PAYING PRICES FOR SWIPED DEVICES: ADDRESSING THE ISSUE OF MEDICAL IDENTITY THEFT FROM UNENCRYPTED STOLEN LAPTOPS

MICHAEL PALUZZI*

Hospitals are plagued by constant attempts at information hijacking. In the face of increased malware threats, there is an incentive to shift focus in healthcare security toward digital breaches. But hospitals would be wise to continue attending to traditional sources of breach liability, like laptop theft, which are much more common and can have similarly damaging effects. Despite federal regulations' best efforts to curb them, these issues persist. This Note analyzes potential solutions from three angles—regulatory, legislative, and judicial—to determine what can best motivate health systems to proactively prevent such breaches. I suggest and explore several options, including a regulatory mandate on laptop encryption, legislation inspired by the European Union's recent data privacy laws, and loosened standing in threat of future harm cases.

TABLE OF CONTENTS

I. INTRODUCTION 1416
II. BACKGROUND 1418
  A. *The Threat of Laptop Theft* 1419
  B. *Regulation: A Rundown on HIPAA Risk Assessments and Breach Notification* 1422
  C. *Legislation: Federal Hesitancy and State Inconsistency* 1424
    1. *Congress Refuses to Follow the European Union's Lead* 1424
    2. *State Breach Laws are a Patchwork of Inconsistency* 1425
  D. *Adjudication: Circuits are Split on Conferring Article III Standing in Laptop Theft Cases* 1425
III. ANALYSIS 1427
  A. *PHI Breach Regulations and What They Do Now* 1427
  B. *Legislative Failings in Privacy Protections* 1431

* University of Illinois College of Law, J.D. expected 2019; University of Notre Dame, B.A. 2015. I would like to thank Robin Fretwell Wilson, Rummana Alam, and Kurt A. Leifheit for their helpful insight and comments. Thank you also to all members of the *University of Illinois Law Review* for their meticulous editing. All views and errors expressed in this Note are my own.

1. Might the GDPR of the European Union Inspire a Second Wave? 1431
2. California is Leading the Way in State Law Consumer Protections 1432
C. When Laptop Theft Goes to Court, Article III Standing has Courts Divided 1433
1. Article III Standing Generally and Shifting Supreme Court Standards 1433
2. How the Courts are Divided over Speculative Harm in Data Breach Cases 1436
IV. RECOMMENDATION 1442
A. HHS Should Mandate Portable Device Encryption for Covered Entities 1442
B. Legislatures Should Put an End to Statutory Inconsistencies 1443
C. The Supreme Court Should Resolve the Circuit Split by Conferring Standing in Data Breach Cases of This Kind 1443
V. CONCLUSION 1445

I. INTRODUCTION

There are many concerns that one might have when attending a hospital for medical care. What if my doctor is young and inexperienced? What if I catch an illness from a nearby patient? What if they cannot cure my illness? While all questions of this kind are important to ask, they all presume that the sky is falling. Healthcare today is generally safe and effective. Healthcare management, however, struggles to keep up. To add a new, more concerning and horrifyingly justified question to the docket, one should ask, what if my healthcare provider is not adequately protecting my healthcare information, which can include everything from prescriptions, to banking information, social security numbers, addresses, phone numbers, and so on. Most people probably assume, because a hospital holds itself as the paragon of safety, that their medical information is safe within it. Unfortunately, that is often not the case. Take, for example, a common form of information breach: the stolen laptop.

You find yourself in an ambulance being rushed to the hospital. A machine to your right continuously monitors your vital signs and contains clinical information specific to your current situation. That data, along with what information the hospital can reach through your and others' input after admission, is loaded and secured in a medical database, which exists across the health system's network. A medical professional revisits your clinical information on his laptop. After work, he leaves that laptop in the backseat of his car in the hospital parking lot, and it's stolen. The laptop, according to agency suggested guidelines, should

have been encrypted.[1] But hospitals often don't encrypt their laptops.[2] This may result from ineffective laws and regulations, little to no judicial liability, or a lack of management within the healthcare entity itself. Whatever the cause, the result is your vulnerability as a patient. Hospitals are meant to care for those most vulnerable in our society, and the law is meant to do the same. With regard to medical information protection, neither are meeting our needs.

Identity theft can take on many forms. Common forms include account, tax, and employment identity theft, each of which carry their own dangers.[3] The danger posed by medical identity theft, the incidence of which has recently risen,[4] is that in addition to these common acts, fraudsters can use your information for medical purposes. They can buy drugs, gain access to care, and do just about anything that you can with that information. "Medical identity theft is one of the fastest growing areas of identity fraud in the world,"[5] and its effects are harsh.

Hospitals are plagued by constant threats of information hijacking. Given the immense value found in medical information,[6] and the liability that comes with its loss,[7] protection of this information makes both public policy and business sense for healthcare systems. Still, hospitals seem reluctant to change longstanding habits of nonencryption that might otherwise mitigate dangerous data disclosure.[8] If health systems are lax about protecting this information, patients are at risk of having their identities stolen when that data gets into the wrong hands. While recent events have shifted focus to concerns about malware proliferation and digital breaches, especially considering hospitals' unique vulnerability to such threats,[9] hospitals should keep their attention on this much

1. *See* HIPAA SECURITY GUIDANCE, U.S. DEP'T OF HEALTH & HUMAN SERVS. 5–6 (2006) [hereinafter HIPAA SECURITY GUIDANCE], https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/remoteuse.pdf.

2. Laura Wagner, *Study: Some Hospitals Lack Even Basic Data Protection for Patient Records*, SLATE (Aug. 23, 2016, 5:19 PM), https://slate.com/technology/2016/08/new-study-shows-your-medical-records-could-be-at-risk.html.

3. Kim Porter, *10 Types of Identity Theft You Should Know About*, LIFELOCK, https://www.lifelock.com/learn-identity-theft-resources-types-identity-theft.html (last visited May 21, 2019).

4. *See Identity Theft Victim Stunned by $52G Hospital Bill: report*, FOX NEWS (Oct. 27, 2017) [hereinafter Fox Report], http://www.foxnews.com/health/2017/10/27/identity-theft-victim-stunned-by-52g-hospital-bill-report.html.

5. Mike Delgado, *Helping Hospitals Prevent Medical Identity Theft to Protect Patients from Fraud*, EXPERIAN (Mar. 18, 2017), http://www.experian.com/blogs/news/2017/03/18/medical-identity-fraud/.

6. Caroline Humer & Jim Finkle, *Your Medical Record is Worth More to Hackers than Your Credit Card*, REUTERS (Sept. 24, 2014, 1:25 PM), https://www.reuters.com/article/us-cybersecurity-hospitals/your-medical-record-is-worth-more-to-hackers-than-your-credit-card-idUSKCN0HJ21I20140924 ("Your medical information is worth 10 times more than your credit card number on the black market.").

7. Generally, liability for nonprotection of health information is considered a breach of regulations set out by the Department of Health and Human Services. *See infra* Section II.B.

8. Wagner, *supra* note 2.

9. For a discussion on the reasons for hospitals' unique vulnerability to malware breaches, see Selena Larson, *Why Hospitals Are So Vulnerable to Ransomware Attacks*, CNN (May 16, 2017, 1:46 PM), http://money.cnn.com/2017/05/16/technology/hospitals-vulnerable-wannacry-ransomware/index.html.

more common style of breach resulting from laptop thefts[10] to better protect themselves and their patients. The industry likely will not make this change independently; regulators, legislators, and the courts can each play a part in motivating hospitals to amend internal policies in favor of disclosure mitigation by way of preventing laptop theft and mandating laptop encryption.

Part II of this Note provides background information on the history of regulations, statues, and court rulings relevant to medical data breaches.[11] Part III of this Note analyzes from three perspectives—regulatory, legislative, and judicial—how pressure can be placed on health systems to encrypt their devices.[12] Part IV of this Note suggests three resolutions: that the Department of Health and Human Services ("HHS") should mandate encryption of portable devices; that Congress or state legislatures should enact statutes that make consistent data breach laws and provide for private rights of action for patients whose information has been disclosed; and that courts should resolve a current circuit split by granting standing to victims of laptop theft cases, thus creating greater incentive for hospitals to encrypt their devices.[13]

II. BACKGROUND

Electronic devices are necessary in medical care, as is the sharing of information between those devices.[14] Proper care benefits from clear lines of communication between providers. Unfortunately, that same communication can harm patients when it is done outside of regulatory bounds or with a lack of consideration for device protection. To properly defend patients against the risk of data breach from device theft, health systems must increase protective measures over such devices and the data within. Without some motivation to do so, they will continue to resist such a change. This Note analyzes possible means of motivation through regulatory, legislative, and judicial frameworks that make it likely that hospitals will be proactive about breach prevention. The following sections will first discuss the threat of laptop theft generally and then move on to explaining the regulations, statutes, and court rulings that create today's mostly ineffective patchwork system of data breach enforcement against health systems.

10. *See* Philip L. Gordon, *Employers and Health Care Providers Receive New Guidance on HIPAA Security Breach Notification*, LITTLER (Aug. 25, 2009), https://www.littler.com/es/publication-press/publication/employers-and-health-care-providers-receive-new-guidance-hipaa-0.

11. *See infra* Part II.

12. *See infra* Part III.

13. *See infra* Part IV.

14. Evan Schuman, *Why Does Healthcare Resist Encryption?*, HEALTHCARE IT NEWS (Apr. 17, 2014, 8:51 AM), http://www.healthcareitnews.com/news/why-does-healthcare-resist-encryption.

A. The Threat of Laptop Theft

Despite recent concerns about the threat of malware breach, unsecured protected healthcare information ("PHI") is the most at risk in laptop thefts.[15] Laptops are stolen at alarming rates.[16] Recently, the Office of Civil Rights ("OCR") has stepped up their enforcement protocols of HIPAA violations through audits.[17] Since 2008, fourteen major incidents of laptop theft have resulted in an average of $1.95 million paid in resolution, paired with corrective action plans.[18] Enforcement and resolution payments over laptop theft continue to rise.[19] At present, the penalties fall far short of motivating healthcare entities to encrypt their devices—their incidence is proof of enforcement and noncompliance alike.[20] The continuation of data breaches may be attributable to a number of different reasons: perhaps hospitals suffer from the "it won't happen to us" mentality or maybe management structures create conflicts among cost analyses, efficiency of care, and liability protection.

The most obvious risk of laptop theft is off-campus use or storage. While healthcare privacy regulations do not explicitly prohibit removal of portable devices from health provider centers, HHS has warned against it in recognition of the unique issue surrounding their theft.[21] The agency asserts that entities should be "extremely cautious about allowing the offsite use of, or access to, EPHI" (electronic PHI).[22] But some situations may warrant such use, like work done by home-health nurses, off-campus responses to requests for prescription refills, and transporting backup data to an off-site facility.[23]

Entities are required to complete and implement their own security risk analyses related to off-cite use.[24] HHS issued guidance on what factors to consider when determining security policies. These include: "(i) The size, complexity, and capabilities of the covered entity . . . (ii) The covered entity's . . . technical infrastructure, hardware, and software security capabilities. (iii) The costs of security measures. (iv) The probability and criticality of potential risks to

15. Michael Ollove, *The Rise Of Medical Identity Theft In Healthcare*, KAISER HEALTH NEWS (Feb. 7, 2014), https://khn.org/news/rise-of-indentity-theft/.

16. Kevin Helliker, *A New Medical Worry: Identity Thieves Find Ways to Target Hospital Patients*, WALL ST. J. (Feb. 22, 2005, 12:01 AM), https://www.wsj.com/articles/SB110902598126260237. *See, e.g.*, Resnick v. AvMed, Inc., 693 F.3d 1317 (2012).

17. Meggan Bushee & Nathan Kottkamp, *New Government Audits to Target Non-compliance with HIPAA and the HITECH Act*, BENDER'S HEALTH CARE L. MONTHLY, Oct. 1, 2015, at 1.

18. Statistics calculated from information listed in *OCR/FTC HIT Enforcement Summary Table*, AM. HEALTH LAW. ASS'N (Oct. 2017) [hereinafter *Summary Table*], https://www.healthlawyers.org/Members/PracticeGroups/HIT/Toolkits/Pages/OCRFTC_HIT_Enforcement_Summary_Table.aspx.

19. 2016 showed the highest incidence of enforcement related to laptop thefts, resulting in an average of 3.29 million dollars of payment. *Id.*

20. Ollove, *supra* note 15.

21. For the earliest and most relevant discussion by HHS on this matter, see HIPAA SECURITY GUIDANCE, *supra* note 1, at 1.

22. *Id.*

23. *Id.* at 1–2.

24. *See infra* Section II.B.

[EPHI]."[25] When narrowly discussed with relevance to portable device usage and access, HHS states that "[c]overed entities should place significant emphasis and attention on their: Risk analysis and risk management strategies; Policies and procedures for safeguarding EPHI; Security awareness and training on the policies & procedures for safeguarding EPHI."[26] In addition to requiring policies relevant to storage of health information, HHS recommends that entities train personnel on "password management procedures (for changing and safeguarding passwords); remote device/media protection to reinforce policies that prohibit leaving devices/media in unattended cars or public thoroughfares; as well as training on policies prohibiting the transmission of EPHI over open networks (including email) or downloading EPHI to public or remote computers."[27] For entities whose policies allow for off-site use and access of PHI, HHS suggests management strategies as responses to specific risks.[28] Risk management strategies specific to laptop theft include developing inventory systems, recording who is allowed to move devices with access to PHI, requiring lock-down measures on unattended devices, password-protecting devices and files within, employing encryption technologies of "appropriate strength," regularly updating security of the devices, and "[c]onsider[ing] the use of biometrics, such as fingerprint readers, on portable devices."[29]

These suggestions are all uniquely aimed at known vulnerabilities like laptop theft, but to date they are simply not enough to motivate healthcare entities to encrypt their devices or otherwise avoid unwanted disclosures of this kind. It may be that anything short of mandatory encryption allows industry judgment to justify nonencryption, thus leaving patients at risk of identity theft now and in the future.

It seems, according to current statistics on laptop theft and liability therefore, that laptop encryption is the most important security measure of those suggested by HHS.[30] This is because encryption, when it relates to stored data, effectively makes health information not definable as PHI under HIPAA, thus providing a safe harbor in breach regulations for hospitals faced with potentially required notification procedures.[31] According to the governing regulation, encryption is "the use of an algorithmic process to transform data into a form in

25. 45 C.F.R. § 164.306(b)(2) (2018). Once the entity has analyzed potential risks associated with remote access and use of PHI, it must develop risk management measures to reduce such risks in compliance with § 164.306(a).

26. *See* HIPAA SECURITY GUIDANCE, *supra* note 1, at 2.

27. *Id.* at 3.

28. For a comprehensive list of all risks specified by HHS and related management strategies, see *id.* at 4–6.

29. *Id.* at 5.

30. The OCR specifically mentions and admonishes health entities' lack of laptop encryption. *See Summary Table*, *supra* note 18.

31. *Guidance to Render Unsecured Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals*, U.S. DEP'T OF HEALTH & HUM. SERVS., https://www.hhs.gov/hipaa/for-professionals/breach-notification/guidance/index.html (last visited Aug. 8, 2019).

which there is a low probability of assigning meaning without use of a confidential process or key."[32] Entities that have properly encrypted their devices can enjoy a safe harbor from HIPAA's Breach Notification Rule and avoid having to contact every patient whose information is stored in the encrypted laptop.[33] Encryption should be low hanging fruit for healthcare entities—an easy way to avoid millions of dollars in resolution payments, corrective action plans by the OCR, and class action lawsuits by patients whose information was stolen. This safe harbor, however, has proven insufficient to motivate health systems to encrypt their devices diligently.

In light of the fact that an estimated 45% of all healthcare breaches occur as a result of laptop thefts,[34] why does the healthcare industry continue to leave laptops unencrypted and thus make themselves vulnerable to OCR investigation and potential lawsuits over patient identity theft? One suggestion is that resistance to change may exist mostly at the individual level.[35] "Healthcare organization executives themselves are not resisting encryption, but when it gets to the doctor and nurse level, there is a more heated battle."[36] Physicians and their cohort are motivated to resist encryption to increase efficiency in an industry that is dependent on continuous horizontal movement of information.[37] But "[p]roperly done encryption should not interfere with medical systems."[38] Another possibility is a comingling of management groups that have incongruent goals. For instance, information security, as a group that identifies these sorts of risks and implements policies aimed at resolving them, may at times be embedded within the information technology or risk management groups at healthcare organizations. This can create a dissonance between encryption and a need for pushing vital information to physicians, one of which will inevitably succumb to the other. Encryption is a difficult stance to take when HHS does not make it explicitly mandatory.

Something must put pressure on health systems to move toward increased protection measures over patient information. As penalty rates rise, and breaches still occur, it becomes apparent that the current administration's solution is insufficient to shift the balance. The following sections will discuss three potential sources of such pressure: regulation, legislation, and adjudication.

32. 45 C.F.R. § 164.304 (2018).

33. *See* 45 C.F.R. §§ 164.400–414 (2018).

34. Mark Santamaria, *45% of Healthcare Breaches Occur on Stolen Laptops*, DIGICERT (Apr. 13, 2016), https://www.digicert.com/blog/45-percent-healthcare-breaches-occur-on-laptops/.

35. Schuman, *supra* note 14 (quoting Lysa Myers, a security researcher at software vendor ESET).

36. *Id.*

37. *Id.*

38. *Id.*

B. Regulation: A Rundown on HIPAA Risk Assessments and Breach Notification

Congress passed the Health Information Portability and Accountability Act ("HIPAA") as a response to the "rapid evolution of health information systems."[39] This empowered HHS to establish regulations over the past twenty-one years related to PHI safety, namely the Privacy Rule from 2000,[40] the Security Rule from 2003,[41] the Enforcement Rule from 2006,[42] the Breach Notification Rule from 2009,[43] and the Omnibus Rule—which modified all previous rules—from 2013.[44] In 2011, OCR launched its audit program.[45] Phase Two of this program "enhanced protocols . . . to be used in the next round of audits . . . in evaluating the compliance efforts of the HIPAA regulated industry."[46] Put simply, regulations have been built slowly as a response to growing concerns over medical data breaches, and through them HHS and OCR have been tightening their grip on healthcare entities who refuse to comply.

Hospitals are constantly at risk of information breaches that result in violations of these federal laws and regulations, and that puts their patients at risk. Since its enactment in 1996,[47] HIPAA has protected the confidentiality of patients' PHI.[48] "PHI is individually identifiable information in any form relating to an individual's healthcare, payment for healthcare, or physical or mental

39. Standards for Privacy of Individually Identifiable Health Information, 67 Fed. Reg. 53,182 (Aug. 14, 2002) (codified at 45 C.F.R. pts. 160 and 164).

40. Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. 82,462 (Dec. 28, 2000) (codified at 45 C.F.R. pts. 160 and 164). Revisions were published at 67 Fed. Reg. 53,182, (Aug. 14, 2002) (codified at 45 C.F.R. pts. 160 and 164).

41. Health Insurance Reform: Security Standards, 68 Fed. Reg. 8334 (Feb. 20, 2003) (codified at 45 C.F.R. pts. 160, 162, and 164).

42. HIPAA Administrative Simplification: Enforcement, 71 Fed. Reg. 8390 (Feb. 16, 2006) (codified at 45 C.F.R. pts. 160 and 164). Revisions were published at HIPAA Administrative Simplification: Enforcement, 74 Fed. Reg. 56,123 (Oct. 30, 2009) (codified at 45 C.F.R. pt. 160).

43. Breach Notification for Unsecured Protected Health Information, 74 Fed. Reg. 42,740 (Aug. 24, 2009) (codified at 45 C.F.R. pts. 160 and 164).

44. Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act. Other Modifications to the HIPAA Rules, 78 Fed. Reg. 5566 (Jan. 25, 2013) (codified at 45 C.F.R. pts. 160 and 164).

45. *HIPAA Privacy, Security, and Breach Notification Audit Program*, U.S. DEP'T HEALTH & HUM. SERVS., https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/index.html (last updated Dec. 1, 2016).

46. *Id.*

47. Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936.

48. Jesse Pines & Jane Hyatt Thorpe, *10 Times HIPAA May Not Apply*, EMERGENCY PHYSICIANS MONTHLY (Sept. 1, 2015), http://epmonthly.com/article/10-times-hipaa-may-not-apply/.

health condition."[49] HIPAA protects this information through limiting disclosures outside of the physician-patient relationship.[50] A breach occurs when PHI is disclosed in violation of HIPAA.[51] In the event of a disclosure, the health provider's internal counsel does a risk assessment to determine whether there is a low probability of risk associated with the violation.[52] HHS provides factors to consider, which include the disclosed-to party, the type and amount of PHI disclosed, and any mitigating steps taken by the hospital to prevent risk.[53] The risk assessment generally attends to public concerns of financial, reputational, or other harm to an affected patient.[54] Notice must be made without reasonable delay, and within sixty days of the incident's discovery by a "workforce member"—this includes many actors in a hospital. Large breaches involving more than 500 victims must be made public by notification to HHS and to local prominent media.[55] Enforcement by HHS can range from fines of a few thousand dollars to more than a million dollars.[56] These settlements are often a drop in the bucket for healthcare companies valued at billions of dollars.[57]

There is constant debate over whether HIPAA's restrictions should be loosened; while "complete information is vital to making the best clinical decision[,]"[58] "protecting the privacy of people who seek care and healing" is of utmost importance.[59] Herein lies the dissonance from which an industry-wide oversight has grown. While encryption is viewed by some as a hindrance to patient care, the reality is that nonencryption is just as dangerous, if not more so. Due to the ongoing lack of consensus, current regulations under HIPAA do not require encryption.[60] And too often encryption is foregone because enforcement falls so short of deterrence that it feels like a slap on the wrist.

49. *Id.*; *see also Summary of the HIPAA Privacy Rule*, U.S. DEP'T HEALTH & HUM. SERVS. (July 26, 2013) [hereinafter *HIPAA Summary*], https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html ("'Individually identifiable health information' is information, including demographic data, that relates to: the individual's past, present or future physical or mental health or condition, the provision of health care to the individual, or the past, present, or future payment for the provision of health care to the individual, and that identifies the individual or for which there is a reasonable basis to believe it can be used to identify the individual. Individually identifiable health information includes many common identifiers . . . .").

50. Pines & Thorpe, *supra* note 48.

51. Gordon, *supra* note 10.

52. *Id.* For information on how a risk assessment is done, see *Guidance on Risk Analysis*, U.S. DEP'T OF HEALTH & HUM. SERVS. (Mar. 9, 2017), https://www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis/index.html.

53. Gordon, *supra* note 10.

54. *Id.*

55. *See id.*

56. For a description of enforcement fine ranges, see *HIPAA Violations & Enforcement*, AM. MED. ASS'N, https://www.ama-assn.org/practice-management/hipaa-violations-enforcement (last visited May 21, 2019).

57. *See, e.g.*, John Ribeiro, *EMC, Hospital to Pay $90,000 Over Stolen Laptop with Medical Data*, CSO (Nov. 9, 2015), https://www.csoonline.com/article/3003084/data-protection/emc-hospital-to-pay-90-000-over-stolen-laptop-with-medical-data.html (describing a healthcare provider whose laptop was stolen was fined $90,000 while undergoing an acquisition of by Dell at a value of $67 billion).

58. Pines & Thorpe, *supra* note 48.

59. *HIPAA Summary*, *supra* note 49.

60. For a good discussion of exactly what HIPAA does require with reference to encryption and other digital protection measures, see Patrick Townsend, *Does HIPAA Require Encryption of Patient Information*

C. Legislation: Federal Hesitancy and State Inconsistency

Legislative history of medical data protection goes not far past those statutes that empower HHS to promulgate the regulations described above. The U.S. Congress, despite its infatuation with privacy law enactment from the 1970s through the 1990s,[61] is now an irrelevant wasteland when it comes to new data protections. To fill this vacuum, many states have their own data privacy laws, none of which seem to agree about how enforcement should be handled.[62] By contrast, the European Union now has a broad, consistent, and powerful data-breach law—a suit which the U.S. Congress seems unwilling to follow.[63]

1. Congress Refuses to Follow the European Union's Lead

The United States has no central authority that protects data privacy.[64] While HHS acts to protect medical information, its regulations weakly punish at best. For perspective, compare the U.S. system to that of the European Union, which has enacted the General Data Protection Regulation ("GDPR").[65] The GDPR requires consent for data collection, simple language regarding data use, mandatory breach reporting, and—maybe most importantly—a private right of action for those whose data has been breached.[66] Unlike the U.S. regulatory regime, in which a relatively small number of regulators infrequently enforce pithy rules, the EU's health systems face about 500 million "regulators"—the approximate population of the EU.[67] Several more advanced economies, like Israel, Japan, and Canada, have begun moving toward the EU structure rather than the U.S.'s patchwork structure.[68]

(EPHI)?, TOWNSEND SECURITY DATA PRIVACY BLOG (Apr. 1, 2016, 8:53 AM), https://info.townsendsecurity.com/bid/74330/Does-HIPAA-Require-Encryption-of-Patient-Information-ePHI.

61. A long strand of data privacy enactments, starting with the Fair Credit Reporting Act in 1970 to the Gramm-Leach-Bliley Act in 1999, slowed considerably at the turn of the millennium. For a brief explanation, see Daniel Solove, *The U.S. Congress Is Not the Leader in Privacy or Data Security Law*, TEACH PRIVACY (Apr. 9, 2017), https://teachprivacy.com/us-congress-is-not-leader-privacy-security-law/.

62. *See* discussion *infra* Section II.C.2.

63. This refers to the General Data Protection Regulation ("GDPR"). Regulation (EU) 2016/679 of the European Parliament and of the Council, 2016 O.J. (L 119/1) [hereinafter, GDPR. For a discussion of the U.S. Congressional perspective, see Derek Hawkins, *The Cybersecurity 202: Why a Privacy Law Like GDPR Would be a Tough Sell in the U.S.*, WASH. POST (May 25, 2018), https://www.washingtonpost.com/news/powerpost/paloma/the-cybersecurity-202/2018/05/25/the-cybersecurity-202-why-a-privacy-law-like-gdpr-would-be-a-tough-sell-in-the-u-s/5b07038b1b326b492dd07e83/?noredirect=on&utm_term=.a790f845395f.

64. Leuan Jolly, *Data Protection in the United States: Overview*, LOEB & LOEB (Oct. 1, 2018), https://www.scribd.com/document/357996265/Data-Protection-in-the-United-States-Overview.

65. GDPR, *supra* note 63.

66. *Id.*

67. If considering the adult population alone, a better estimate might be around 300 million; still, a group this size can have a powerful impact on the social and market pressures that cause health systems to comply with the EU's laws. *European Union Demographics Profile 2018*, INDEX MUNDI, https://www.indexmundi.com/european_union/demographics_profile.html (last visited May 21, 2019).

68. Nuala O'Connor, *Reforming the U.S. Approach to Data Protection and Privacy*, COUNCIL ON FOREIGN RELATIONS (Jan. 30, 2018), https://www.cfr.org/report/reforming-us-approach-data-protection.

The best explanation for why the U.S. Congress refuses to follow the EU's path in making a federally consistent data breach law that provides a private right of action is that Congress prefers to leave such lawmaking and enforcement to the states. Whether one agrees with this politically, its result is a bundle of disagreeing, and often confusingly inconsistent, state-specific laws.

2. *State Breach Laws are a Patchwork of Inconsistency*

In the absence of federal legislation tying breach laws together consistently, states have opted to enact their own laws at varying degrees of potency. Some define personal information quite broadly, including things like passwords and biometric data, while others stick to a more conventional definition much like that of HIPAA.[69] Only Connecticut, Florida, New Jersey, and Puerto Rico laws trigger notification requirements by access of information, while the rest do not include access in the definition of breach.[70]

Most inconsistent is how these diverse laws enforce against breaches. While some states require notice to the Attorney General, who will then impose penalties, others provide for a private cause of action.[71] Sometimes this private right is interpreted from another statute entirely, further disrupting any consistency that might be salvaged in these laws, as is the case for the Illinois' Patient Information Protection Act ("PIPA").[72] Any violation of PIPA is by extension a violation of the Consumer Fraud and Deceptive Business Practices Act ("CFDBPA"), and thus all potential remedies are shared between them, including a private right of action.[73] This is only true, however, in the event of injury.[74]

This Note will advocate for consistency in state laws in the form of broadly granted private rights much like the EU standard discussed in the previous section. As is, the state framework of data privacy and breach enforcement is haphazard and just as ineffective as its federal regulatory analogs.

D. *Adjudication: Circuits are Split on Conferring Article III Standing in Laptop Theft Cases*

While regulators and legislators fail to enact change, the courts are in a unique position to put pressure on health systems to encrypt their devices. As discussed above, private rights of action do not always exist in breach laws. As

69. *Data Breach Charts*, BAKERHOSTETLER (July 2018), https://www.bakerlaw.com/files/Uploads/Documents/Data%20Breach%20documents/Data_Breach_Charts.pdf.

70. *Id.*

71. *Id.*

72. Personal Information Protection Act, 815 ILL. COMP. STAT. 530 (2018).

73. 815 ILL. COMP. STAT. 530/20 (2018).

74. *See* Smith v. Prime Cable of Chicago, 658 N.E.2d 1325 (Ill. App. Ct. 1995) (explaining that the CFDBPA provides for a private cause of action only where the plaintiff can show that he or she suffered damage as a result of unlawful conduct proscribed by statute). A portion of this Note will explore the possibility of extending recourse options to patients who merely suffer the threat of future identity theft. While courts are split over standing in these claims, their admission would put heavy pressure on providers to encrypt laptops to prevent breaches.

a default, HIPAA does not provide a private right of action for individuals who suffer harm from a health system's breach.[75] Instead, it allows for OCR enforcement actions and civil money penalties, with the perspective in mind that HIPAA breaches are a detriment to the public at large, not just the individual affected patient whose PHI was disclosed or used in violation:

> [E]lectronic health data is becoming increasingly 'national'; as more information becomes available in electronic form, it can have value far beyond the immediate community where the patient resides. Neither private action nor state laws provide a sufficiently comprehensive and rigorous legal structure to allay public concerns, protect the right to privacy, and correct the market failures caused by the absence of privacy protections.[76]

Given the lack of success with enforcement by way of administrative penalty, however, compounding liability with judicial action may be the next best option. The EU's model shows that private rights of action can be a powerful motivating tool.[77] This Note does not rally for change in the federal judiciary's stance on HIPAA private rights of action. But given that hospitals are required to notify patients whose data has been breached,[78] there are droves of patients who are forced to respond to their provider's lack of preparedness or to sit idly while their personal information is shuffled beyond their control. The solution is to follow what some federal circuits have allowed in cases of data breach—a claim for the threat of future identity theft.[79] As of now, standing for such claims is in question, as a circuit split exists on the matter.

The concept of standing is not explicitly outlined by the Constitution, but it has been inferred by the Supreme Court from Article III, Section 2, that federal courts must require the plaintiff in a case or controversy to show genuine interest and stake in the outcome of the matter.[80] Federal courts will dismiss a case if no plaintiff meets this standing standard.[81] The standard is that a plaintiff must prove a three part test: (1) that he or she has suffered an "injury in fact" that is (a) "concrete and particularized"[82] and (b) "actual or imminent" (not conjectural or hypothetical);[83] (2) "there [is] a causal connection between the injury and the conduct complained of—the injury has to be fairly . . . traceable to the challenged

75. *See HIPAA Summary*, *supra* note 49. *See also District Court Ruling Confirms No Private Cause of Action in HIPAA*, HIPAA J. (June 25, 2018), https://www.hipaajournal.com/district-court-ruling-confirms-no-private-cause-of-action-in-hipaa/.

76. 78 Fed. Reg. 5566 (Jan. 25, 2013) (codified at 45 C.F.R. pts. 160 and 164).

77. John Patzakis, *GDPR Provides a Private Right of Action. Here's Why That's Important.*, EDISCOVERY LAW AND TECH BLOG (Feb. 28, 2018), https://blog.x1discovery.com/2018/02/28/gdpr-provides-a-private-right-of-action-heres-why-thats-important/.

78. *Breach Notification Rule*, U.S. DEP'T OF HEALTH & HUM. SERVS., https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html (last visited Aug. 8, 2019).

79. *See* discussion *infra* Section III.C.

80. U.S. CONST. art. III, § 2.

81. *See id.*

82. Lujan v. Defenders of Wildlife, 504 U.S. 555, 560 (1992).

83. *Id.*

action of the defendant";[84] and (3) "it [is] 'likely,' as opposed to merely 'speculative,' that the injury will be 'redressed by a favorable decision.'"[85]

Appellate courts are split regarding Article III standing in the event of a data breach when the plaintiff has not proven misuse of their information and thus the threat of harm is considered too speculative.[86] When a laptop that contains unencrypted PHI is stolen, a patient may have a claim against the breacher for the threat of future harm (of identity theft).[87] While the threat of future harm of identity theft is insufficient to confer Article III standing in the First, Fourth, and Fifth Circuits, it is sufficient in the Third, Sixth, Seventh, and Ninth Circuits.[88] A resolution to this split in favor of conferring standing could potentially incentivize encryption in a way that the existing laws and regulations have failed to do.

III. ANALYSIS

With the ever-present need for mobile technology in healthcare, breaches are common and hard to predict. Liability for laptop theft is wholly preventable for hospitals and is a constant hot topic for courts. Given the severity of medical identity theft, as recognized by the creation of regulations to prevent it, hospitals' best means of insulating themselves from liability and protecting their patients is to prevent access to PHI by encrypting such devices. The following sections will analyze potential avenues for change that may motivate health systems to recognize and react to these problems.

A. PHI Breach Regulations and What They Do Now

Recent audits have shown that HIPAA violations as a result of laptop thefts settle in the range of millions.[89] Many instances of stolen laptops leading to identity theft are from employees leaving the hospital premises with an unencrypted laptop containing PHI.[90] While many hospitals have policies about encrypting PHI, laptops are still a source of liability.[91] Some systems also "beef up [their] digital security" as a response to laptop theft.[92] Hospitals often face class actions

84. *Id.* (internal quotation omitted).

85. *Id.* at 561.

86. *See* discussion *infra* Section III.C.

87. *See, e.g.*, In re Horizon Healthcare Servs. Inc. Data Breach Litig., 846 F.3d 625, 639 (3d Cir. 2017).

88. *See* DaimlerChrysler Corp. v. Cuno, 547 U.S. 332, 340–41 (2006) (explaining why the Supreme Court infers that Article III's case and controversy requirement requires standing limitations and stating that "if a dispute is not a proper case or controversy, the courts have no business deciding it").

89. *See* Bushee & Kottkamp, *supra* note 17.

90. Jacqueline Klosek, *Exploring the Barriers to the More Widespread Adoption of Electronic Health Records*, 25 ND J. L. ETHICS & PUB. POL'Y 429, 436 (2012).

91. *See, e.g.*, *BARNES-JEWISH HOSPITAL*: Faces Class Action Over Stolen Laptop, 13-132 CLASS ACTION REPORTER (July 6, 2011) [hereinafter *BARNES-JEWISH*], http://bankrupt.com/CAR_Public/110706.mbx. For a rundown on recent laptop theft liability, see *Summary Table*, *supra* note 18.

92. Jeff Overly, *HIPAA Fine Follows Stolen Laptop At Mass. Hospital*, L. 360 (Nov. 25, 2015, 3:32 PM), https://www.law360.com/articles/731620/hipaa-fine-follows-stolen-laptop-at-mass-hospital.

despite strict encryption policies.[93] They also receive orders from OCR for mandated corrective actions.[94] OCR has recently increased their emphasis on investigating smaller breaches.[95] Lack of evidence of identity theft does not always shield hospitals from liability nor dissuade settlement action.[96] Even when no evidence of personal identity theft is found, steps must be taken to ensure that the potentially affected patients are aware of the risk.[97]

The 2003 Security Rule established baseline security requirements for covered entities to follow, anticipating the sharing and storage of electronic information on portable devices as discussed in this Note.[98] Prior to its promulgation, there were no security standards that were generally accepted or followed by healthcare entities.[99] "A major goal of the Security Rule is to protect the privacy of individuals' health information while allowing covered entities to adopt new technologies to improve the quality and efficiency of patient care."[100] This regulation was created with an understanding of the underlying conflict discussed by this Note—the pull between information protection and efficiency of care. Importantly however, the Federal Register publication on the Security Rule makes no mention of encryption, nor portable devices directly.[101] The only mention is of photocopiers:

> Although such devices are not generally relied upon for storage and access to stored information, covered entities and business associates should be aware of the capabilities of these devices to store protected health information and must ensure any protected health information stored on such devices is appropriately protected and secured from inappropriate access, such as by monitoring or restricting physical access to a photocopier or a fax machine that is used for copying or sending protected health information.[102]

The Enforcement Rule, as a matter of administrative simplification, granted HHS the authority to impose civil penalties for HIPAA violations, and OCR the

93. *See, e.g.*, *BARNES-JEWISH*, *supra* note 91.

94. John Kennedy, *$3.9M HIPAA Deal Follows Research Institute's Lapses*, L. 360 (Mar. 17, 2016, 9:45 PM), https://www.law360.com/articles/773158/-3-9m-hipaa-deal-follows-research-institute-s-lapses.

95. Helen Pfister & Michelle Gabriel McGovern, *Data Security in Health Care: HIPAA Enforcement Trends*, N.Y. L.J., July 14, 2014.

96. Allison Grande, *SC Hospital Reveals Stolen Laptop Contained Patient Info*, L. 360 (July 28, 2014, 6:30 PM), https://www.law360.com/articles/561656/sc-hospital-reveals-stolen-laptop-contained-patient-info; *see also* Kennedy, *supra* note 94.

97. *See HIPAA Summary*, *supra* note 49.

98. *Id.*

99. *Id.*

100. *Id.*

101. Other Modifications to the HIPAA Rules, 78 Fed. Reg. 5566 (Jan. 25, 2013) (codified at 45 C.F.R. pts. 160 and 164).

102. *Id.*

authority to impose criminal penalties.[103] It was a response to widespread non-compliance by healthcare entities with the 2003 Security Rule.[104] Under this rule, covered entities are allowed to "submit, within 30 days of receipt of [notification by HHS], written evidence of any mitigating factors or affirmative defenses."[105] The rule also allows the Secretary of HHS to conduct compliance reviews of covered entities, and includes responsibilities for covered entities regarding such reviews, namely "providing records and compliance reports to the Secretary and cooperating during a compliance review or complaint investigation."[106]

The Breach Notification Rule and the Health Information Technology for Economic and Clinical Health Act of 2009 ("HITECH") were created as a response to health entities transitioning to electronic health records as opposed to paper. It requires that covered entities notify local prominent media and the Secretary of HHS in the event that a breach involves more than 500 individuals.[107] It also requires that the Secretary post a list of all entities that suffer such a breach online.[108] This rule also supplemented the Security Rule by determining what constituted "unsecured protected health information," simply that PHI that is not protected according to HHS guidance.[109] This presumed to heavily incentivize data encryption, but stated that "a covered entity may be in compliance with the Security Rule even if it reasonably decides not to encrypt electronic protected health information and instead uses a comparable method to safeguard the information."[110] The guidance for rendering PHI unusable was published by HHS later that year.[111] It explained that data should be either encrypted or destroyed according to the National Institute of Standards and Technology specifications.[112] In specifically responding to concerns about whether these new regulations imposed encryption responsibilities on healthcare entities, HHS stated that:

103. HIPAA Administrative Simplification: Enforcement, 71 Fed. Reg. 8390 (Feb. 16, 2006) (codified at 45 C.F.R. pts. 160 and 164).

104. For more information, see *Summary of HIPAA Security Rule*, U.S. DEP'T OF HEALTH & HUMAN SERVS., https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html (last visited May 21, 2019).

105. 45 C.F.R. § 160.312 (2018).

106. 45 C.F.R. § 160.310 (2018).

107. Breach Notification for Unsecured Protected Health Information, 74 Fed. Reg. 42,740 (Aug. 24, 2009) (codified at 45 C.F.R. pts. 160 and 164).

108. *Id.*

109. *Id.* (The act defines unsecured PHI as "protected health information that is not secured through the use of a technology or methodology specified by the Secretary in guidance, and provides that the guidance specify the technologies and methodologies that render protected health information unusable, unreadable, or indecipherable to unauthorized individuals.").

110. *Id.*

111. *Security Guide Guidance Material*, U.S. DEP'T OF HEALTH & HUM. SERVS., https://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html (last visited May 11, 2019).

112. Guidance Specifying the Technologies and Methodologies That Render Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals for Purposes of the Breach Notification Requirements Under Section 13402 of Title XIII (Health Information Technology for Economic and Clinical Health Act) of the American Recovery and Reinvestment Act of 2009. Request for Information, 74 Fed. Reg. 19,006 (Apr. 27, 2009) (to be codified at 45 C.F.R. pts. 160 and 164).

> Under [the new regulations], a covered entity must consider implementing encryption as a method for safeguarding electronic protected health information; however, because these are addressable implementation specifications, a covered entity may be in compliance with the Security Rule even if it reasonably decides not to encrypt electronic protected health information and instead uses a comparable method to safeguard the information.[113]

The Omnibus Rule, issued in 2013, filled gaps in the HIPAA and HITECH regulations.[114] Major provisions of this rule amended the process by which a HIPAA breach is determined.[115] This effectively replaced the old "risk of harm" standard—which directed hospitals to determine whether the severity of the risk of harm from disclosure would constitute a breach. The new standard is that the impermissible use or disclosure of PHI is presumed to be a breach unless the Covered Entity or Business Associate demonstrates that there is a low probability that the PHI has been comprised.[116] The rule included factors to consider in performing a risk assessment:

> (1) the nature and extent of the Protected Health Information involved, including the types of identifiers and the likelihood of re-identification; (2) the unauthorized person who used the Protected Health Information or to whom the Protected Health Information was disclosed; (3) whether the Protected Health Information was actually acquired or viewed; and (4) the extent to which the risk to the Protected Health Information has been mitigated.[117]

In the Federal Register publication on this regulation, HHS stated that "covered entities and business associates are beginning to recognize areas of potential weakness and to take systemic actions to prevent breaches from occurring in the future, such as encrypting portable devices to avoid having to provide breach notifications in the event the device is lost or stolen[,]" but did not elect to suggest mandatory encryption.[118]

While multiple laptop thefts are reported to the OCR each month, most do not result in payouts.[119] This may explain why many healthcare entities decide not to encrypt, assuming that they will not be affected by the few breaches that do surface. Recently, however, the OCR has stepped up their enforcement protocols of HIPAA violations through audits.[120] In 2005, 200,000 patients were affected by stolen technology, and many who seek to steal identities target health

113. Breach Notification for Unsecured Protected Health Information, 74 Fed. Reg. 42,740 (Aug. 24, 2009) (codified at 45 C.F.R. pts. 160 and 164).

114. HIPAA Administrative Simplification: Enforcement, 71 Fed. Reg. 8390 (Feb. 16, 2006) (codified at 45 C.F.R. pts. 160 and 164).

115. 45 C.F.R. § 164.402 (2018).

116. *Id.*

117. *Id.*

118. Other Modifications to the HIPAA Rules, 78 Fed. Reg. 5566 (Jan. 25, 2013) (codified at 45 C.F.R. pts. 160 and 164).

119. *See, e.g.*, Grande, *supra* note 96.

120. Bushee & Kottkamp, *supra* note 17.

systems due to this vulnerability.[121] As these numbers rise,[122] the OCR is mandating corrective action plans.[123] These plans include developing encryption reports on all devices, policy review regarding device access and control, enhancement of training protocols, enterprise-wide risk analyses, and internal investigations of possible noncompliance.[124] These plans place further burdens on health systems because they come in addition to potential payment for liability for patient harm in realized breaches. The next logical step is to mandate encryption. This change could shift providers' perspectives from risking corrective actions plans and penalties to proactively preventing HIPAA violations—a shift that is desperately needed in an industry that consistently makes vulnerable our population's most sensitive data.

B. Legislative Failings in Privacy Protections

The United States' Congress, if asked whether laptop theft leading to identity theft was their problem to address, would likely respond with a resounding, "No." Early delegation of such regulation puts it out of the minds of legislators on the federal level. Recognizing the shortcomings of our current framework, states have drawn up their own laws in a disjunctive and uncoordinated manner.

1. Might the GDPR of the European Union Inspire a Second Wave?

In 1996, Congress passed HIPAA to delegate regulatory authority of medical information privacy and protection to HHS in hopes, as is always the case in administrative law, that the agency's expertise in the industry will inform their judgment as to how regulation and enforcement should be constructed.[125] This, to many, marked the end of Congress' interest in having any major impact on data privacy as it pertained to medical information and was part of a mass delegation to agencies like HHS and the FTC that resulted in a fracturing of privacy protections and enforcement. By contrast, the European Union has enacted an extremely pro-consumer law, the GDPR, on the basis that "[e]ffective protection of personal data . . . requires strengthening and detailing the rights of data subjects [in] monitoring and ensuring compliance with the rules for the protection of personal data."[126] Impressively, the GDPR allows for a private right of action—something that our Congress, courts, and administrative bodies refuse to allow:

121. *See* Helliker, *supra* note 16.

122. *See Summary Table*, *supra* note 18.

123. *Id.*

124. *Id.*

125. The Health Insurance Portability and Accountability Act of 1996, Pub. L. 104-191, 110 Stat. 1936 (1996).

126. Position of the European Parliament adopted at first reading on 12 March 2014 with a view to the adoption of Regulation (EU) No .../2014 of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), P7_TC1-COD(2012)0011.

> Data subjects should have the right to . . . an effective judicial remedy . . . if they consider that their rights under this Regulation are infringed or where the supervisory authority does not react on a complaint or does not act where such action is necessary to protect the rights of the data subject.[127]

Of note is that this right is broad enough to encompass any violation of the GDPR, and that no injury requirement is explicitly read into it.[128]

There is no question that a more powerful and consistent form of data privacy would work wonders. This was last recognized by the Obama administration in 2012 when it offered up the Consumer Privacy Bill of Rights.[129] This bill aimed to give power back to consumers in a way that the GDPR has achieved.[130] Former United States Deputy Chief Technology Officer for Internet Policy Daniel J. Weitzner stated that "[t]he critical transition . . . was this focus on individual rights."[131] Unfortunately, Congress let this bill die slowly, but the GDPR, which aligns well with the above-stated sentiment, might inspire a second wave—one that finally puts control back into the hands of patients whose data is at risk, thus creating enough pressure from consumers to motivate hospitals to adequately protect their sensitive information.

2. *California is Leading the Way in State Law Consumer Protections*

As discussed briefly *supra*, states fill the void of congressional data privacy and protection with their own statutes, some of which recognize the need for individual private rights of action. Unfortunately, common to almost all of these is a required cognizable injury.[132] Some states are realizing the difficulty that this poses to victims of data theft. The California legislature, for example, is now considering SB 1121.[133] If enacted, the law would empower anyone whose personal information has been or is reasonably believed to have been breached to file a civil lawsuit against a business on whose watch the personal information was breached, whether the person suffered any actual harm or monetary loss.[134]

---

127. *Id.*

128. In fact, the term "injury" is nowhere to be found in the GDPR's Remedies, liability and penalties section. GDPR, *supra* note 63, art. 77–84. The right to judicial remedy is so powerful in the GDPR that it also allows for actions against supervisory authorities that do not effectively handle a complaint lodged by the data subject. *Id.* art. 78.

129. For a rundown on what was suggested, see Marcia Hofmann, *Obama Administration Unveils Promising Consumer Privacy Plan, but the Devil Will Be in the Details*, ELECTRONIC FRONTIER FOUNDATION (Feb. 23, 2012), https://www.eff.org/deeplinks/2012/02/obama-administration-unveils-promising-consumer-privacy-plan-devil-details.

130. *Id.*

131. Natasha Singer, *Why a Push for Online Privacy Is Bogged Down in Washington*, N.Y. TIMES (Feb. 28, 2016), https://www.nytimes.com/2016/02/29/technology/obamas-effort-on-consumer-privacy-falls-short-critics-say.html.

132. *See, e.g.*, Shafran v. Harley-Davidson, Inc., No. 07 CIV. 01365 (GBD), 2008 WL 763177, at *2–3 (S.D.N.Y. Mar. 20, 2008).

133. California Consumer Privacy Act of 2018, Senate Bill No. 1121 (2018).

134. *Id.* Since the writing of this piece, SB 1121 has been passed by the California legislature and is in full effect. Alexandra Scott, *California Legislature Passes Amendments to Expansive Consumer Privacy Law*, INSIDE

This is a step in the right direction for state legislatures. While the U.S. Congress drags its feet, at least states are forging a trend toward consumer protection by way of granting private rights of action.

C. When Laptop Theft Goes to Court, Article III Standing has Courts Divided

In the current U.S. position on data breach laws: regulations are mostly ineffective and wholly retrospective, legislatures are either indifferent toward or slow to enact change. Courts, however, are affecting change. As stated *supra*, private rights of action are sometimes available in cases involving data breaches, but injury requirements are stringent.[135] There is some confusion as to whether an affected patient has standing to sue the breaching party. Recognizing that victims of data breaches suffer from hard-to-define injuries, like time spent with law enforcement and banking representatives, deactivation of cards, monthly charges for credit monitoring, etc., some courts are loosening threshold injury inquiries. As a result, the most commonly alleged injury in data breach actions, an increased risk of future harm, is garnering success.[136] Considerable focus will be given to this subject in the following sections due to its immediate potential impact in remedying the problem of nonencryption.

1. Article III Standing Generally and Shifting Supreme Court Standards

For a federal court to have jurisdiction over a claim, at least one plaintiff must prove it has standing for each form of relief sought.[137] The Supreme Court has established a three-part test for constitutional Article III standing in the event of a data breach:[138] (1) that he or she has suffered an "injury in fact" that is (a) "concrete and particularized"[139] and (b) "actual or imminent" (not conjectural or hypothetical);[140] (2) "there [is] a causal connection between the injury and the conduct complained of—the injury has to be fairly . . . traceable to the challenged action of the defendant";[141] and (3) "it [is] 'likely,' as opposed to merely 'speculative,' that the injury will be 'redressed by a favorable decision.'"[142] If a plaintiff proves these elements, Article III standing is conferred.

The Supreme Court has used conflicting tests concerning potential future injuries and their imminence in constituting an injury for Article III standing.[143]

PRIVACY (Sep. 4, 2018), https://www.insideprivacy.com/united-states/state-legislatures/california-legislature-passes-amendments-to-expansive-consumer-privacy-law/.

135. *See* discussion *supra* Section II.D.

136. For an explanation of how courts are allowing such claims, see discussion *infra* Section III.C.2.

137. *See* DaimlerChrysler v. Cuno, 547 U.S. 332, 352 (2006) ("[A] plaintiff must demonstrate standing separately for each form of relief sought") (quoting Friends of the Earth, Inc. v. Laidlaw Environmental Services, Inc., 528 U.S. 167, 185 (2000)).

138. *Id.* at 342.

139. Lujan v. Defenders of Wildlife, 504 U.S. 555, 555 (1992).

140. *Id.*

141. *Id.* at 560 (internal quotation omitted).

142. *Id.* at 561.

143. Kowalsi v. Tesmer, 543 U.S. 125, 130 (2004).

In 2013, in *Clapper v. Amnesty International USA*, plaintiffs brought suit against James Clapper, the Director of National Intelligence, challenging the Foreign Intelligence Surveillance Act amendments of 2008, which empowered the Foreign Intelligence Surveillance Court to authorize surveillance of an individual without showing probable cause that the individual is an agent of a foreign power.[144] Plaintiffs alleged "that they are suffering ongoing injuries that are fairly traceable to [the amendment] because the risk of surveillance under [the amendment] requires them to take costly and burdensome measures to protect the confidentiality of their communications."[145] In analyzing the "fairly traceable" standing element, the Supreme Court rejected the lower court's "relaxed reasonableness standard"[146] and instead established a "certainly impending" standard.[147] A cursory review of *Clapper* does not make it clear whether this standard applies to data breach cases or other factual scenarios devoid of questions concerning separation of powers and political-question-doctrine, which are at issue in *Clapper*.[148] In the same case, in response to Justice Breyer's dissent from the opinion, a footnote addressed a "substantial risk" standard,[149] a less strict alternative standard for the "fairly traceable" element.[150]

A year after *Clapper*, in 2014, the Supreme Court in *Susan B. Anthony List v. Driehaus* referred to both the "substantial risk" standard and the "certainly impending" standard,[151] but relied on the "substantial risk" standard.[152] In a 2010 election, a pro-life organization Susan B. Anthony List ("SBA") accused Congressman Steve Driehaus, who was running for re-election to Congress, of supporting a healthcare bill that used taxes to support abortion services.[153] In retort, Driehaus filed a claim with the Ohio Elections Commission alleging a violation of the false-statement statute.[154] The Commission found that the statute had been violated in a two to one vote.[155] After unsuccessfully seeking injunctive relief in federal court,[156] SBA filed suit in federal court challenging the constitutionality of the false-statement statute on First Amendment grounds.[157] SBA's main contention was that its

> speech about Driehaus had been chilled; that SBA intend[ed] to engage in substantially similar activity in the future; and that it faced the prospect of

144. *See generally* Clapper v. Amnesty Int'l USA, 568 U.S. 398, 401 (2013).
145. *Id.* at 415.
146. *Id.*
147. *Id.* at 401.
148. *Id. See* Bradford C. Mank, *Data Breaches, Identity Theft, and Article III Standing: Will the Supreme Court Resolve the Split in Circuits?*, 92 NOTRE DAME L. REV. 1323, 1332 (2017).
149. *Clapper*, 568 U.S. at 414 n.5.
150. For a brief overview of different standards, see *Federal Practice Manual for Legal Aid Attorneys*, SHRIVER CENTER, http://www.federalpracticemanual.org/chapter3/section1 (last visited May 21, 2019).
151. Susan B. Anthony List v. Driehaus, 573 U.S. 149, 158 (2014).
152. *Id.*
153. *Id.* at 153–54.
154. *Id.* at 154.
155. *Id.*
156. *Id.* at 155.
157. *Id.* at 154.

> its speech and associational rights again being chilled and burdened, because any complainant can hale it before the Commission, forcing it to expend time and resources defending itself.[158]

The Supreme Court granted certiorari and discussed what standard is applicable to these facts. While it cited both the "certainly impending" and "substantial risk" standards both referred to in *Clapper*, the decision relied on the "substantial risk" standard, and concluded that "the threat of future enforcement of the false statement statute [was] substantial."[159] The court reasoned that SBA had standing under the Article III injury requirement because they alleged "a credible threat of enforcement"[160] in that their intention to make future accusations is hindered by the threat of future enforcement "because the burden of facing a hearing may chill free speech even if there is no conviction."[161]

The importance of the decision in *Driehaus* is that the Supreme Court moved away from the strict "certainly impending" standard in *Clapper* and toward a more lenient "substantial risk" standard when adjudicating over matters involving the threat of future harm under an Article III standing analysis.[162] This is the existing standard for the "fairly traceable" prong of the standing test.

Relevant to the first prong of the standing test, regarding the injury in fact, subsequent "circuit court decisions issued in data breach litigation cases . . . arguably weakened the 'actual or imminent' injury prong of standing, taking a broader view of what is 'imminent' than many federal courts had previously accepted in the data breach context."[163]

In 2016, the Supreme Court discussed the injury requirement of Article III standing further in *Spokeo, Inc. v. Robins*.[164] The case concerned the Fair Credit Reporting Act ("FCRA"), which "requires consumer reporting agencies to 'follow reasonable procedures to assure maximum possible accuracy of' consumer reports."[165] Spokeo, a consumer reporting agency that "operates a people search engine, which searches a wide spectrum of databases to gather and provide personal information about individuals to a variety of users, including employers wanting to evaluate prospective employees,"[166] was sued for violating the FCRA when Thomas Robins discovered that his Spokeo profile contained inaccurate information.[167] The Ninth Circuit lower court concluded "that Spokeo violated *his* statutory rights and . . .that Robins' personal interests in the handling of his credit information are *individualized*"[168] sufficient to adequately allege an injury

158. *Id.* at 155 (internal quotations omitted).
159. *Id.* at 164.
160. *Id.* at 167.
161. Mank, *supra* note 148, at 1335.
162. *See generally* Susan B. Anthony List v. Driehaus, 573 U.S. 149 (2014).
163. Cinthia Granados Motley & Laurie A. Kamaiko, *Spokeo's Impact On Data Breach Litigation*, L. 360 (June 16, 2016, 4:21 PM), https://www.law360.com/articles/807990/spokeo-s-impact-on-data-breach-litigation.
164. Spokeo, Inc. v. Robins, 136 S. Ct. 1540 (2016).
165. *Id.* at 1542–43 (citing 15 U.S.C. § 1681e(b)).
166. *Id.* at 1543 (quotations omitted).
167. *Id.*
168. *Id.* (emphasis added) (quotations omitted).

in fact for standing. The Supreme Court held that the Ninth Circuit's analysis was incomplete, because it focused only on the "particularized" element, and not the "concrete" element, of the injury in fact requirement.[169] "A 'concrete' injury must be '*de facto*'; that is, it must actually exist."[170] However, "'[c]oncrete' is not . . .necessarily synonymous with 'tangible.' Although tangible injuries are perhaps easier to recognize, [the Supreme Court has] confirmed in many . . . previous cases that intangible injuries can nevertheless be concrete."[171] Importantly, the court in *Spokeo* explains that "[i]n determining whether an intangible harm constitutes injury in fact, both history and the judgment of Congress play important roles."[172] The *Spokeo* court defined two general principles in its conclusion: (1) that when Congress "plainly [seeks] to curb [a particular violation] by adopting procedures designed to decrease that risk,"[173] it can elevate the concreteness of an injury despite being previously inadequate in law; (2) that a plaintiff "cannot satisfy the demands of Article III by alleging a bare procedural violation."[174] In applying these general principles to the case at bar, the Supreme Court found that Robins did not have standing because "[a] violation of one of the FCRA's procedural requirements may result in no harm," and "not all inaccuracies [in posted information] cause harm or present any material risk of harm."[175] In applying these general principles to data breach litigation, one reading of this may suggest that a court should "look for factual allegations supporting intended misuse, such as the nature of the information taken . . . that indicate a purpose of extracting personal data for identity fraud."[176] Another reading may suggest that any material risk of harm, so long as it goes beyond a bare procedural violation, and especially when supplemented by Congressional intent to avoid such a risk, is sufficient to allege an injury in fact. Circuits are split over whether the threat of future harm in data breach litigation, which lies at the root of laptop theft and HIPAA violation matters, can suffice for Article III standing.

2. *How the Courts are Divided over Speculative Harm in Data Breach Cases*

When a laptop is stolen which contains unencrypted PHI, a patient may have a claim against the breacher for the threat of future harm of identity theft.[177] Appellate courts are split regarding Article III standing in the event of a data breach when the plaintiff has not proven misuse of their information and thus the

169. *Id.*
170. *Id.* at 1548.
171. *Id.* at 1549.
172. *Id.*
173. *Id.* at 1550.
174. *Id.*
175. *Id.*
176. Granados Motley & Kamaiko, *supra* note 163.
177. While this Note outlines the potential legal framework for allowing such a claim, note that general HIPAA regulation does not in itself allow for a private right of action.

threat of harm is considered to be too speculative.[178] While the threat of future harm of identity theft is insufficient to confer Article III standing in the First, Fourth, and Fifth Circuits, it is sufficient in the Third, Sixth, Seventh, and Ninth Circuits.[179]

Before *Clapper*, the threat of future harm was sufficient to confer standing in the Seventh Circuit.[180] In *Pisciotta v. Old National Bancorp*, Old National Bancorp ("ONB") was a bank whose marketing website, on which individuals who sought banking services could provide personal and financial information for an online application, suffered a security breach.[181] While citing district court opinions that refused to confer Article III standing in data breach cases in a footnote,[182] the court in *Pisciotta* noted that, "[a]s many [other] circuits have noted, the injury-in-fact requirement can be satisfied by a threat of future harm or by an act which harms the plaintiff only by increasing the risk of future harm that the plaintiff would have otherwise faced, absent the defendant's actions."[183] This implies that, in the Seventh Circuit, standing in data breach cases could be conferred simply by showing that the defendant's actions, by even a slim probability, could cause a future harm.

This was true in the Ninth Circuit as it applied to a stolen laptop.[184] In *Krottner v. Starbucks Corp.*, an unencrypted Starbucks company laptop, which contained private information of former employees, was stolen from a Starbucks location.[185] The laptop contained the information of approximately 97,000 individuals.[186] After Starbucks sent a breach notification letter and offered credit monitoring services to past employees of Starbucks, plaintiffs filed a class action lawsuit against Starbucks on negligence and breach of contract claims.[187] While the underlying claims failed in the appellate court, the question of standing was discussed as a separate issue.[188] The court in *Krottner* relied on the same cases as did the Seventh Circuit in *Pisciotta*, and reasoned that, "[b]ecause the plaintiffs had alleged an act that increased their risk of future harm, they had alleged an injury-in-fact sufficient to confer standing."[189] Notably, the court disagreed with the Sixth Circuit in *Lambert v. Hartman*, which concluded that the risk of future identity theft is "somewhat 'hypothetical' and 'conjectural,'"[190] and stated that the plaintiffs alleged "a credible threat of real and immediate harm stemming

178. Kristen L. Burge, *Your Data Was Stolen, But Not Your Identity (Yet)*, ABA (Jan. 11, 2018), https://www.americanbar.org/groups/litigation/publications/litigation-news/featured-articles/2018/your-data-was-stolen-not-your-identity-yet/.

179. *Id.*

180. *See, e.g.*, Pisciotta v. Old Nat'l Bancorp, 499 F.3d 629, 634 (7th Cir. 2007).

181. *Id.* at 631.

182. *Id.* at 634 n.2.

183. *Id.* at 634.

184. Krottner v. Starbucks Corp., 628 F.3d 1139, 1143 (9th Cir. 2010).

185. *Id.* at 1140.

186. *Id.*

187. *Id.* at 1140–41.

188. *Id.* at 1141.

189. *Id.* at 1143.

190. *Id.* (citing Lambert v. Hartman, 517 F.3d 433, 437 (6th Cir.2008)).

from the theft of a laptop containing their unencrypted personal data."[191] The court further explained that, "[w]ere [the] allegations more conjectural or hypothetical—for example, if no laptop had been stolen, and Plaintiffs had sued based on the risk that it would be stolen at some point in the future—we would find the threat far less credible."[192]

A year later, the Third Circuit denied standing for the threat of future harm in a data breach case.[193] In *Reilly v. Ceridian*, two law firm employees brought a lawsuit against Ceridian Corporation, a payroll processing company, after their computer system was hacked.[194] The hacker gained access to "personal and financial information belonging to Appellants and approximately 27,000 employees at 1,900 companies."[195] In reviewing the district court's dismissal for lack of standing, the Third Circuit concluded that allegations of threat of future harm were too hypothetical because the chain of causation was too long to satisfy the "certainly impending" standard.[196] The court reasoned that unless "the hacker: (1) read, copied, and understood their personal information; (2) intend[ed] to commit future criminal acts by misusing the information; and (3) [was] able to use such information to the detriment of Appellants by making unauthorized transactions in Appellants' names," no injury would be recognized as certainly impending.[197] Of note, the *Reilly* court distinguished *Pisciotta* and *Krottner*, asserting that those data breaches suggested more certain future harm.[198] *Pisciotta* was rightfully set aside because it involved "sophisticated, intentional and malicious" hackers.[199] *Krottner*, the laptop theft case, was unjustifiably distinguished merely because "someone attempted to open a bank account with a plaintiff's information following the physical theft of the laptop."[200] The court in *Krottner* did not use this fact to evaluate whether the threat of future harm satisfied the injury in fact requirement, it merely stated that the fact of a stolen laptop makes the threat more than hypothetical.[201]

Prior to *Clapper*, courts were split on whether the threat of future harm was sufficient to establish the injury-in-fact requirement of Article III standing in data breach cases, but the only major case related specifically to laptop theft suggested that some reasonable analysis could find that standing should be conferred.[202]

In the wake of *Clapper*, in 2015, the Seventh Circuit ruled in a case concerning a data breach at Neiman Marcus, a department store, involving the credit card numbers of its customers.[203] Remijas, a customer of the store, had made

191. *Id.*
192. *Id.*
193. Reilly v. Ceridian, 664 F.3d 38, 46 (3rd Cir. 2011).
194. *Id.* at 40.
195. *Id.*
196. *Id.* at 42.
197. *Id.*
198. *Id.* at 44.
199. *Id.* (quoting Pisciotta v. Old Nat'l Bancorp, 499 F.3d 629, 632 (7th Cir. 2007)).
200. *Id.* (quoting Krottner v. Starbucks Corp., 628 F.3d 1139, 1142 (9th Cir. 2010)).
201. *Krottner*, 628 F.3d at 1143.
202. *Id.*
203. Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688, 689 (7th Cir. 2015).

purchases at the time of the cyberattack.[204] In discussing whether the threat of future harm was sufficient in the fact at bar to satisfy the injury in fact requirement, the court posed a rhetorical question: "Why else would hackers break into a store's database and steal consumers' private information? Presumably, the purpose of the hack is, sooner or later, to make fraudulent charges or assume those consumers' identities."[205] Thus, under the Seventh Circuit's analysis, speculative harm can be made more concrete or certainly impending if the underlying breach involved some form of intent. The court also noted that "[r]equiring the plaintiffs to wait for the threatened harm to materialize in order to sue would create a . . . problem: the more time that passes between a data breach and an instance of identity theft, the more latitude a defendant has to argue that the identity theft is not fairly traceable to the defendant's data breach."[206] This reasoning gives greater value to the importance of allowing standing in cases alleging the threat of future harm.

The intent distinction travelled beyond the Seventh Circuit and persisted through subsequent Supreme Court opinions. Two years later, in 2016 and after *Spokeo*, the Sixth Circuit conferred standing without evidence of data misuse.[207] In *Galaria v. Nationwide Mutual Insurance Company*, plaintiffs sued Nationwide Insurance following a breach in their security.[208] Nationwide Insurance's computers held records containing private information of 1.1 million individuals.[209] In their complaint, the plaintiffs cited a "study purporting to show that in 2011 recipients of data-breach notifications were 9.6 times more likely to experience identity fraud, and had a fraud incidence rate of 19%."[210] In discussing whether the threat of future injury is sufficient to satisfy the injury in fact requirement, the court reasoned that "[t]here is no need for speculation where Plaintiffs allege that their data has already been stolen and is now in the hands of ill-intentioned criminals."[211] While it might be suggested that this line of reasoning is unique to hacking incidents, which are more sophisticated than are simple laptop thefts, the Sixth Circuit cited the *Krottner* decision as support for its finding.[212] The court also distinguished *Reilly* by highlighting the need for intent to suggest a threat of future harm.[213] While *Krottner* and other cases that granted standing showed evidence of intended theft of information, or a device that held such information, in *Reilly* "all that is known is that a firewall was penetrated."[214]

204. *Id.* at 691.
205. *Id.* at 693.
206. *Id.* (internal quotations omitted) (citing In re Adobe Sys., Inc. Privacy Litig., 66 F.Supp. 3d 1197, 1215 n.5 (N.D. Cal. 2014)).
207. Galaria v. Nationwide Mut. Ins. Co., 663 Fed. Appx. 384, 385–86 (6th Cir. 2016).
208. *Id.* at 386.
209. *Id.*
210. *Id.*
211. *Id.* at 388.
212. *Id.* at 389.
213. *Id.*
214. *Id.* (quoting Reilly v. Ceridian Corp., 664 F.3d 38, 44 (3rd Cir. 2011)).

For the purpose of laptop theft, which is in most instances intentional (or so it was considered in the *Galaria* opinion), *Reilly* seems to hold much less weight.

The following year, the Fourth Circuit declined to follow *Remijas*, determining that the threat of future harm was too speculative and thus insufficient to satisfy the injury requirement in Article III standing.[215] In *Beck v. McDonald*, a laptop was stolen from the William Jennings Bryan Dorn Veterans Affairs Medical Center ("Dorm VAMC"), which contained unencrypted personal information of approximately 7,400 individuals.[216] Plaintiff Beck filed a putative class action suit against McDonald, the Secretary of Veteran Affairs for violation of the Privacy Act, alleging that the breach caused "embarrassment, inconvenience, unfairness, mental distress, and the threat of current and future substantial harm from identity theft and other misuse of their Personal Information."[217] In dismissing for lack of standing, after first dismissing the possibility of satisfying the "certainly impending" standard with little analysis, the court relied on the district court's reasoning that "[t]he plaintiffs' calculations that 33% of those affected by the laptop theft would have their identities stolen and that all affected would be 9.5 times more likely to experience identity theft [would] not suffice to show a substantial risk of identity theft."[218] This is a dramatic dissent from the Seventh Circuit's reasoning in *Pisciotta*, that simply increasing the risk of future harm that the plaintiff would have otherwise faced, absent the defendant's actions, would be sufficient. Here, a substantial increase in likelihood of identity theft (a 9.5 multiplicative increase) was deemed to be insufficient.[219] Instead, the court distinguished cases in which "the data thief intentionally targeted the personal information,"[220] and the matter at bar, in which the plaintiff showed "no evidence that the information contained on the stolen laptop has been accessed or misused or that they have suffered identity theft, nor, for that matter, that the thief stole the laptop with the intent to steal their private information."[221] This highlights a major split in inferential reasoning dividing this analysis among the federal circuits. While the Ninth Circuit will infer the sort of intent that gives rise to an injury in fact in a laptop theft as in *Krottner*, and other courts will also infer intent in data breach cases citing the *Krottner* opinion, the Fourth circuit in *Beck* refuses to make such an "attenuated" inferential chain.[222] In modern courts, this divergence arises out of mixed readings of *Spokeo*, in determining whether it requires "factual allegations supporting intended misuse, such as the nature of the information taken . . . that indicate a purpose of extracting personal data for

215. *See generally* Beck v. McDonald, 848 F.3d 262 (4th Cir. 2017).
216. *Id.* at 267.
217. *Id.*
218. *Id.* at 268 (internal quotations omitted).
219. *Id.*
220. *See id.* at 274.
221. *See generally id.*
222. *See id.* at 275 (using the "attenuated chain" language to refer to that same phrase in the *Clapper* opinion).

identity fraud,"[223] or simply any material risk of harm, so long as it goes beyond a bare procedural violation, to properly allege an injury in fact.

The Third Circuit's reading of *Spokeo* differs from that of the Fourth Circuit's in *Beck*. In *In re Horizon Healthcare Services Inc. Data Breach Litigation*, two laptops containing unencrypted PHI of approximately 839,000 individuals were stolen from Horizon Healthcare Services, Inc., a health insurance provider.[224] Affected patients filed suit on grounds of willful and negligent violation of the Fair Credit Reporting Act ("FCRA").[225] The court reasoned, following their reading of *Spokeo*, that, because the plaintiffs allege "the unauthorized dissemination of their own private information—the very injury that FCRA is intended to prevent"[226] there is an injury in fact, and thus Article III standing should be conferred.[227] The question remains whether breach laws can be analogized to the FCRA by courts to the same end—might the unwanted use or disclosure of patient PHI be seen by courts as a de facto injury because that is the sort of injury that these laws are intended to prevent?

It seems that, under these new circuit court cases, the mere threat of future harm of identity theft is insufficient to confer Article III standing in the First, Fourth, and Fifth Circuits, while the threat is sufficient in the Third, Sixth, Seventh, and Ninth Circuits. It is hard to determine whether future readings of *Spokeo* resolve this split favorably. *Beck* suggests that a simple laptop theft with no evidence of data misuse is insufficient to confer standing because an injury in fact cannot be established.[228] But *Horizon* suggests that at least FCRA violations are de facto injuries sufficient to establish standing, and leaves open the possibility of extension to breach laws aimed at preventing such acts.[229]

The Supreme Court can affect change in the healthcare industry to better protect patients from the threat of identity theft by resolving this split in favor of conferring standing for the threat of future identity theft in cases where misuse of data has not been proven, thereby motivating hospitals to encrypt their devices more regularly. This is a broad reading of *Spokeo*, but one that tracks with reasoning from several circuits in existing valid precedent. The current trend in *Spokeo* seems to suggest that the Court is interested in protecting hospitals from speculative claims in enforcing a higher standard when the plaintiff lacks evidence to justify the claimed threat. But *Horizon* may persuade the Court that, on policy grounds, *Spokeo* should be read to allow for a right of action in cases involving violations of state breach protection laws, which includes laptop theft.

223. Granados Motley & Kamaiko, *supra* note 163.
224. In re Horizon Healthcare Servs. Data Breach Litig., 846 F.3d 625, 630 (3d Cir. 2017).
225. *Id.* at 631.
226. *Id.* at 640.
227. *Id.* at 635.
228. *See supra* notes 215–23.
229. *See supra* notes 224–27.

IV. RECOMMENDATION

Laptop theft is increasingly common, and medical identity theft is on the rise as a result. The dangers posed by identity theft caused by medical information breach are enormous when considering the depth of information stored in medical files. As theft of this type persists, patients continue to be at risk. While the onus generally rests on the regulators to promulgate rules regarding information protection and enforcement services like the OCR to act on those rules, a recent rise in enforcement has yet to prove effective in motivating health systems to encrypt their devices. Were the legislature to enact a broad data privacy law like that of the EU, encryption might seem more necessary for health systems. The judiciary may also create an incentive by conferring Article III standing for claims that allege a threat of future harm when laptops are stolen. Some form of pressure must be put on healthcare entities to promote encryption, and to put an end to patient vulnerability.

A. HHS Should Mandate Portable Device Encryption for Covered Entities

While OCR's increased enforcement suggests to hospitals that they should encrypt their devices to protect their patients, mandating encryption guarantees positive change, and creates a means by which a violation can give rise to an injury in fact in the courts. To date, this sort of regulation hasn't been promulgated due to push-back from the medical industry, who cite the change as a potential financial burden.[230] It's clear that something has convinced hospitals that nonencryption is passable financially, despite clear information that suggests otherwise.[231]

The ideological foundation for mandatory encryption is in place. HHS has conceded, however, that the current framework is not financially motivational:

> Benefits to the HIPAA covered entity will rest with the actions it takes to prevent data breaches. As our analysis demonstrates, the costs of notification for an entity may be significant, although in the aggregate in terms of overall health care costs, they are extremely small. Nevertheless, we believe that the costs . . . are avoidable if either before a covered entity experiences a breach or following one, the entity adopts measures to strengthen its data security. As pointed out, the most frequent form of data loss is the result of lost or stolen laptops . . . . If the data on these devices is encrypted, then under the interim final rule definition of a breach, the event would not require the covered entity or the business associate to notify affected individuals.[232]

230. Mike Semel, *HIPAA doesn't require data encryption, but you should*, HITECH ANSWERS (Feb. 6, 2013), https://www.hitechanswers.net/hipaa-doesnt-require-data-encryption-but-you-should/.

231. *Id.*

232. Breach Notification for Unsecured Protected Health Information, 74 Fed. Reg. 42,740 (Aug. 24, 2009) (codified at 45 C.F.R. pts. 160 and 164).

The rationale for not mandating encryption already is to "permit[] the use of firewalls and access controls[, which are] reasonable and appropriate safeguards,"[233] but such safeguards are signaled as still inferior to encryption as they are not awarded the same safe harbor protection from breach notification: "a covered entity that seeks to ensure breach notification is not required in the event of a breach of the information in the database would need to encrypt the information pursuant to the guidance."[234] If regulators determine at a later date that such a benefit is insufficient to motive encryption, as it seems to be, they may resolve to mandate encryption.

B. Legislatures Should Put an End to Statutory Inconsistencies

While admittedly its most far-fetched plea, given the history of the U.S. Congress' role in data privacy, this Note advocates for a federally consistent data breach law that adequately protects consumers, in this case patients. Inspiration may best be sourced from the EU's GDPR—especially the inclusion of a private right of action to strengthen front-end regulation—but any added protection would be welcomed.

Given the unlikely nature of the above recommendation, in the alternative, states should aim to collaborate on a more consistent data breach law that would have the same effect. This Note advocates for a model similar to that of California's recent SB 1121, which provides a private right of action to consumers whose information was breached regardless of whether an injury is shown to have resulted (that is, an injury in the conventional sense of the term).[235] This would not only signal a trend toward patient protections, but also open the door for courts to impose their own pressure by way of the following recommendation.

C. The Supreme Court Should Resolve the Circuit Split by Conferring Standing in Data Breach Cases of This Kind

The judicial history surrounding Article III standing and data breaches is complex and difficult to decipher. Indeed, circuit courts are likely split due to mixed readings of the Supreme Court's most recent ruling in *Spokeo*. The very foundation of Article III standing is even ambiguous, citing two standards for injury in fact that vary widely in stringency, from "concrete and particularized" to "substantial risk."[236] The eventual resolution rests on a final determination of whether an injury in fact can be established in the absence of data misuse when the threat of future harm is simply increased by the fact and conditions of a theft, whether mere theft sufficiently suggests an intent to misuse the data within the

233. *Id.* at 42,742.
234. *Id.*
235. *See* California Consumer Privacy Act of 2018, Senate Bill No. 1121 (2018).
236. *See* discussion *supra* Section II.C.1.

stolen device, and whether Congressional intent in preventing statutory and regulatory violations can be extended to those state breach laws that currently protect patients. To better protect patients by putting pressure on health systems to encrypt their laptops and other portable devices, the Supreme Court should resolve that: an injury in fact can be established by any increase in the likelihood of threat of future harm, accompanied by a showing at least that identity theft is common in similar situations; the mere theft of a laptop suggests the misuse of the PHI contained within it, thus satisfying the "certainly impending" standard; that state breach laws were established to prevent the kind of unwanted disclosure of PHI at play in laptop thefts; and that violations of these statutes constitute a foundation for standing under the injury prong.

In *Beck,* the Fourth Circuit court read *Spokeo* to suggest that the threat of future harm of identity theft in cases involving stolen laptops is too speculative when there is no evidence of the misuse of that data.[237] While this standard might seem practical for the industry's protection, the goal of legal change should be to protect those made vulnerable by legal inconsistencies—here, the patient, whose sensitive information is up for grabs by anyone smart enough to break into a car in a hospital lot. Patients are left open to the threat of identity theft because hospitals are reluctant to implement change and encrypt their portable devices despite agency guidelines.[238] The judiciary can, and should, motivate positive change for the protection of the patient population by conferring Article III standing in data breach claims where misuse of data is absent.

In *Horizon*, the Third Circuit recognized the need for a public policy argument in the determination of Article III standing, specifically from the perspective of Congressional intent and what sorts of behaviors Congress intends to prevent with its laws.[239] This signals a positive step toward putting pressure on hospitals to encrypt their devices such that information cannot be inadvertently used or disclosed, the very behavior that state breach laws intend to prevent. If the court in *Horizon* can read an injury in fact into the FCRA, the Supreme Court can read an injury in fact into state breach laws when a breach occurs.

If the Supreme Court were to lean in the other direction, toward the more fact-dependent reading of the *Spokeo* standard, this would suggest a change in perspective on data breach cases. The Court's focus on factual allegations and purposes of extraction creates a more difficult case for standing in matters involving laptop theft. Requiring facts that support a purpose to a theft seems to suggest that the Court is uninterested in alleviating the threat of identity theft or does not trust that identity theft is common or likely. Surveys conducted by the Identity Theft Resource Center show that 43% of all identity thefts are from medical information.[240] Further, "[a]ccording to HHS, the theft of a computer or other

237. *See supra* notes 215–23 and accompanying text.

238. Schuman, *supra* note 14.

239. In re Horizon Healthcare Servs. Data Breach Litig., 846 F.3d 625, 637 (3d Cir. 2017).

240. Michael Ollove, *Nearly Half of Identity Thefts in U.S. Are Medical Info*, USA TODAY (Feb. 7, 2014, 11:20 AM), http://www.usatoday.com/story/news/nation/2014/02/07/stateline-identity-thefts-medical-information/5279351/.

electronic device is involved in more than half of medical-related security breaches."[241] Courts have an opportunity to place pressure on health systems to motivate encryption now and should do so.

V. CONCLUSION

Laptop thefts are increasingly common, and identity theft as a result is a threat that can be avoided with encryption. Current laws and regulations have proven to weakly reprimand a common practice of negligence in the healthcare industry. Something more must be done to motivate encryption. This Note suggests three possible avenues for change: regulation, legislation, and adjudication.

A long history of regulatory promulgation signals an ever-conscious effort to force healthcare systems to encrypt, but everything short of mandate has fallen flat. HHS should mandate encryption, not merely suggest it.

Federal legislators should follow in the footsteps of the European Union in enacting a consistent, consumer-friendly law governing data privacy. Similarly, state legislators should collaborate on breach laws, following California's lead in granting a private right of action.

Courts should continue to confer Article III standing in laptop theft cases where there is an alleged threat of future harm. The Supreme Court should resolve that: an injury in fact can be established by any increase in the likelihood of threat of future harm, accompanied by a showing at least that identity theft is common in similar situations; the mere theft of a laptop suggests the misuse of the PHI contained within it, thus satisfying the "certainly impending" standard; that breach laws were established to prevent the kind of unwanted disclosure of PHI at play in laptop thefts; and that violations of those statutes constitute a foundation for standing under the injury prong. If these assertions are made precedent, laptop encryption would certainly be on the rise.

The most common concern for healthcare providers is allocation of resources and capital. While compliance, legal, and cybersecurity teams wrestle with responses to breaches and threats of potential law suits over digital and physical theft, patients continue to need medical care. Patient care should continually be hospitals' top priority in allocating funds. In implementing proactive mitigating measures and policies like laptop encryption and safety, hospitals can better ensure that all patients are properly cared for.

241. *Id.*