]

Part IV: Opportunities beyond Regulatory Enforcement

This section will explore the different remedies available to consumers outside of regulatory enforcement.

---

[132] Legislating Cybersecurity: 2018 Adds Patches to the Quilt of Data Privacy Law Across the US; New Jersey Law Journal (online); November 28, 2018 Wednesday; ALM Media Properties; Page 3
[133] Developments in State Data Breach Notification Laws; Law 360; July 23, 2018; page 1
[134] *Id.*
[135] *Id.* At page 2
[136] *Id.* At page 2
[137] *Id.* At Page 2
[138] *Id.*
[139] Legislating Cybersecurity: 2018 Adds Patches to the Quilt of Data Privacy Law Across the US; New Jersey Law Journal (online); November 28, 2018 Wednesday; ALM Media Properties; Page 3
[140] *Id.*
[141] Developments in State Data Breach Notification Laws; Law 360; July 23, 2018; page 2
[142] *Id.*

Privacy Enforcement Abilities under State Laws

Federal courts have been consistent that there is no private right of action under HIPAA and state courts have followed suit; however, there are some instances that a state law may make it possible.[143] The forthcoming paragraphs explore the different ways state courts have enforced HIPAA at the state level.

In the 2007 case, *Webb v. Smart Documents Solutions*, LLC, the Ninth Circuit Court of Appeals in California agreed that there is no private right of action under HIPAA; however, the plaintiffs raised state law claims under the California unfair competition statute that makes violations of other federal and state laws independently actionable.[144] The plaintiffs in *Webb v. Smart Documents Solutions, LLC*, alleged that the charges imposed on patient requests for medical records made on behalf of an attorney were "excessive and unlawful."[145] Specifically, the plaintiffs argued that *Smart* is required to comply with the provisions under HIPAA regardless if the request for records come from the patient, or through the patient's lawyer.[146] *Smart* agreed with the requirement to charge patients only the actual cost of copying; however, argued that a patient relinquishes their protections under HIPAA when the requests come from an attorney.[147] *Smart* charged the plaintiff's attorney a per-page price of $ 0.35, which was more than actual cost of copying; an unexplained "basic fee" of $32.00; and a "retrieval fee" of $15.00.[148] The plaintiff's attorney passed the charges to the plaintiff for payment, which is the standard practice in contingent fee contracts between attorneys and clients.[149] In this particular case, it was concluded that the plaintiff did not successfully allege a HIPAA violation since the fee limitations under HIPAA does not apply to attorneys acting on behalf of the patient; therefore, could not state a claim under the California unfair competition statue, California Unfair Competition Law (UCL), Business & Prof. Code Section 17200 et seq.[150]

Espinoza v. Gold Cross Servs (2010) was a similar case involving patients in Utah who referenced the *Webb* case to bring action against an ambulance company for unjust enrichment after alleging they overcharged for copies of medical records.[151] In this case, the plaintiffs used HIPAA as a standard for setting the allowable fees to charge for copies of records.[152] Similar to *Webb*, the court first agreed that there was no private right of action under HIPAA; however, the court cited the *Webb* case when concluding that states may create their own HIPAA-related causes of action

[143] HIPAA Compliance Handbook 2018 page 6-91
[144] HIPAA Compliance Handbook 2018 page 6-91
[145] *Webb v. Smart Document Solutions*; No. 05-56282; United States Court of Appeals for the Ninth Circuit; January 6, 2006; 2006 US 9th Cir. Briefs LEXIS1244*; page 2
[146] *Id.*
[147] *Id.*
[148] *Id.* At page 3
[149] *Id.*
[150] HIPAA Handbook 2018 page 6-91
[151] *Id.*
[152] *Id.*

by statute.[153] However, the courts analysis determined that Utah had not created a private right of action that would redress HIPAA violations.[154]

There is also opportunities for individuals to pursue liability causes of action at the state level when their protected health information is misused.[155] The causes of actions vary by states and could include liability under state privacy statutes or tort law.[156] Statutory claims under state laws could include state medical records act, consumer fraud act, or through a licensing complaint.[157] Tort claims could include negligence, professional malpractice, breach of fiduciary duty, or invasion of privacy.[158] The next several paragraphs will further explore these types of claims.

The *Acosta v. Byrum* case from 2006 involved a patient, Heather Acosta, in North Carolina who alleged her former employer, a psychiatric clinic, permitted the office manager (Robin Byrum) to improperly disclose her medical record information to a third party without her authorization.[159] Specifically, the plaintiff alleged that the clinic's owner, a physician, allowed Byrum to use his user name and password to access her records numerous times that resulted in the unauthorized disclosure.[160] The plaintiff further argued that the physician violated the hospital systems policy and HIPAA by sharing his user name and password with the office manager.[161] The clinic owner, Dr. Faber, filed a motion to dismiss pursuant to Rules 12(b)(2) and (6) which was granted by the trial court.[162] During appeal, the plaintiff argued that she "sufficiently stated a claim for negligent infliction of emotional distress against Dr. Faber," which the appeals court agreed.[163] In conclusion, the appeals court reversed the trial court decision to dismiss complaint against Dr. Faber and stated that HIPAA was used as evidence of the appropriate standard of care, which is a necessary element in negligence claims.[164]

In *Sorensen v. Barbuto, 2008 UT 8,* the plaintiff sued a driver and insurer for damages after a car accident.[165] In this case, the plaintiff's doctor disclosed his medical record to the defendant and became the defendants' expert witness.[166] The plaintiff sued the doctor for breach of covenant of good faith and fair dealing and in tort.[167] The doctor argued that since the plaintiff placed his personal condition at issue in a lawsuit, he authorized him to have communications with the defense counsel.[168] The defendant further argued that he did not breach his duty of care because his actions were protected under Utah Code section 78-24-8(4) and Rule 506 (d)(1) of the Utah

---

[153] *Id.*
[154] *Id.*
[155] *Id.* Page 6-92
[156] *Id.*
[157] *Id.*
[158] *Id.*
[159] *Acosta v. Byrum*, 638 S.E.2d 246; Court of Appeals of North Carolina; October 11, 2006, Heard in the Court of Appeals; December 19, 2006; filed; No. COA06-106; page 2
[160] *Id.*
[161] *Id.* At page 4
[162] *Id.*
[163] *Id.*
[164] Id At page 8
[165] *Sorensen v. Barbuto*, 2008 UT 8; Supreme Court of Utah; February 1, 2008, Filed; No. 20060816; page 1
[166] *Sorensen v. Barbuto*; Court of Appeals of Utah; August 10,2006, file; case no. 200505501-CA page 1
[167] *Id.*
[168] *Id.* At page 7

Rules of Evidence.[169] The court held that "the statutory privilege has no further effect. Physician-patient and therapist-patient privileges are now exclusively controlled by Rule 506," which defines the physician-patient privileges and any exceptions.[170] The appeals court analysis included the *DeBry* case which involved a husband putting his wife's mental state as a defense in a divorce proceeding.[171] The husband solicited an affidavit from his wife's therapist that was ultimately disclosed without consulting with the wife or getting her consent.[172] In the *DeBry* case, the court held that the patient must be afforded the opportunity to protect under these circumstances and a physician or therapist has an obligation to protect his patient's confidentiality.[173] Therefore, the appeals court in *Sorensen v. Barbuto* held that "ex parte communication between a physician and opposing counsel does constitute a breach of the physician's fiduciary duty of confidentiality."[174]

In 2003, a patient sued St. Mary's Medical Center in West Virginia after the unauthorized disclosure of psychiatric and medical health information to the patient's estranged wife and her divorce lawyer.[175] In this suit, the patient was not alleging a private right of action under HIPAA but was making state tort claims.[176] The hospital argued that the court should see the patient's claims as assertions of a private right of action under HIPAA and that HIPAA preempted state law causes of actions, with which the court disagreed.[177] The plaintiff appealed the dismissal of his claims, which included "negligence, outrageous conduct, intentional infliction of emotional distress, negligent entrustment, breach of confidentiality, invasion of privacy, and punitive damages."[178] Ultimately, the Supreme Court of Appeals of West Virginia held that HIPAA does not preempt state cause of action claims for unauthorized disclosures of health information and that the lower court improperly dismissed the case.[179] When reviewing the case, the state's Supreme Court referenced *Yath v. Fairview Clinics, N.P., 767 N.W.2s 34 (Minn. Ct. App. 2009)* which involved a medical assistant of the clinic accessing the sensitive medical information of a patient and disclosing that information to the patient's husband.[180] The plaintiff in *Yath* asserted several theories that included the violation of a Minnesota statue in regards to the improper disclosure of her health information.[181] The clinic was awarded summary judgment by the trial court after successfully arguing that HIPAA supersedes provisions of state law that is contradictory.[182] However, the Court of Appeals disagreed with the trial court and reasoned that a state law would be considered "contrary" to HIPAA if it: (1) "would be impossible to comply with both the State and federal requirements," or (2) if the state law makes it impossible to accomplish

[169] *Id.*
[170] *Id.*
[171] *Id.*
[172] *Id.*
[173] *Id.*
[174] *Id.*
[175] *Id.*
[176] *Id.*
[177] *Id.*
[178] *R.K. v. St Mary's Med. Ctr., Inc.*; Supreme Court of Appeals of West Virginia; October 17, 2012, Submitted; November 15, 2012, File; No. 11—9424; page 1
[179] HIPAA Compliance Handbook 2018 page at page
[180] *St. Mary's Med. Ctr., Inc. v. R.K.*, 2013 US S. Ct. Briefs LEXIS 1129; page 17
[181] *Id.*
[182] *Id.*

the full purposes of HIPAA.[183] The Supreme Court in *R.K. v St. Mary's Medical Center* reversed and remanded the order of the Circuit Court of Cabell County.[184]

Similarly, a patient claim against Avery Center for Obstetrics and Gynecology in Connecticut was not dismissed for HIPAA preemption.[185] The plaintiff signed an acknowledgment form on July 15, 2003 stating she reviewed a copy of Avery's Privacy Policy, which detailed how her records would be handled by the facility.[186] The Privacy Policy specifically addressed how the facility would comply with subpoenas and how the facility was not obligated to get the patient's authorization or provide an opportunity to object in response to being served a subpoena for medical records, which was contradictory to the facilities Privacy Manual produced by the plaintiff.[187] The plaintiff notified Avery in October 2004 that she did not want her information disclosed to her ex-boyfriend; this was documented in her medical record file.[188] In March 2005, she moved to Vermont and was no longer a patient of Avery.[189] By July 5, 2005, Avery was served a subpoena ordering them to produce the entirety of the plaintiff's medical record at a court hearing.[190] Avery copied the entirety of the medical records and mailed them to the court without doing any of the following: appearing in court as commanded; notifying plaintiff of the subpoena; obtaining consent from plaintiff to disclose; obtaining "satisfactory assurances" of notice to plaintiff; seeking a qualified protective order; or seeking to limit the production of patient information to what was relevant to the issue.[191] The plaintiff sued Avery to recover damages for breach of contract, negligence, negligent misrepresentation and negligent infliction of emotional distress after her ex-boyfriend used the information from her medical records to harass her.[192] The trial court held that HIPAA preempted the entirety of the plaintiff's claims and dismissed the case, which was appealed.[193] The defendant's cross appeal was denied for lack of subject matter jurisdiction and the plaintiff's appeal was transferred to the Supreme Court of Connecticut.[194] In March 2013, the Supreme Court of Connecticut held that the trial court erred when dismissing the plaintiff's state law negligence claim and that HIPAA did not preempt state tort actions.[195] The court continued stating HIPAA could inform the standard of care applicable for negligence claims.[196] Thus, the court reversed the

[183] *Id.*
[184] *Id.*
[185] HIPAA Compliance Handbook 2018 page
[186] *Byrne v. Avery Ctr for Obstetrics & Gynecology, PC*; SC 18904; Supreme Court of Connecticut; March 1, 2012; 2012 CT S. Ct. Briefs LEXIS 95*; page 2
[187] *Id.*
[188] Byrne c. Avery Ctr for Obstetrics & Gynecology, 2012 CT S Ct Briefs LEXIS 96; March 1, 2012; 2-12 Ct S. Ct Briefs; Page 2
[189] *Id.*
[190] *Id.*
[191] *Id.*
[192] *Id.*
[193] *Id.* At page 4
[194] *Byrne v. Avery Ctr. for Obstetrics & Gynecology, P.C.*, 314 Conn. 433; Supreme Court of Connecticut; March 12, 2013, Argued; November 11, 2014, Officially Released; SC 18904; page 2
[195] Id
[196] *Id.*

judgment.[197] During appeal in May 2017, the court reversed the judgement and the case was remanded for further proceedings in occurrence with the appeal courts opinion.[198]

In a 2012 Indiana case, *Hinchy v. Walgreen Co*., (21 N.E. 3d 99), a jury awarded a customer with $1.44 million dollars in damages after a Walgreens pharmacist accessed a customer's prescription information for personal reasons and further disclosed the information to her husband who was the customer's ex-boyfriend.[199] The customer successfully argued that HIPAA sets the standard of care and the pharmacist breached her common law duty of confidentiality.[200] The court held Walgreens and the pharmacist jointly responsible under the theory of vicarious responsibility.[201] In 2014, Walgreens challenged the vicarious responsibility theory, which was denied by the Court of Appeals.[202] Walgreens also argued that the amount of damages awarded was excessive and was the result of the jury motivated by "passion, prejudice, partiality, or the consideration of improper evidence."[203] Walgreens further argued that the plaintiff did not have a physical injury or condition because of the breach; did not lose wages because of the breach; or offer any testimony by a medical professional or counselor to support her emotional distress claim.[204] The court found that the evidence did support the award and denied Walgreens' appeal.[205] The court further explained, "The jury exercised its discretion to evaluate and weigh the evidence to reach a conclusion regarding damages" after finding the ex-boyfriend responsible for 20% of the damages.[206] In 2015, Walgreens filed a petition for rehearing arguing that the plaintiff did not make a direct claim against Walgreens for negligence and professional malpractice.[207] The court disagreed noting that the state of Indiana only required that the operative facts be plead to place the defendant on notice of the evidence that will be presented at trial, which was included in the plaintiff's complaint.[208]

The theory of vicarious responsibility has not been consistent between states.[209] In a 2015 case, *Sheldon v. Kettering Health Network*, the Court of Appeals in Ohio considered the *Hinchy* case before concluding that an employer is not liable to an employee's independent self-serving actions.[210] This case claimed a hospital administrator illegally accessed the hospitals electronic medical information for an affair.[211]

---

[197] *Id.*
[198] *Byrne v. Avery Ctr. for Obstetrics & Gynecology, P.C.*; Supreme Court of Connecticut; May 1, 2017, Argued; January 16, 2018; Officially released; SC 19873; page 16
[199] *Id.*
[200] *Id.*
[201] *Id.* At page 6-93 and 6-94
[202] *Id.*
[203] *Walgreen Co. v. Hinchy*, 21 N.E.3d 99; Court of Appeals; November 14, 2014; page 11
[204] *Id.*
[205] *Id.*
[206] *Id.*
[207] *Walgreen Co. v. Hinchy*, 25 N.E.3d 748; Court of Appeals; January 15, 2015; page 1
[208] *Id.*
[209] *Id.* At 6-94
[210] *Id.*
[211] *Id.*

Privacy Enforcement through Class Actions

Class actions have become a crucial means for individuals to ensure relief and justice from data breaches.[212] This section will explore how HIPAA violations have been used when filing a class action suit and review some relevant cases.

To establish a class action, a plaintiff must prove standing under Article III of the Constitution to establish jurisdiction before a federal court.[213] There are three elements under Article III that must be proved by the plaintiff when filing a data breach class action.[214] The three elements includes proving an injury-in-fact; proving the connection to the challenged action of the defendant; and it must be readdressable by a favorable decision.[215]

The biggest obstacle for plaintiffs when pursuing a class action litigation has historically been proving the Article III's injury-in-fact requirement.[216] Plaintiffs commonly attempt to support theory of harm by alleging that there is an increased risk of future identity theft or fraudulent charges connected to the data breach.[217] It is clear in the law that the allegations of possible future injury does not satisfy the standing requirement; therefore, this did not work in the early courts that faced this issue.[218] Instead, the early courts held that the alleged increase for future harm was not sufficient to support standing.[219]

However, there have been instances more recently when the court has ruled differently. Plaintiffs in *Fero v. Excellus Health Plan* alleged various injuries after hackers gained access to their personal information through Excellus Health Plan's computer network systems on December 23, 2014.[220] Several potential victims filed individual lawsuits, which were consolidated into a class action on April 15, 2016.[221] In February 2017, the court dismissed certain plaintiff's for no allegations of injury-in-fact and for a lack of evidence on misuse of their information since the occurrence of the data breach.[222] The plaintiffs moved for reconsideration in March 2017, based on the Second Circuit's decision in *Whalen v. Michaels Stores, Inc. 689 F. App'x 89 (2d Cir. 2017)*[223] The *Whalen* case was on appeal from dismissal for lack of standing by the district court when the guidance was provided to the court.[224] The *Whalen* case ultimately concluded that the

---

[212] Article: Standing Together: An Analysis of the Injury Requirement in Data Breach Class Actions; 2016/1017; 52 Gonz. L. Rev. 59*; Daniel Bugni; page 3
[213] *Id.*
[214] Standing in the Midst of a Data Breach Class Action; July 2017; Allison Holt , Joby Ryan, and Joseph W Ryan Jr.
[215] *Id.*
[216] *Id.*
[217] *Id.*
[218] *Id.*
[219] *Id.*
[220] *Fero v. Excellus Health Plan, Inc*.; United States District Court for the Western District of New York; January 19, 2018, Decided; January 19, 2018, Filed; 6:15-CV-06569 EAW; 304 F. Supp. 3d 333; 2018 U.S. Dist. LEXIS 8999**; page 4
[221] *Id.*
[222] *Id.*
[223] *Id.* At page 6
[224] *Id.*

plaintiff lacked an increased risk of identity theft, thus lacked a standing.[225] However, the Court of Appeals in the *Fero* case concluded that it was strongly implied by the Second Circuit during the *Whalen* case that the court would follow the other circuit court's decision that held the risk for future harm through identity theft was sufficient in pleading an injury in fact.[226] The other circuit courts referenced in *Whalen* and reviewed during *Fero* were the Sixth, Seventh, and Ninth Circuit Courts that found standing on the increased risk for future harm through identity theft.[227] The Third and Fourth Circuit courts found that this type of injury was too speculative to warrant standing.[228] Nonetheless, on January 19, 2018, the New York judge in the Second U.S. Supreme Court of Appeals found that there was sufficient allegations of injury from the risk of future identity theft, so the previous decision to dismiss should be reconsidered[229]

In another case out of Massachusetts, plaintiffs were notified by letter in April 2014 of a data breach involving Boston Medical Center Corporations (BMC).[230] The letters explained that unauthorized individuals could have had access to patient's medical records for an unknown amount of time after records were made accessible on a medical record transcription service's website.[231] The class action was commenced on June 10, 2015 with the plaintiffs seeking damages for the exposure of their sensitive information to the public.[232] At the time of the commencement, the plaintiffs were unsure if their information was actually viewed; however, they were fearful that the information on the internet would not ever completely go away.[233] The plaintiff's complaint included "invasion of privacy under G.L. C. 214 Section 1B; Breach of Confidentiality; Breach of Fiduciary Duty; Negligence; Negligent Supervision; Breach of Implied Contract; and Breach of Contract against MDF Transcription, LLC and Fagan."[234] Boston Medical Center moved to dismiss arguing that the plaintiff's complaint did not allege a specific injury without the allegation of their medical records actually being accessed or their information being used by an unauthorized individual.[235] The court referenced the decision under the Supreme Judicial Court in *Pugsley v. Police Department of Boston, 472 Mass 367, 34 N.E. 3d 1235 (2015)* , citing that the court affirmed the motion to dismiss for a lack of standing upon a summary judgement and not a motion to dismiss.[236] The court in *Pugsley* further acknowledged that a risk of injury that is "real and immediate" could be enough to establish a standing.[237] The plaintiffs in *Walker v. BMC* allege a real risk of harm; therefore, a motion for summary judgement should decide the standing question and plaintiffs are entitled to discovery to determine if their information was accessed.[238] For these

[225] *Id.*
[226] *Id.* At page 7
[227] *Id.* At page 6
[228] *Id.*
[229] Plaintiffs' Claims Against Insurer Reinstated in Data Breach Class Action; Mealey's Litigation Report: Class Actions15 (2018); Volume 17; Issue #23; Rochester, NY
[230] *Walker v. Boston Med. Ctr Corp*.; Superior Court of Massachusetts, At Suffolk; November 19, 2015, Decided; Civil Action No. 2015-1733-BLS 1; Page 2
[231] *Id.*
[232] *Id.*
[233] *Id.*
[234] *Id.*
[235] *Id.* At page 3
[236] *Id.*
[237] *Id.*
[238] *Id.* At page 2

reasons, on November 20, 2015, the court denied the BMC's motion to dismiss due to the lack of standing.[239]

On February 25, 2014, the Henry County Sheriff's Office in Alabama uncovered a scheme involving a Flower's Hospital phlebotomist who had fifty-four patient records in his possession, which he took from his place of employment at the hospital.[240] The phlebotomist obtained the information from an unsecured file cabinet and used the information to file 124 fraudulent tax returns.[241] After being notified of the scheme, Flowers Hospital conducted an audit that uncovered several missing folders containing patient records and sent letters to 1,208 patients detailing the events.[242] The hospital claimed they sent letters to all patients whose records could not be located in an effort to be overly cautious and to comply with HIPAA, even though it was unknown if all patients were actually affected by the data breach.[243] The plaintiffs filed a class-action against the hospital alleging violations under the "Fair Credit Reporting Act (FCRA), 15 U.S.C. Section 1681 et seq, negligence, and invasion of privacy,"[244] On March 17, 2017, the Magistrate Judge found standing for a class action while denying the claim on invasion of privacy and denying the hospitals motion to dismiss.[245] In October 2017, defendant's (Triad of Alabama) motion to decertify the class action was denied while the motion to seek to redefine the class was granted.[246]

In March 2015, Premera Blue Cross notified consumers that there was a data breach exposing the sensitive information of millions insured after their computer system was hacked.[247] The hackers began their attack on Premera's servers on May 5, 2014 by use of a phishing email claiming to be one of their IT employees.[248] The data breach went unnoticed by Premera for almost one year and did not notify insurers until several months after discovery.[249] Prior to notifying the insurers, Premera contracted with Mandiant, a Cyber Security Firm, to assess Premera's network security.[250] On January 30, 2015, the firm discovered malware on the network that affected two servers since May 2014.[251] The FBI was notified shortly after in February 2015 but the complete remediation of its network was not performed until the weekend of March 6-8, 2015.[252] This resulted in a number of class actions filed against Premera Blue Cross that was ultimately consolidated into one by the U.S. Supreme Court in the District of Oregon.[253] The plaintiffs alleged several violations

---

[239] *Id.*
[240] *Smith v. Triad of Ala., LLC*; United States District Court for the Middle District of Alabama, Southern Division; March 17, 2017, Decided; March 17, 2017, Filed; Case No. 1: 14-CV-324- WKW; page 2-3
[241] *Id.* at page 3
[242] *Id.*
[243] *Id.*
[244] *Id.*
[245] *Id.*
[246] TRIAD OF ALABAMA: Bid to Reconsider Class Cert Partly Denied; Class Action Reporter; October 24, 2017
[247] Plaintiffs Seek Sanctions for Premera's Spoliation In Data Breach Suit; 4-5 Mealey's Data Privacy Report 7 (2018)
[248] *In re Premera Blue Cross Customer Data Sec. Breach Litig.*; United States District Court for the District of Oregon; August 1, 2016, Decided; August 1, 2016 Filed; Case No. 3: 15-md-2633-SI; page 3
[249] *Id.* at page 1
[250] *Id.* at page 3
[251] *Id.*
[252] *Id.*
[253] Plaintiffs Seek Sanctions for Premera's Spoliation In Data Breach Suit; 4-5 Mealey's Data Privacy Report 7 (2018)

of different laws, which included: "the Washington Consumer Protection Act (CPA), Rev. Code Wash. § 19.86.010 et seq.; the Washington Data Breach Disclosure Law (DBDL), Rev. Code Wash. § 19.255.010(2); the California Confidentiality of Medical Information Act (CMIA), Calif. Civ. Code § 56 et seq.; and various state consumer protection and data breach notification laws, as well as negligence, breach of express and implied contract, restitution or unjust enrichment, breach of fiduciary duty and misrepresentation by omission."[254] On August 1, 2016, the court granted Premera's motion to dismiss the plaintiff's allegations of fraud by affirmative misrepresentation, active concealment, or omission; allegation of breach of express contract and breach of implied contract; allegation of breach of fiduciary duty.[255] However, the court denied Premera's motion to dismiss the plaintiff's allegations of unjust enrichment; violation of the California Confidentiality of Medical Information Act; causation; and damages.[256]

Similar to the Premera breach, Anthem Inc, the second largest insurer in the country, was hit with a cyberattack associated with a phishing scheme in 2015, which exposed the private information of approximately 79 million people.[257] The OCR investigation identified several deficiencies that included failure to conduct full a risk analysis; failure to implement pertinent policy and procedures; failure to implement the right access controls to prevent hackers; and failure to detect or respond to security incidents.[258] The OCR settled with Anthem at a record $16 million.[259] Anthem was also involved in a class action suit related to the cyberattack where they settled with consumers for $115 million in June 2017.[260] This class action settlement was a record for a private civil claim involving a data breach and included two years of credit monitoring; out-of-pocket expenses incurred by consumers; and cash compensation to consumers who already paid for their credit monitoring.[261] Anthem admitted to no liability and stated that they were unaware of any instances of fraud or identity theft to the affected consumers due to the attack.[262]

CONCLUSION

To conclude, there was much expansion on the enforcement abilities under HIPAA with the enactment of HITECH, including providing state attorneys general with the authority to bring action on behalf of their state's residents, which has been effective.[263] HITECH also increased the amounts of imposed civil money penalties to covered entities, while also proposing sharing a percentage of the penalties with the affected individual.[264] Although the sharing of CMPs has yet to pass, it could provide additional incentives to consumers to report potential violations and to covered entities to comply with the regulations to protect patient information.

---

[254] *Id.*
[255] *Id.* at page 16
[256] *Id.*
[257] Anthem to Settle Health Care Data Breach for Record $16 million; October 15, 2018; Law 360; Christopher Crosby
[258] *Id.*
[259] *Id.*
[260] *Id.*
[261] *Id.*
[262] *Id.*
[263] See Footnotes 89-105
[264] See Footnotes 41

There has also been consistency in the amounts of self-reported breaches by covered entities. To date, there has been 191,052 self-reported breaches affecting less than 500 individuals and 2,513 self-reported breaches affecting more than 500 individuals to the OCR.[265] Covered entities are required to notify the media of breaches affecting 500 or more individuals while the HHS Secretary is required to make public the breach by posting on the internet.[266] Regardless of the potential negative impacts on reputation for reporting these breaches, entities remain consistent, which demonstrates that there are covered entities that take their responsibilities to comply with the regulations seriously without a private right of action to incentivize the behavior.

Furthermore, similar to HIPAA, there are other federal privacy regulations under different government enforcers, such as the FTC, that do not provide a private right of action. For instance, the FTC enforces privacy related to unfair and deceptive practices, Children's Online Privacy Protection Act, and the Gramm-Leach Bliley act, which do not provide a private right of action.[267] In addition, similar to how states implemented their own versions of the FTCs unfair and deceptive trade practices, all states now have enacted their own data breach notification laws similar the HIPAA's Breach Notification Rule.[268]

Lastly, there are other ways consumers can redress misuse of their private medical information. For instance, as explored in this paper, the courts held in *Acosta* and *Hinchy* that HIPAA can be used as evidence of the standard of care for negligence claims, with *Hinchy* receiving a $1.44 million judgement.[269] Then in *R.K. v. St. Mary's* and *Avery*, the courts held that HIPAA did not preempt state tort claims.[270] There have also been advances in the data breach class actions suits where the courts have consistently agreed that a risk of future harm could be enough to establish Article III standing, with the *Anthem* case resulting in a $115 million settlement regardless of any known misuse of the compromised data.[271]

Accordingly, due to strengthening of the HIPAA privacy and security regulations with the implementation of the provisions under HITECH and the ability for consumers to remedy HIPAA violations in other methods, a private right of action under HIPAA is not necessary.

[265] See Footnote 119
[266] See Footnote 266
[267] See Footnote 91 and 99
[268] See Footnotes 120-142
[269] See Footnotes 199-208
[270] See Footnotes 175-198
[271] See Footnotes 257-262