Byrne: Closing the Gap Between HIPAA and Patient Privacy

AUSTIN RUTHERFORD*

TABLE OF CONTENTS

* © 2016 Austin Rutherford. J.D. 2015, University of San Diego School of Law. Author would like to thank Professor Dov Fox, as well as the *San Diego Law Review* Editorial Board, especially Misty Ann Giles, Editor-in-Chief.

I. INTRODUCTION

The magnitude of information sharing in the digital age requires a legal structure that protects an individual's right to privacy. Privacy violations, willful or negligent, can cause irreversible emotional and financial harm.[1] Recently, Anthem, the second largest health insurer in the United States, was hacked.[2] Hackers inappropriately accessed over eighty million people's personal information, including social security numbers.[3] Anthem could have encrypted the information, as suggested by the Health Insurance Portability and Accountability Act (HIPAA), but did not.[4] Social security numbers are particularly precious because they are not reissued. Hackers can open credit cards, take out loans, and fraudulently obtain tax returns. As a result, these people will suffer torment, anxiety, and financial and emotional stress wondering if and when this information will be used against them. Anthem's failure to fully comply with HIPAA caused irreversible harm to these individuals.

Initially, HIPAA received praise for expanding and standardizing the sharing of health information.[5] However, Congress did not prioritize information privacy when enacting HIPAA.[6] The public expressed concern

---

1. Darius Tahir & Bob Herman, *Data Breaches Can Lead to Major Medical Identity Theft Issues*, MODERN HEALTHCARE (Mar. 4, 2014), http://www.modernhealthcare.com/article/20150304/NEWS/150309960 [https://perma.cc/3PXT-VZT8] ("You have this lifelong corruption of your [medical] record.").

2. Danny Yadron & Melinda Beck, *Health Insurer Anthem Didn't Encrypt Data in Theft*, WALL ST. J. (Feb. 5, 2015), http://www.wsj.com/articles/investigators-eye-china-in-anthem-hack-1423167560 [https://perma.cc/9NYX-EYP4].

3. *Id.*

4. *Id.* Encryption is an addressable safeguard under HIPAA. *See* 45 C.F.R. § Addressable safeguards promote flexibility for entities subject to HIPAA. *See What is the Difference Between Addressable and Required Implementation Specifications in the Security Rule*, U.S. DEP'T HEALTH & HUM. SERVS., http://www.hhs.gov/ocr/privacy/hipaa/faq/securityrule/2020.html [https://perma.cc/8QYJ-QEF8] (last visited Feb. 8, 2016). Anthem would be required to encrypt information if, after a risk assessment, it determined that encryption is a "reasonable and appropriate safeguard" to manage the privacy of PHI. *See Is the Use of Encryption Mandatory in the Security Rule*, U.S. DEP'T HEALTH & HUM. SERVS., http://www.hhs.gov/hipaa/for-professionals/faq/2001/is-the-use-of-encryption-mandatory-in-the-security-rule/index.html [https://perma.cc/4CM3-2P25] (last visited Feb. 8, 2016).

5. Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (codified in scattered sections of 42 U.S.C.).

6. H.R. REP. NO. 104-496, at 70 (1996), *reprinted in* 1996 U.S.C.C.A.N. 1865, 1869.

> [HIPAA was meant] to improve portability and continuity of health insurance coverage in the group and individual markets, to combat waste, fraud, and abuse in health insurance and health care delivery, to promote the use of medical savings accounts, to improve access to long-term care services and coverage, [and] to simplify the administration of health insurance . . . .

about this new element to healthcare, specifically worrying about privacy.[7] Individuals who share sensitive health information deserve protection and privacy of that information. The government responded by enacting the HIPAA Privacy Rule, which provides individuals access to their health information and prohibits inappropriate use and disclosure of that information.[8]

Notably absent in HIPAA is a private right of action.[9] Thus, a victim whose information is improperly used or disclosed, according to HIPAA, has no recourse—until recently. In 2014, the Connecticut Supreme Court unequivocally recognized that HIPAA creates a standard of care in *Byrne v. Avery Center for Obstetrics & Gynecology, P.C.*.[10] This, in turn, makes a company's breach of HIPAA requirements a breach of a duty owed, enabling individuals harmed by the breach to sue under a negligence theory.[11]

Id. at 1; *see also* Byrne v. Avery Ctr. for Obstetrics & Gynecology, P.C., 102 A.3d 32, 43 (Conn. 2014) (citing S.C. Med. Ass'n v. Thompson, 327 F.3d 346, 349 (4th Cir. 2003) (indicating that HHS took five years to promulgate the Privacy Rule)).

7. *See* Health Insurance Portability and Accountability Act of 1996, 42 U.S.C § 1320d-2 (1996); Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. 82,462, 82,463 (Dec. 28, 2000) (to be codified at 45 C.F.R. pt. 160, 164).

8. 45 C.F.R. § 164.500–164.534 (2014). *See also* U.S. DEP'T HEALTH & HUMAN SERVS., SUMMARY OF THE HIPAA PRIVACY RULE (2003), http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/privacysummary.pdf [https://perma.cc/QZN3-DGT5].

9. Spencer v. Roche, 755 F. Supp. 2d 250, 271 (D. Mass 2010) (citing Acara v. Banks, 470 F.3d 569, 571 (5th Cir. 2006)); Univ. of Colo. Hosp. Auth. v. Denver Publ'g Co., 340 F. Supp. 2d 1142, 1145 (D. Colo. 2004) ("[L]egal commentators appear to unanimously assume that there is no private right of action under HIPAA, including to enforce the 'privacy rule' of § 1320d-6."); Nw. Mem'l Hosp. v. Vill. of S. Chi. Heights Health & Welfare Fund, No. 03-C-4006, 2004 WL 1687057, at *4 (N.D. Ill. July 27, 2004); O'Donnell v. Blue Cross Blue Shield of Wyo., 173 F. Supp. 2d 1176, 1179–80 (D. Wyo. 2001); Brock v. Provident Am. Ins. Co., 144 F. Supp. 2d 652, 657 (N.D. Tex. 2001); 45 C.F.R. § 160.306, 160.308 (2014); Deborah F. Buckman, Annotation, *Validity, Construction, and Application of Health Insurance Portability and Accountability Act of 1996 (HIPAA) and Regulations Promulgated Thereunder*, 194 A.L.R. Fed. 133, § 18 (2004).

10. *See Byrne*, 102 A.3d at 42. Other courts recognize this standard of care argument. *See e.g.*, Acosta v. Byrum, 638 S.E.2d 246, 251 (N.C. Ct. App. 2006); Sorensen v. Barbuto, 2006 UT App 340, ¶ 11, 143 P.3d 295, 299, *aff'd*, 2008 UT 8, ¶¶ 6, 29, 177 P.3d 614, 616, 621 (affirming issues on appeal other than the HIPAA standard of care issue). Additionally, the West Virginia Supreme Court of Appeals made note of this possibility, but only held as to the preemption issue. *See* R.K. v. St. Mary's Med. Ctr., Inc., 735 S.E.2d 715, 723–24 (W. Va. 2012).

11. *Byrne*, 102 A.3d at 42.

HIPAA's lack of an individualized remedy harmed individuals and left the law a toothless monster, but *Byrne* begins to fill the longstanding gap by offering greater protection for individuals and their sensitive information.[12] *Byrne* will also incentivize better compliance with HIPAA by instilling in companies a fear of sizeable tort suit damage awards.[13]

Part II of this Note introduces HIPAA and its ability to protect sensitive health information. Part III discusses the facts, holding, and reasoning of *Byrne*, in which a state supreme court, for the first time, recognized HIPAA requirements as a duty owed in negligence claims. Part IV examines the available remedies for injured individuals before and after *Byrne*. Part V analyzes how the *Byrne* decision, in combination with HIPAA's expansion under the Health Information Technology for Economic and Clinical Health Act (HITECH), affects companies subject to HIPAA. Part VI demonstrates that *Byrne* and other similar state court decisions are trending toward recognizing HIPAA as a standard of care nationwide. Part VII concludes.

II. THE BASICS OF HIPAA

HIPAA is the primary American law regulating privacy and security of health information.[14] In 2009, Congress amended and strengthened HIPAA by passing HITECH.[15] HITECH expanded HIPAA's regulatory power, forcing many new businesses to comply with HIPAA's requirements.[16]

HIPAA's Privacy Rule governs the use and disclosure of protected health information (PHI) by covered entities and business associates.[17] PHI is information that identifies, or provides a reasonable basis to identify an individual, and relates to (i) "an individual's past, present, or future physical or mental health condition"; (ii) "the provision of healthcare to

12. *See* Ian Traynor, *New EU Rules To Curb Transfer of Data to US After Edward Snowden Revelations*, THE GUARDIAN (Oct. 17, 2013), http://www.theguardian.com/world/2013/oct/17/eu-rules-data-us-edward-snowden [https://perma.cc/7F2A-XPUJ] (showing that the EU equivalent of HIPAA, the Data Protection Directive, has drastically stiffer penalties for noncompliance).

13. *See infra* Part VI.B.

14. Health Insurance Accountability and Portability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (codified in scattered sections of 42 U.S.C.). HIPAA is comprised of the Privacy, Security, Enforcement and Breach Notification Rules. *Id.*

15. Health Information Technology for Economic and Clinical Health Act, Pub. L. No. 111-5, 123 Stat. 115 (codified as amended in scattered sections of 26 U.S.C. and 42 U.S.C.). Although HITECH was passed in 2009, the Omnibus Rule did not implement it until 2013. *See* Press Release, Dep't Health & Human Servs., New Rule Protects Patient Privacy, Secures Health Information (Jan. 17, 2013), http://www.hhs.gov/news/press/2013pres/01/20130117b.html [https://perma.cc/FR33-FHX2].

16. *See infra* notes 20–24 and accompanying text.

17. 45 C.F.R. § 160.103 (2014); *infra* notes 20–24 and accompanying text.

an individual"; or (iii) "the past, present, or future payment for the provision of healthcare to an individual".[18] HIPAA specifies eighteen individual identifiers, including social security, medical record, and phone numbers.[19]

HIPAA and HITECH regulate two different entities: covered entities and business associates.[20] A covered entity is a health plan, health clearinghouse, or healthcare provider that transmits PHI electronically.[21] A business associate is a person or entity, except workforce members of the covered entity, "who performs functions or activities on behalf of, or provides certain services to, a covered entity that involve access by the business associate to protected health information."[22] HITECH expanded HIPAA's definition of business associate to include any subcontractor, *ad infinitum*, "that creates, receives, maintains, or transmits protected health information on behalf of the business associate."[23] This amendment vastly increased the number of entities subject to HIPAA.[24]

---

18. *See* 45 C.F.R. § 160.103. Note that there are some minor exceptions to the definition of PHI that do not pertain to this Note. For example, the Privacy Rule excludes PHI all employment records held by a covered entity in its capacity as employer. *See* U.S. DEP'T HEALTH & HUMAN SERVS., *supra* note 8, at 4.

19. *See* U.S. DEP'T HEALTH & HUMAN SERVS., *supra* note 8, at 4 & 19 n.15. The eighteen identifiers are: names, geographic subdivisions smaller than a state, all elements of dates related to an individual, telephone numbers, fax numbers, email addresses, social security numbers, medical record numbers, health plan beneficiary numbers, account numbers, certificate/license numbers, vehicle identifiers and serial numbers, device identifiers and serial numbers, Web Universal Resource Locators, Internet Protocol addresses, biometric identifiers, full-face photographs, and any other unique identifying number. OFFICE FOR CIVIL RIGHTS, U.S. DEP'T HEALTH & HUMAN SERVS., GUIDANCE REGARDING METHODS FOR DE-IDENTIFICATION OF PROTECTED HEALTH INFORMATION IN ACCORDANCE WITH THE HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPAA) PRIVACY RULE 8 (2013), http://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/

20. *See* U.S. DEP'T HEALTH & HUMAN SERVS., *supra* note 8, at 3.

21. *See* 45 C.F.R. § 160.103.

22. UNIV. OF TEX. SYS. ADMIN., HIPAA PRIVACY MANUAL (2013), https://www.utsystem.edu/sites/utsfiles/documents/employee-benefits/section-61-contracts-business-associates-involving-office-employment-benefits-phi/hipaapolicy61.pdf [https://perma.cc/5G5W-E7L6]; *see also* 45 C.F.R. § 160.103 (defining "business associate").

23. *See* 45 C.F.R. § 160.103.

24. *See HIPAA Omnibus Rule Significantly Expands Privacy, Security, Enforcement Standards, Breach Notification Requirements, and Penalties for Non-Compliance*, COOLEY (Feb. 12, 2013), http://www.cooley.com/HIPAA-omnibus-rule [https://perma.cc/AGA2-ZNMM]. For instance, a company that stores data for a hospital is now a business associate. Even though the company never accesses the data, it is subject to HIPAA because it receives and stores data on behalf of a covered entity. *See id.*

Broadly speaking, a covered entity or business associate may only use or disclose information as required or permitted by the Privacy Rule, or as authorized by the individual.[25] The Privacy Rule requires covered entities and business associates to safeguard PHI from impermissible uses and disclosures.[26] To safeguard PHI, a covered entity or business associate must implement reasonable administrative, technical, and physical safeguards.[27] Examples of these safeguards include, respectively, training employees, encrypting information, and limiting access to buildings where PHI is stored.[28] HIPAA and the Privacy Rule create a floor, not a ceiling, from which states can enact more stringent laws to protect patient privacy.[29]

III. THE DECISION: *BYRNE V. AVERY CENTER FOR OBSTETRICS & GYNECOLOGY, P.C.*

A. The Facts

In *Byrne*, the Connecticut Supreme Court examined whether a plaintiff could sue using HIPAA as a standard of care after her doctor negligently released her confidential medical records in violation of HIPAA.[30] Emily Byrne and Andro Mendoza were romantically involved from May to

25. 45 C.F.R. § 164.502(a) (2014). For instance, a covered entity is required to disclose HIPAA. *Id*. § 164.502(a)(2). On the other hand, a covered entity is permitted to disclose PHI to provide health care services. *Id*. § 164.506(c).

26. 45 C.F.R. § 164.530(c) (2014).

27. *Id.* These safeguards are more fully described in the HIPAA Security Rule. 45 C.F.R. §§ 164.308, 164.310 & 164.312 (2014).

28. *See* Patrick Ouellette, *A Look at HIPAA Administrative Safeguard Requirements*, HEALTHIT SECURITY (Nov. 26, 2012) (citing 45 C.F.R. § 164.308), http://healthitsecurity.com/2012/11/26/a-look-at-hipaa-administrative-safeguard-requirements/ [https://perma.cc/N6YC-ENEH] (addressing workforce training); Patrick Ouellette, *A Look at HIPAA Technical Safeguard Requirements*, HEALTHIT SECURITY (Nov. 20, 2012) (citing 45 C.F.R. § 164.312), http://healthitsecurity.com/2012/11/20/a-look-at-hipaa-technical-safeguard-requirements/ [https://perma.cc/J2F4-F9TE] (addressing encryption); Patrick Ouellette, *A Look at HIPAA Physical Safeguard Requirements*, HEALTHIT SECURITY (Nov. 8, 2012) (citing 45 C.F.R. § 164.310 (2014)), http://healthitsecurity.com/2012/11/08/looking-back-at-hipaa-physical-safeguard-requirements/ [https://perma.cc/NP9J-N94S] (addressing building access).

29. *See* 45 C.F.R. § 160.203(b) (2014). For instance, California recently enacted the California Online Privacy Protection Act, which requires website operators to specifically explain their policies and procedures regarding "do not track" signals. CAL. BUS. & PROF. CODE § 22575(b)(5) (West Supp. 2015).

30. Byrne v. Avery Ctr. for Obstetrics & Gynecology, P.C., 102 A.3d 32, 35–36, 41 (Conn. 2014).

September of 2004, and during that time Mendoza impregnated Byrne.[31] Byrne sought treatment from the defendant, Avery Center for Obstetrics and Gynecology, in relation to the pregnancy.[32] After Byrne and Mendoza's relationship ended, but before Ms. Byrne gave birth, she fled Connecticut for Vermont.[33] Mendoza, in response, filed paternity suits in both states.[34]

Byrne instructed Avery Center not to release her medical information to Mendoza.[35] In the course of the paternity suits, Mendoza subpoenaed Byrne's medical records.[36] Avery Center staff "did not alert [Byrne of] the subpoena, file a motion to quash it or appear in court."[37] Instead, Avery Center staff mailed a copy of Byrne's medical file to the court.[38] Subsequently, Mendoza used that information "for a campaign of harm, ridicule, embarrassment and extortion."[39]

Byrne sued Avery Center, alleging that it acted negligently by failing to use proper and reasonable care to protect her medical information, in violation of HIPAA.[40] Byrne further alleged that Avery Center engaged in conduct sufficient to establish negligent infliction of emotional distress.[41]

---

31. *Id.* at 36 & n.4; Brief of Defendant-Appellee at 2, *Byrne*, 102 A.3d 32 (No. SC18904).

32. Brief of Defendant-Appellee, *supra* note 31, at 2–3.

33. *Id.* at 3.

34. *Byrne*, 102 A.3d at 36.

35. *Id.* at 36. She has a right to request that Avery Center restrict its use and disclosure of her protected health information under HIPAA. *See* 45 C.F.R. § 164.522(a) (2014). However, HIPAA does not require the covered entity to comply with that request. *Id.*

36. *Byrne*, 102 A.3d at 36.

37. *Id.*

38. *Id.*

39. Marianne Kolbasuk McGee, *Court Allows HIPAA Negligence Claim*, GOV INFO SECURITY (Nov. 7, 2014), http://www.govinfosecurity.com/court-allows-hipaa-negligence-claim-a-7535 [https://perma.cc/DY72-HUNB]. Mendoza harassed Byrne by filing a series of civil actions against not only Byrne, but also her attorney, her father, and her father's employer. *See Byrne*, 102 A.3d at 36 n.5. Additionally, Mendoza threatened Byrne with criminal charges. *Id.*

40. *Byrne*, 102 A.3d at 36–37.

41. *Id.* at 37.

The trial court dismissed these claims, explaining that HIPAA preempted the state law tort claims.[42] Byrne immediately appealed.[43]

B. The Court's Decision

The Connecticut Supreme Court considered two issues. The court first examined whether HIPAA preempted Byrne's state law claims of negligence against the doctor who released her information in violation of state law and HIPAA.[44] It then decided whether HIPAA may establish a standard of care in a negligence claim.[45]

To resolve the preemption issue, the court analyzed HIPAA's framework, which states that HIPAA "shall supersede any contrary provision of State law."[46] A state law is contrary if (1) "a covered entity or business associate would find it impossible to comply with both the State and Federal requirements" or (2) the state law stands as an "obstacle to the accomplishment and execution of the full purposes" of HIPAA.[47] However, more stringent state laws relating to the privacy of individually identifiable information are exempt from preemption.[48] In *Byrne* the court held that the Connecticut state law was more stringent because it provides greater privacy protection for the individual.[49]

The court also considered regulatory history and legislative intent when deciding the preemption issue.[50] During the Privacy Rule implementation phase, the Department of Health and Human Services (HHS) stated, "the fact that a state law allows an individual to file [a civil action] to protect privacy does not conflict with the HIPAA penalty provisions."[51] The

---

42. *Id*. at 37–38 (quoting the lower court, "plaintiff has labeled her claims as negligence claims, but this does not change their essential nature. They are HIPAA claims."). Additionally, the trial court denied the defendant's motion for summary judgment on counts (1) and (3), finding there were genuine issues of material fact. *Id.* at 41.

43. *Id.* at 41; *see also id.* at 35 n.3 (discussing the special permission granted for Ms. Byrne to pursue her appeal).

44. *Id.* at 35. CONN. GEN. STAT. § 52-146(o) (2015) prohibits a doctor from releasing health information without patient consent. Additionally, HIPAA requires that the health care provider alert the patient of the subpoena or seek a protective order. 45 C.F.R. § 164.512(e)(1)(ii) (2014).

45. *Byrne*, 102 A.3d at 42.

46. 42 U.S.C. 1320d-7(a)(1) (2012).

47. 45 C.F.R. § 160.202 (2014).

48. 45 C.F.R. § 160.203(b) (2014). A state law is more stringent if it narrows the requirements regarding use or disclosure of individually identifiable health information, or otherwise increases individuals' privacy protections. 45 C.F.R. § 160.202.

49. *See Byrne*, 102 A.3d at 36, 49.

50. *Id.* at 42–43 (quoting Hackett v. J.L.G. Props., LLC, 940 A.2d 769, 773 (Conn. 2008)).

51. *Byrne*, 102 A.3d at 46. HHS is the primary governmental agency for protecting the health of Americans. *About HHS*, U.S. DEP'T HEALTH & HUM. SERVS., http://www.

court interpreted this statement as strong evidence that the Privacy Rule allows state law claims for violation of HIPAA.[52]

The Connecticut Supreme Court held that HIPAA did not preempt state law claims for two reasons. First, Connecticut laws expanded patients' privacy rights and thus were not preempted. Second, legislative intent indicated HIPAA was not intended to preempt the Connecticut law because the state law improved patient privacy.[53] Because the court decided HIPAA did not preempt Byrne's state law claims, it could address the second issue.

The court next addressed whether HIPAA establishes a standard of care in a negligence claim.[54] The Connecticut Supreme Court answered in the affirmative.[55] The court reasoned that HIPAA could inform the standard of care "to the extent it has become the common practice for Connecticut health care providers to follow . . . HIPAA."[56] HIPAA compliance is mandatory for a wide array of businesses inside and outside the health care industry, so it is very likely customary practice for health care providers and a baseline for standard of care.[57] The court's ruling in *Byrne* increased patient privacy rights by empowering individuals to bring suits, while simultaneously encouraging an increasing number of entities to comply with HIPAA in order to avoid civil liability.

---

hhs.gov/about/ [https://perma.cc/EP3N-886T] (last visited Feb. 8, 2016). HHS promulgated rules to implement both HIPAA and HITECH. *See, e.g.*, Modifications to HIPAA Under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act, 78 Fed. Reg. 5566 (Jan. 25, 2013) (to be codified at 45 C.F.R. pt. 160, 164). And, through its Office for Civil Rights, HHS enforces HIPAA. *Who Enforces the Health Information Privacy and Security Standards established Under the Health Insurance Portability and Accountability Act (HIPAA)?*, U.S. DEP'T HEALTH & HUM. SERVS., http://www.hhs.gov/hipaa/for-professionals/faq/2019/who-enforces-hippa/index.html [https://perma.cc/YGM4-EA2A] (last visited Feb. 8, 2016).

52. *Byrne*, 102 A.3d at 46 (citing Exelon Generation Co. v. Local 15, Int'l Bhd. of Elec. Workers, 676 F.3d 566, 570 (7th Cir. 2012)) (recognizing that courts should defer to agency interpretations of its own rule).

53. *Id.* at 36, 46–47.

54. In order to prevail on a negligence claim, a plaintiff must prove: (1) she was owed a duty of care, (2) the defendant breached that duty owed, (3) the breach caused harm, and (4) the damage caused by that breach. *See* 57A AM. JUR. 2D *Negligence* § 5 (2004).

55. *Byrne*, 102 A.3d at 45. However, the court did not decide the merits of the case and remanded for further proceedings. *Id.* at 42, 47.

56. *Id.* at 49.

57. *See supra* Part II.

IV. AVAILABLE REMEDIES FOR INDIVIDUALS BEFORE AND AFTER *BYRNE*

With *Byrne* decided, a new era of patient privacy begins. Contrasting an individual's available remedies for invasion of privacy pre- and post-*Byrne* supports this Note's main assertion—recognizing HIPAA as a standard of care is an important shift that benefits patient privacy in the digital age.

*A. Remedy Available pre-*Byrne

Prior to the Connecticut Supreme Court's decision in *Byrne*, plaintiffs, such as Emily Byrne, could not have successfully sued a HIPAA-violating entity for negligence.[58] Her sole remedy would have been filing a complaint with HHS.[59] After receiving a complaint, HHS may initiate an investigation.[60] If HHS discovers a HIPAA violation, HHS can assess civil monetary penalties.[61] However, the maximum amount HHS can assess against a violator is $50,000 per incident and $1.5 million annually.[62]

Although the civil monetary penalties are useful, the harmed individual does not receive any portion of the penalty. HITECH required rulemaking bodies to develop a methodology to provide a percentage of collected fines to the harmed individual.[63] However, the rulemakers repeatedly

58. Prior to *Byrne*, litigants tried and failed to establish HIPAA as a standard of care. *See, e.g.*, Fisher v. Yale Univ., No. X10NNHCV044003207S, 2006 WL 1075035 (Conn. Super. Ct. Apr. 3, 2006). *Fisher* involved a woman whose information was improperly accessed by an employee and used to harass her. *Id.* at *1. The court granted the defendant's motion to dismiss her claim that HIPAA informs a standard of care, thus leaving her damaged but not compensated. *Id.* at *5.

59. *See* 45 C.F.R § 160.306 (2014).

60. *Id.* § 160.306(c).

61. 42 U.S.C. § 1320d-5 (2012). The U.S. Department of Justice can criminally prosecute covered entities and individuals for "knowingly" violating HIPAA. 42 U.S.C. § 1320d-6 (2012). However, the criminal sanctions are beyond the scope of this Note.

62. 42 U.S.C. § 1320d-5. These amounts reflect the increase penalties as amended by HITECH. *See* Patrick Ouellette, *HIPAA Omnibus and HITECH Civil Penalty Changes*, HEALTHIT SECURITY (Jan. 23, 2013), http://healthitsecurity.com/2013/01/23/ hipaa-omnibus-and-hitech-civil-penalty-changes/ [https://perma.cc/Z6HL-XCKF]. Prior to HITECH, HIPAA violators were only fined $100 per incidents and $25,000 annually. *Id.* Although these are substantial changes, the annual cap fails to adequately deter violating entities and compensate harmed individuals on a massive scale such as the eighty million people affected by the Anthem breach. *See* Yadron & Beck, *supra* note 2.

63. 42 U.S.C. § 17939 (2012).

neglected this obligation.[64] As a result, plaintiffs continue to file suits like *Byrne* to obtain deserved compensation for their losses.[65]

*B. Remedy Available post-*Byrne

After *Byrne*, plaintiffs in Connecticut can sue a HIPAA violator directly.[66] Unlike the formal complaint and investigation process with HHS, where money from penalties goes to the government, a successful lawsuit using HIPAA as a standard of care awards monetary damages to the injured individual.[67] Additionally, damage awards are not limited to the $1.5 million cap under HIPAA and can quickly exceed that cap. Although *Byrne* affects entities doing business in Connecticut, these entities often do business in numerous states and establish compliance with the strictest state for a baseline in all states.[68] Therefore, *Byrne* empowers violated individuals to seek compensation and deters companies from noncompliance by subjecting them to a material risk of litigation.

---

64. The HITECH Act included a provision that provided for a portion of a collected fine to return to the individual. *See* 42 U.S.C. § 17939(c). As the applicable agencies promulgated rules for the Act, they repeatedly failed to develop a methodology to compensate the injured individual. *See* Modifications to the HIPAA Privacy, Security, and Enforcement Rules, 75 Fed. Reg. 40,868, 40,870 (July 14, 2010) (to be codified at 45 C.F.R. pt. 160, 164) ("These provisions [regarding individual compensation] will be the subject of future rulemakings."); Modifications to HIPAA Under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act, 78 Fed. Reg. 5566, 5568 (Jan 25, 2013) (to be codified at 45 C.F.R. pt. 160, 164) ("[T]he penalty distribution methodology requirement . . . will be the subject of a future rulemaking.").

65. *See, e.g.*, Sheldon v. Kettering Health Network, 2015-Ohio-3268, 40 N.E.3d 661 (2d Dist.).

66. *See* Byrne v. Avery Ctr. for Obstetrics & Gynecology, P.C., 102 A.3d 32, 42 (Conn. 2014).

67. *See How OCR Enforces the HIPAA Privacy & Security Rules*, U.S. DEP'T OF HEALTH & HUM. SERVS., http://www.hhs.gov/ocr/privacy/hipaa/enforcement/process/howocrenforces.html [https://perma.cc/FC9R-43QP] (last visited Feb. 8, 2016).

68. Companies generally do not segregate data for each state. The more common approach is to comply with the strictest standard such that the single database is compliant with all states. In this case, companies should recognize *Byrne* proposes a large risk for the business and protect all of their data to that standard, thus benefitting all data under the company's control.

V. IMPLICATIONS OF BYRNE FOR COVERED ENTITIES AND BUSINESS ASSOCIATES

HITECH expanded the number of companies subject to the HIPAA Privacy Rule to include all subcontractors of business associates who create, receive, transmit, or maintain PHI.[69] Hypothetically, the doctor's office in *Byrne* could have contracted with an electronic medical record (EMR) company to store Byrne's records. That EMR company could have subcontracted to another company to host the data. If the hosting company released the records pursuant to the subpoena, it would be defending this lawsuit, instead of the doctor's office because it *received* and *maintained* PHI.[70]

Critics may argue that tort suits like *Byrne*, combined with HITECH's expansion of entities subject to HIPAA, impose excessive liability. However, the expansion of entities subject to HIPAA makes sense given the increase in data breaches and sensitive information shared among various entities, both inside and outside the traditional healthcare space.[71] The sensitive information is no less sensitive when in the hands of a software company (a business associate) than when in the hands of the doctor (a covered entity). Thus, the information should be afforded the same protections and the entities should bear the same liabilities.

A. Data Breaches and HIPAA Violations Are Increasingly Common

Data breaches and HIPAA complaints, increasingly common, provide the basis for negligence claims akin to those in *Byrne*.[72] Negligent

69. *See* 42 U.S.C. § 17938 (2012); Modifications to HIPAA Under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act, 78 Fed. Reg. at 5572; *supra* Part II.

70. Modifications to HIPAA Under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act, 78 Fed. Reg. at 5572.

71. H.R. REP. NO. 111-16, at 485–86 (2009). In March 2015, Premera Blue Cross, another large health insurer, announced that eleven million customers' medical records were improperly accessed. Jim Finkle, *Premera Blue Cross Breached, Medical Information Exposed*, REUTERS, Mar. 17, 2015, http://www.reuters.com/article/2015/03/17/ us-cyberattack-premera-idUSKBN0MD2FF20150317 [https://perma.cc/F2EJ-NG5P]. In August 2014, Community Health Systems, a hospital operator, also announced a major data breach. Jason Millman, *Health Care Data Breaches Have Hit 30M Patients and Counting*, WASH. POST (Aug. 19, 2014), http://www.washingtonpost.com/blogs/wonkblog/ wp/2014/08/19/health-care-data-breaches-have-hit-30m-patients-and-counting/ [https://perma. cc/BRG3-UHDD]. Chinese hackers stole 4.5 million medical records. *Id.*

72. *See Health Information Privacy Complaints Received by Calendar Year*, U.S. DEP'T HEALTH & HUMAN SERVS., http://www.hhs.gov/ocr/privacy/hipaa/enforcement/ data/complaintsyear.html [https://perma.cc/48AJ-WP4B] (last visited Feb. 8, 2016).

employees caused at least thirty percent of data breaches in 2014.[73] In addition to negligence, hackers have incentive to pursue health information. An individual's health information is worth approximately ten dollars, which is ten to twenty times the value of the same person's credit card number.[74] Also in 2014, data breaches reached a record high in the United States.[75] These statistics show that a negligent employee's mistake may cause an employer to bear liability in a negligence suit. And, the monetary incentive for hackers warrants companies strengthening policies, procedures, and training to ensure effective HIPAA compliance.

Additionally, HIPAA complaints are on the rise.[76] Between 2004 and 2013, the number of HIPAA complaints increased consistently.[77] The number of complaints in 2014 is nearly double the number in 2004.[78] This increase can be explained by two reasons. First, as discussed above, data breaches are occurring more often because health information is increasingly valuable.[79] Second, HITECH requires covered entities and business associates to notify individuals and the Secretary of HHS when unsecured health information is breached.[80] This notification requirement alerts individuals of potential claims against negligent entities.

---

73. *See* PONEMON INST., 2014: A YEAR OF MEGA BREACHES 11 (2015), http://www.ponemon.org/local/upload/file/2014%20The%20Year%20of%20the%20Mega%20Breach%20FINAL_3.pdf [https://perma.cc/NK3B-5PMQ]. In addition, an executive at Experian's data breach resolution group estimates that 80% of the breaches he works with are caused by a negligent employee. Elizabeth Weise, *43% of Companies Had a Data Breach in the Past Year*, USA TODAY (Sept. 24, 2014, 3:33 PM), http://www.usatoday.com/story/tech/2014/09/24/data-breach-companies-60/16106197/ [https://perma.cc/H8NH-R2J2].

74. Caroline Humer & Jim Finkle, *Your Medical Record Is Worth More to Hackers than Your Credit Card*, REUTERS, Sept. 24, 2014, http://www.reuters.com/article/2014/09/24/us-cybersecurity-hospitals-idUSKCN0HJ21I20140924 [https://perma.cc/SQK9-D5NV].

75. *Identity Theft Research Center Breach Report Hits Record High in 2014*, IDENTITY THEFT RESOURCE CTR. (Jan. 12, 2015), http://www.idtheftcenter.org/ITRC-Surveys-Studies/2014databreaches.html [https://perma.cc/9HD6-E3A5]; IDENTITY THEFT RES. CTR., DATA BREACH REPORTS (2014), http://www.idtheftcenter.org/images/breach/DataBreachReports_2014.pdf [https://perma.cc/N7Q4-GR98] (finding 783 known breaches affecting over eighty-five million records).

76. *Health Information Privacy Complaints Received by Calendar Year*, *supra* note 72.

77. *Id.* But, from 2008 to 2009 there was a slight decrease in complaints. *Id*.

78. *Id.* (receiving 6,534 violations in 2004 and 12,915 violations in 2014).

79. Humer & Finkle, *supra* note 74.

80. *See generally*, 45 C.F.R. §§ 164.400–414 (2014).

B. Damages—The Nail in the Coffin

The threat of damages in tort suits should improve compliance by the various entities subject to HIPAA regulation. Although the Connecticut Supreme Court did not award damages because it remanded for further proceedings, the core holding in *Byrne*, combined with HITECH's expansion of applicability, opens the door to a flood of litigation.[81]

To demonstrate the possible implications from *Byrne*, consider a similar case in a different state where damages were awarded. The plaintiff in *Walgreen Company v. Hinchy* successfully sued Walgreen for negligence.[82] The plaintiff claimed that Walgreen was negligent for failing to monitor its employee's use and disclosure of PHI.[83] A Walgreen's employee disclosed the plaintiff's prescription records, which were used to harass and extort the plaintiff.[84] An Illinois court of appeals held Walgreen's and its employee liable under a theory of negligence for a HIPAA violation and affirmed a $1.44 million damages award.[85]

The *Walgreen* damages award far exceeds the $50,000 maximum fine that HHS could levy against Walgreen for a single incident.[86] This should frighten Walgreen because tort suits are not subject to the cap. Thus, Walgreen is subject to both the damages award and HHS civil monetary penalty for its behavior. The result gives teeth to the formerly toothless monster. Covered entities and business associates subject to HIPAA would be wise to take note and increase their efforts to comply with HIPAA because failure to do so may result in a multitude of large damages awards that are not subject to the HIPAA statutory cap.

VI. *BYRNE* IS BIGGER THAN CONNECTICUT

Byrne is the first state supreme court case to establish HIPAA requirements as a standard of care in tort.[87] Although this is a state court

---

81. *See* Byrne v. Avery Ctr. for Obstetrics & Gynecology, P.C., 102 A.3d 32, 42 (Conn. 2014) ("We note . . . that whether Connecticut's common law provides a remedy for a health care provider's breach of its duty of confidentiality . . . is not an issue present in this appeal."). Thus, the court remanded the case with the instruction that HIPAA can be used as the standard of care if the trial court determines the plaintiff can sufficiently plead her negligence claim. *Id.* at 51.

82. Walgreen Co. v. Hinchy, 21 N.E.3d 99, 105, 114 (Ind. Ct. App. 2014).

83. *Id.* at 105.

84. *Id.* at 104–05.

85. *Id.* at 106, 109–10, 114.

86. 42 U.S.C. § 1320d-5(a)(3)(D) (2012).

87. Many other states have considered the issues, some holding that HIPAA does not preempt state law. *See e.g.*, Acosta v. Byrum, 638 S.E.2d 246 (N.C. Ct. App. 2006); Sorensen v. Barbuto, 2006 UT App 340, 143 P.3d 295, *aff'd*, 2008 UT 8, 177 P.3d 614 (affirming issues on appeal other than the HIPAA standard of care issue). Additionally,

ruling, it carries national implications for two reasons. First, the tort right established in *Byrne* belongs to each Connecticut resident.[88] Therefore, every entity subject to HIPAA with PHI of a Connecticut resident owes a standard of care based on HIPPA compliance and is subject to tort suits for negligent noncompliance. Second, other state appellate courts recognize HIPAA as a standard of care.[89] This not only increases entities' exposure to liability—as individuals in multiples states are owed a duty of care and can sue upon breach—but it also affirms a nationwide trend.

A. The Right to Use HIPAA as a Standard of Care Belongs to Connecticut Residents

To illustrate the subsequent points, consider the most recent data breach at Anthem, the second largest health insurer in the United States.[90] Of the eighty million people whose information was stolen, Connecticut officials estimate over one million Connecticut residents will be affected by the breach.[91] Each plaintiff can likely recover money if Anthem was negligent and there are cognizable damages.[92]

---

the West Virginia Supreme Court of Appeals made note of this possibility, but only held as to the preemption issue. *See* R.K. v. St. Mary's Med. Ctr., Inc., 735 S.E.2d 715, 723–24 (W. Va. 2012). But, Connecticut's Supreme Court is the first high court to squarely hold that HIPAA is a reasonable standard of care. *See De Facto Private Right of Action Under HIPAA: Is Ohio Next?*, THOMPSON HINE (Dec. 16, 2014), http://www.thompsonhine.com/publications/de-facto-private-right-of-action-under-hipaa-is-ohio-next [https://perma.cc/7Y6B-ACRL].

88. *See supra* Part VI.A.

89. *See* cases cited *supra* note 87. *But see*, Young v. Carran, 289 S.W.3d 586, 588 (Ky. Ct. App. 2008) ("HIPAA does not create a state-based private cause of action for violations of its provisions."); Bonney v. Stephens Mem'l Hosp., 2011 ME 46, ¶ 20, 17 A.3d 123, 128 (holding that because HIPAA does not provide a private cause of action, it cannot create a standard for violation of state common law).

90. *See generally* Supriya Kurane & Jim Finkle, *Health Insurer Anthem Hit by Massive Cybersecurity Breach*, REUTERS, Feb. 5, 2015, http://www.reuters.com/article/2015/02/05/us-anthem-cybersecurity-idUSKBN0L907J20150205 [https://perma.cc/X9G3-QEDC].

91. *Anthem Breach Could Affect 1.4 Million Connecticut Residents*, NBC CONN. (Feb. 5, 2015, 11:55 AM), http://www.nbcconnecticut.com/news/local/Connecticut-Officials-Looking-Into-Anthem-Cyber-Attack-290932161.html [https://perma.cc/H9T3-PXJP].

92. Although hacking is a crime, a negligent action can make it easier for the hacker. For instance, a class action plaintiff alleges that failure to encrypt medical records was negligent. Class Action Complaint & Demand for Jury Trial at 18, 20, Liu v. Anthem, Inc., No. 8:15-cv-00215 (C.D. Cal. Feb. 6, 2015), 2015 WL 5968438.

For the *Byrne* holding to apply to Anthem when sued by a Connecticut plaintiff in Connecticut state court, the plaintiff would need to prove that the Connecticut court has personal jurisdiction over Anthem, and that the court should apply Connecticut state law. The court would be able to exercise personal jurisdiction because it is within the purview of Connecticut's long-arm statue, Anthem regularly conducts business in Connecticut, and Anthem has minimum contacts with Connecticut.[93] The court would also apply Connecticut state law because the injury occurred in Connecticut, and the parties' relationship is more heavily centered in Connecticut where most, if not all, insurance benefits are provided to the Connecticut resident.[94]

This analysis shows the far-reaching implications of *Byrne*. Any entity that creates, receives, transmits, or maintains the PHI of a Connecticut resident will be subject to Connecticut state law and thus the ruling in *Byrne*. Therefore, if this entity is negligent in safeguarding, using or disclosing PHI, it may be liable in tort.

B. Other States Recognize HIPAA Standard of Care Argument

At least seven other states have also indicated that HIPAA may inform a standard of care in negligence suits.[95] Each of these states would also

---

93. A state court may exercise personal jurisdiction over a foreign corporation if it has statutory authority and satisfies the Due Process clause of the Fourteenth Amendment. *See* Int'l Shoe Co. v. Washington, 326 U.S. 310, 319–20 (1945). Connecticut's long-arm statute reads, in part, "a court may exercise personal jurisdiction over any nonresident individual . . . who . . . (3) commits a tortious act outside the state causing injury to person or property within the state . . . if such person (A) regularly does or solicits business . . . in the state."). CONN. GEN. STAT. § 52-59b(a) (2015), https://www.cga.ct.gov/current/pub/chap_896.htm#sec_52-59b [https://perma.cc/G9X6-HH5S].

94. Connecticut applies the "most significant relationship test" to determine the choice of law. *See* O'Connor v. O'Connor, 519 A.2d 13, 25 (Conn. 1986). This analysis focuses on "(1) the place where the injury occurred, (2) the place where the conduct causing the injury occurred, (3) the domicile, residence, nationality, place of incorporation and place of business of the parties, and (4) the place where the relationship, if any, between the parties is centered." Victor G. Reiling Assocs. & Design Innovation, Inc. v. Fisher-Price, Inc., 406 F. Supp. 2d 175, 200 (D. Conn. 2005).

95. *See* I.S. v. Washington Univ., No. 4:11CV235SNLJ, 2011 WL 2433585, at *2 (E.D. Mo. June 14, 2011) ("[T]he Court finds that Count III may stand as a state claim for negligence per se despite its exclusive reliance upon HIPAA."); Harmon v. Maury Cnty., No. 1:05 CV 0026, 2005 WL 2133697, at *3, *4 (M.D. Tenn. Aug. 31, 2005); Walgreen Co. v. Hinchy, 21 N.E.3d 99, 109–10 (Ind. Ct. App. 2014); Yath v. Fairview Clinics, 767 N.W.2d 34, 49–50 (Minn. Ct. App. 2009) (holding Minnesota statute not preempted by HIPAA); Acosta v. Byrum, 638 S.E.2d 246, 251 (N.C. Ct. App. 2006) ("Here, defendant has been placed on notice that plaintiff will use . . . HIPAA to establish the standard of care. Therefore, plaintiff has sufficiently pled the standard of care in her complaint."); Sorensen v. Barbute, 2006 UT App 340, ¶ 11 n.2, 143 P.3d 295, 300-01, *aff'd*, 2008 UT 8, 177 P.3d 614; R.K. v. St. Mary's Med. Ctr., Inc., 735 S.E.2d 715, 721–23 (W. Va. 2014).

require a personal jurisdiction and choice of law analysis.[96] Although that is beyond the scope of this Note, it is clear that many of them would come to the same result as Connecticut—namely, their laws apply to a tort suit against Anthem. The Anthem breach affected million of people in these seven states, meaning Anthem could spend millions of dollars settling lawsuits.[97]

In addition to highlighting the looming threat of lawsuits, the *Byrne* decision affirms a trend in court decisions—HIPAA as a standard of care is here to stay. Courts recognized this as early as 2005,[98] as recently as November 2014,[99] but the *Byrne* decision was the first by a state supreme court.[100]

C. The Reality of Tort Liability—Class Actions

Given the staggering number of individuals affected by the 2015 breach, Anthem now faces class action lawsuits nationwide.[101] These suits allege that Anthem's failure to safeguard information pursuant to HIPAA was negligent.[102] The class action suit filed in Connecticut has clear precedent

96. *See supra* Part VI.A.

97. *See, e.g.*, Garrett Haake, *Millions in Missouri, Thousands in Kansas Impacted by Anthem Data Breach*, http://www.kshb.com/news/local-news/millions-in-missouri-thousands-in-kansas-impacted-by-data-breach [https://perma.cc/8VN8-KXZV] (last updated Feb. 24, 2015, 9:09 AM) (estimating over two million Missouri residents will be affected); Alena Oakes, *New Details: Anthem Breach Affecting over 700k in NC*, http://wvtm.membercenter.worldnow.com/story/28193680/new-details-anthem-breach-impacting-over-700k-in-nc [https://perma.cc/Z6V3-NLKL] (last updated Mar. 17, 2015) (estimating 775,000 individuals affected in North Carolina). Additionally, Target recently settled a class action lawsuit for ten million dollars relating to its major data breach. *See* Peter Cooney & Supriya Kurane, *Target Agrees To Pay $10 Million To Settle Lawsuit from Data Breach*, REUTERS, Mar. 19, 2015, http://www.reuters.com/article/2015/03/19/us-target-settlement-idUSKBN0MF04K20150319 [https://perma.cc/Y4H9-MYGD]. Anthem is likely to face an even higher settlement amount because it had twice the number of affected records and stored health information, which is more valuable than the consumer information Target held. Class action lawsuits have already been filed against Anthem. *See, e.g.*, Class Action Complaint & Demand for Jury Trial, *supra* note 92, at 1.

98. *See Harmon*, 2005 WL 2133697, at *4.

99. *See Walgreen*, 21 N.E.3d at 109–10.

100. *See* cases cited *supra* note 87.

101. *See, e.g.*, Class Action Complaint & Demand for Jury Trial, *supra* note 92; Complaint, D'Angelo v. Anthem, Inc., No. 1:15-cv-00371 (N.D. Ga. Feb 5, 2015) [hereinafter D'Angelo Complaint], http://media.bizj.us/view/img/5018191/anthem.pdf [https://perma.cc/GM5S-K4DJ]; Class Action Complaint, Juliano v. Anthem, Inc., No. 2:15-cv-00219-SLB (N.D. Ala. Feb. 5, 2015) [hereinafter Juliano Complaint].

102. *See* Class Action Complaint & Demand for Jury Trial, *supra* note 92, at 17–18; D'Angelo Complaint, *supra* note 101, at 22; Juliano Complaint, *supra* note 101, at 18, 21.

under *Byrne*.[103] However, courts in other states will have to address whether HIPAA preempts the state law claims, and if not, whether HIPAA can inform a standard of care.

For instance, count sixty-eight in *Liu v. Anthem* alleges that Anthem's failure to comply with HIPAA constitutes negligence per se.[104] In order to resolve that case, the court will have to first decide whether HIPAA preempts state law claims of negligence. If HIPAA does not preempt, the court will then decide whether to use HIPAA as a standard of care in negligence suits.

Although the Connecticut Supreme Court decision in *Byrne* is not binding on other states, it is highly persuasive. The plaintiff in *Liu* should use the court's reasoning in *Byrne* because its logic is not unique to Connecticut.[105] First, enforcing state laws regarding negligence increases privacy protection in California, just as it does in Connecticut. Second, the legislative intent of a federal agency (HHS) is applicable to all courts. Thus, a California plaintiff should assert these same arguments when persuading a court to hold HIPAA does not preempt California law.

If the district court of California determines that HIPAA does not preempt California state law, it would then have to determine whether HIPAA should inform the standard of care in a negligence claim. The California plaintiff has ample persuasive authority from eight states to argue that it should join the nationwide trend allowing HIPAA as a standard of care in negligence based lawsuits.[106]

If the plaintiff is successful in *Liu*, Anthem and all other entities subject to HIPAA, are in trouble. To avoid class action litigation these entities must heighten their HIPAA compliance and recognize that failure to address data privacy and security can have a drastic effect on their bottom line.

VII. CONCLUSION

Protecting patient privacy is critical in the digital age. Health information is no longer stored in a locked file cabinet at a doctor's office. Instead, it travels from a doctor's computer, through the cloud, via the Internet and resides on a server that is remotely accessible. The pathway and residence of these data are susceptible to unwarranted access. Adopting technological solutions is critical to fixing the healthcare system. But, shifting a pen

103. Complaint at 13–14, Peterman v. Anthem, Inc., No. 3:15-cv-00250 (D. Conn. Feb. 20, 2015).

104. Class Action Complaint & Demand for Jury Trial, *supra* note 92, at 18.

105. *See supra* Part III.B.

106. *See* Byrne v. Avery Ctr. for Obstetrics & Gynecology, P.C., 102 A.3d 32 (Conn. 2014); cases cited *supra* note 95.

and paper industry to the cloud increases the risk of violating the individual's privacy. The decision in *Byrne* incentivizes increased protection of PHI and empowers individuals with a remedy when entities fail to protect their highly personal and private information.