BYU Law Review

Volume 2014 | Issue 5 Article 7

November 2014

# The Creation of HIPAA Culture: Prioritizing Privacy Paranoia over Patient Care

Jessica Jardine Wilkes

# The Creation of HIPAA Culture: Prioritizing Privacy Paranoia over Patient Care

## INTRODUCTION

> A major goal of [HIPAA] is to assure that individuals' health information is properly protected while allowing the flow of health information needed to provide and promote high quality health care and to protect the public's health and well being. The Rule strikes a balance that permits important uses of information, while protecting the privacy of people who seek care and healing. . . . [HIPAA] is designed to be flexible and comprehensive to cover the variety of uses and disclosures that need to be addressed.[1]

Every American doctor cannot help but be familiar with HIPAA, or the "Health Insurance Portability and Accountability Act," which created a national standard for accessing and handling health information.[2] Under the statute, providers and those who contract with them—called, respectively, covered entities and business associates—must protect the privacy and security of patient health information ("PHI") and provide patients with access to and certain rights associated with their individual PHI.[3] Covered entities traditionally include providers—doctors, clinics, psychologists, dentists, chiropractors, nursing homes, and pharmacies—and health plans, including both health insurance companies and government programs that pay for health care.[4] Business associates contract with covered entities to care for administrative aspects of providing healthcare; for example, a covered entity may contract with a business associate to securely dispose of outdated records. Given the difficulties associated with safely transmitting PHI between these

1. *Summary of the HIPAA Privacy Rule*, DEP'T OF HEALTH & HUMAN SERVS., 1, http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/privacysummary.pdf (last visited Oct. 1, 2014).

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

3. *Summary of the HIPAA Privacy Rule*, *supra* note 1, at 1–13.

4. *Id.* at 2.

various entities, HIPAA originally sought to ease information-sharing burdens while still providing adequate protection for PHI.[5]

Despite these goals, HIPAA privacy laws have "been a common source of unresolved confusion."[6] A two-year, $11.5 million privacy compliance study funded by the Department of Health and Human Services ("HHS"), the department tasked with HIPAA enforcement, found that four years after HIPAA went into effect, covered entities struggled with understanding and implementing basic concepts in the statute.[7] Many covered entities have consequently "implemented business practices in the name of privacy and security that have no basis in law" in an effort to protect themselves from suffering HIPAA's notoriously severe monetary penalties.[8] Whatever the perplexity surrounding HIPAA "basics," the statutory penalties, at least, are well advertised and widely dreaded in the medical community.[9]

This disjointed HIPAA experience—arising from highly publicized, progressively larger fines[10] and increased auditing,[11] but not matched by an understanding of how to adequately prevent the same—has led to heavy overcompensation on preventative measures, at the expense of best patient care as well as privacy obsession among

5. *Id*.

6. *Posts Categorized as "HIPPA"*, HEALTHBLAWG, http://healthblawg.typepad.com/healthblawg/HIPAA/page/17/.

7. Linda L. Dimitropoulos, *Privacy and Security Solutions for Interoperable Health Information Exchange*: *Impact Analysis*, RTI INT'L (December 20, 2007), *available at* http://www.rti.org/pubs/phase2_impactanaly.pdf.

8. *Id*.

9. *See HIPAA Violations and Enforcement*, AM. MED. ASS'N, http://www.ama-assn.org//ama/pub/physician-resources/solutions-managing-your-practice/coding-billing-insurance/hipaahealth-insurance-portability-accountability-act/hipaa-violations-enforcement.page (last visited Oct. 1, 2014) [hereinafter *AMA HIPAA Violations*].

10. With the new Omnibus HIPAA rules, issued January 25, 2013, HHS raised HIPAA violation penalties. 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, 5567 (proposed Jan. 25, 2013) (to be codified at 45 C.F.R. pt. 160 and 164) [hereinafter *Modifications to HIPAA Rules*]; *see also* Amanda McGrory-Dixon, *HHS Toughens HIPAA Violation Penalties*, BENEFITSPRO, http://www.benefitspro.com/2013/04/09/hhs-toughens-hipaa-violation-penalties (last visited Oct. 1, 2014).

11. *Are You Ready for a HIPAA Audit?*, EY, http://www.ey.com/Publication/vwLUAssets/Be_ready_for_a_HIPAA_audit/$FILE/EY_5_Insights-HIPAA_OCR_Audit-March_2013.pdf (last visited Oct. 1, 2014).

providers and, consequently, their patients.[12] The statute's murky standards and tremendous potential for monetary and reputational penalties has taught the medical community at large to resist and even fear sharing PHI. Providers are unwilling to share PHI with one another, and patients have learned to guard their medical records with similar obstinacy.[13] Scholars, politicians, and medical experts widely acknowledge the benefits of health-sharing initiatives, both in terms of monetary savings and enhanced patient care;[14] nevertheless, provider and patient reluctance to transmit PHI has led to serious difficulty employing new technology aimed at sharing that data. Such advancements include electronic health record systems, which are electronically stored medical records, and health information exchanges ("HIEs"), which are avenues through which electronic health records can be transmitted between providers.

This Comment will examine the way that HIPAA, as an expressive law with behavior-altering sanctions, has shaped privacy culture and PHI-sharing behavior within the medical community, particularly in relation to the attempted creation of HIEs. Prior scholarship has discussed how legislation communicates and creates

12. Government publications as well as patient-advocate groups perpetuate this "PHI-phobia" and encourage patients to talk to their doctors for more information about privacy and confidentiality concerns. *See, e.g.*, *Protect Your Medical Records*, USA.GOV http://www.usa.gov/topics/family/privacy-protection/medical.shtml (last updated Sept. 3, 2014) ("Talk with your doctor about confidentiality concerns. . . . Read the fine print. Most authorization forms contain clauses allowing information to be released. You may be able to restrict some disclosures by revising the form. . . . Be sure to initial and date your revisions. . . . Register your objections to disclosures that you consider inappropriate. . . . Be cautious when providing personal information . . . ."); *Empowering Consumers. Protecting Privacy*, PRIVACY RTS. CLEARINGHOUSE, https://www.privacyrights.org/Medical-Privacy (last visited Oct. 1, 2014) ("Many people consider information about their health to be highly sensitive, deserving of the strongest protection under the law."); Judi Hasson, *How Private is Your Medical Info?*, AARP (Sept. 17, 2012) http://www.aarp.org/home-family/caregiving/info-09-2012/how-private-is-your-medical-information.html ("You don't need to be a celebrity to have valid concerns that your medical records might be stolen or read by others.").

13. *Are You Ready for a HIPAA Audit?*, *supra* note 11.

14. *See, e.g.*, Sharona Hoffman & Andy Podgurski, *Finding a Cure: The Case for Regulation and Oversight of Electronic Health Record Systems,* 22 HARV. J.L. & TECH. 103, 112 (2008) ("These systems could facilitate clinicians' access to critical patient information and could prevent medical errors, thereby potentially saving thousands of lives and billions of dollars."); *Transforming Health Care: The President's Health Information Technology Plan*, WHITE HOUSE, http://georgewbush-whitehouse.archives.gov/infocus/technology/economic_policy200404/chap3.html (last visited Oct. 1, 2014); Kory Mertz, *Health Information Technology 2007 and 2008 State Legislation*, NAT'L CONF. ST. LEGISLATURES 1, http://www.ncsl.org/print/health/forum/hit_enacted.pdf (last visited Oct. 1, 2014).

social values[15] and has also evaluated the confusion surrounding HIPAA standards.[16] Benefits of electronic health record access are also widely recognized,[17] but many HIEs have struggled enrolling sufficient providers to create financially sustainable information technology structures.[18] This Comment adds to the scholarship by connecting the two, demonstrating how the HIPAA statute, with its blurred standards and draconian penalties, has created a privacy paranoia in patients through their providers that has obstructed health-enhancing and cost-saving PHI-sharing between consenting providers. HIPAA, instead of enhancing physician collaboration, has actually inhibited patient care and cost health care systems hundreds of millions of dollars.[19] It is the job of lawmakers to change public perception, to reverse this "PHI paranoia" among providers and patients, to enhance patient care through appropriately shared and protected PHI within HIEs, and to fulfill both original goals of

15. *See, e.g.*, Maggie Wittlin, *Buckling Under Pressure: An Empirical Test of the Expressive Effects of Law*, 28 YALE J. ON REG. 419, 420 (2011).

16. *See, e.g.*, Hoffman & Podgurski, *supra* note 14 (citing ATL. INFO. SERVS., INC., WASHINGTON, D.C., HIPAA COMPLIANCE STRATEGIES: NATIONAL REVIEW OF HIPAA COMPLIANCE FINDS RAMPANT CONFUSION, MISTAKES, REP. ON PATIENT PRIVACY (2007)); Jenna Phipps, Note, *State of Confusion: The HIPPA Privacy Rule and State Physician-Patient Privilege Laws in Federal Question Cases*, 12 SUFFOLK J. TRIAL & APP. ADVOC. 159 (2007).

17. *See* Hoffman & Podgurski, *supra* note 14.

18. *See, e.g.*, Mathematica Pol'y Res., Harvard Sch. Pub. Health & Robert Wood Johnson Found., *Health Information Technology in the United States: Better Information Systems for Better Care, 2013*, ROBERT WOOD JOHNSON FOUND., http://www.rwjf.org/content/dam/farm/reports/reports/2013/rwjf406758 (last accessed Oct. 1, 2014); *see also* Susan D. Hall, *HIEs Still Struggle with Interoperability, Finances*, FIERCE HEALTH IT (Nov. 8, 2013), http://www.fiercehealthit.com/story/hies-still-struggle-interoperability-finances/2013-11-08 ("Interoperability issues continue to stifle health information exchange (HIE) organizations' ability to connect, and sustainability remains a struggle . . . ."); Helen Gregg, *Seeing Health Information Exchanges as a Community Effort*, BECKER'S HOSP. REV. (Aug. 16, 2013), http://www.beckershospitalreview.com/healthcare-information-technology/seeing-health-information-exchanges-as-a-community-effort.html.

19. One study at the Mayo Clinic found that HIPAA implementation cost for the statutory privacy requirements was $2,734,855. This number did not include lost resources as a result of implementation, such as repeated testing, diminished communication between practitioners (and between practitioners and patients), and poor drug-use tracking. Arthur R. Williams et al., *HIPAA Costs and Patient Perceptions of Privacy Safeguards at Mayo Clinic*, 34 JOINT COMMISSION J. QUALITY & PATIENT SAFETY 27, 27 (2008). Similarly, the government estimates that the cost of updating HIPAA compliance this year "is estimated to be between $114 million and $225.4 million in the first year of implementation and approximately $14.5 million annually thereafter." *Modifications to HIPAA Rules*, *supra* note 10.

HIPAA: simultaneously "protecting . . . [patient] privacy" and "protect[ing] the public's health and well-being."[20]

Part I of this Comment briefly reviews the history of the HIPAA statute. Part II examines the theory surrounding law's expressive value in shaping culture and decision making. Part III provides an overview of HIPAA standards, current HIPAA enforcement, and the importance of privacy standards. Part IV discusses existing HIE implementation and analyzes the difficulties associated with the enactment of the Houston HIE, Greater Houston Healthconnect, resulting from HIPAA's unintended culture, and briefly reviews potential solutions. In this part, the experience of the author working for the Houston HIE illustrates the challenges that the HIPAA culture presents for successful implementation of HIEs around the country. Part V concludes.

## I. HIPAA HISTORY AND EVOLUTION OF ELECTRONIC HEALTH RECORD SYSTEMS

The evolution of the HIPAA statute provides a framework for evaluating HIPAA culture. This brief overview moves chronologically through the creation and implementation of the HIPAA statute.

Early efforts to regulate and protect electronic PHI transmission were unsuccessful,[21] and initial legislative attempts to construct privacy regulations were also unsuccessful. For example, the "Medical Records Confidentiality Act of 1995" (S. 1360), a bill designed to provide Americans with greater control over their PHI, to standardize PHI protection and handling, and "[t]o ensure personal privacy with respect to medical records and health care-related information,"[22] did not pass.[23]

20. *Summary of the HIPAA Privacy Rule*, *supra* note 1.

21. During the administration of George H.W. Bush, HHS consulted with healthcare industry leaders in order to create an electronic data exchange. HHS Secretary Dr. Louis W. Sullivan teamed up with Bernard R. Tresnowski, president of the Blue Cross Blue Shield Associations, and Joseph T. Brophy, the former president of The Travelers Insurance Company, to build the Workgroup for Electronic Data Interchange to create a national electronic health record system and cut healthcare costs. They failed to finish this project before Bush lost reelection, but the Workgroup for Electronic Data Interchange became a player in future healthcare legislation. STEVE BASS ET AL., HIPAA COMPLIANCE SOLUTIONS 12–13 (2002).

22. Medical Records Confidentiality Act of 1995, S. 1360, 104th Cong. (1995).

23. Gail Dudley, *Electronic Records, Patient Confidentiality, and the Impact of HIPAA*,

Other healthcare bills not directly addressing medical privacy, however, did pass, including HIPAA on August 21, 1996.[24] The original HIPAA statute, though, dealt only tangentially with PHI privacy through the adoption and standardization of electronic health records.[25] The central intent of HIPAA was, ironically, unrelated to its infamous privacy requirements. HIPAA's purpose was to "mak[e] healthcare delivery more efficient and increas[e] the number of Americans with health insurance coverage"[26] primarily by guaranteeing availability of private health insurance coverage for some and "limit[ing] the use of pre-existing condition clauses."[27] Additionally, HIPAA encouraged the purchase of long-term insurance through tax incentives as well as the creation of state insurance pools for high-risk individuals.[28] Though some of these sections arguably had positive effects on universally accessible insurance provisions, this Comment will not address the successes or lack thereof of these portions of the statute particularly because insurance provisions in the Affordable Care Act have largely replaced the insurance portability and accessibility provisions.[29]

The administrative simplification provisions present in the HIPAA statute[30] instructed the Secretary of HHS to create regulatory guidelines concerning the electronic transmission of

PATIENT SAFETY & QUALITY HEALTHCARE (Mar. 20, 2014 8:24 PM), http://www.psqh.com/octdec04/dudley.html.

24. Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub. L. No. 104-191, § 261, 100 Stat. 1936, 2021 (codified as amended in scattered sections of 5–42 U.S.C.).

25. *Id.* ("It is the purpose of this subtitle to . . . encourag[e] the development of a health information system through the establishment of standards and requirements for the electronic transmission of certain health information.").

26. INST. OF MED., COMM. ON HEALTH RESEARCH & THE PRIVACY OF HEALTH INFO., BEYOND THE HIPAA PRIVACY RULE: ENHANCING PRIVACY, IMPROVING HEALTH THROUGH RESEARCH 63 (Sharyl J. Nass et al. eds., 2009), *available at* http://www.ncbi.nlm.nih.gov/books/NBK9576/ [hereinafter BEYOND THE HIPAA PRIVACY RULE].

27. S. REP. NO. 105-5, at 30 (1997). *See also* BARRY R. FURROW ET AL., THE LAW OF HEALTH CARE ORGANIZATION AND FINANCE 352 (7th ed. 2013). HIPAA amended ERISA, the Public Health Services Act, and the Internal Revenue Code to restrict pre-existing condition clauses and prohibit discrimination in rates and coverage within employee groups. *Id.*

28. FURROW ET AL., *supra* note 27, at 407–08.

29. *Id.* at 407. The privacy provisions of HIPAA at issue in this paper are unhindered by the ACA.

30. Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub. L. No. 104-191, § 262, 100 Stat. 1936, 2021 (codified as amended in scattered sections of 5–42 U.S.C.).

PHI.[31] The primary purpose of the HHS requirements was to standardize electronic health records and electronic medical records,[32] not to create federal regulations specifically targeting health information privacy concerns.

HIPAA also delegated enforcement to HHS, which began to establish standards for electronic medical data storage and transmission.[33] HHS first issued proposed HIPAA privacy rules for public comment in 2000, which received an "enormous volume of comments."[34] Perhaps recognizing a rising public concern about electronic PHI transmission, the department widely broadcast its future adoption of uniform security rules,[35] which set minimum requirements for PHI protection and use,[36] thereby temporarily assuaging the public's concerns. After several drafts, the final rule was released in 2002.[37] Thus, the current HIPAA regulation regime is not a "result of a[ny] direct congressional statutory command but [instead arose] from a fairly broad interpretation of the statute by the implementing agency,"[38] and the current state of HIPAA culture bears little resemblance to the original statutory privacy suggestions.

The HIPAA statute as now written is intended "to combat waste, fraud, and abuse in health insurance and health care delivery, . . . to improve access to long-term care services and

31. *Id.*

32. BEYOND THE HIPAA PRIVACY RULE, *supra* note 26. "EMR" refers to "electronic medical record," and though widely used interchangeably with "EHR," or "electronic health record," EMR is technically a computerized patient record maintained within one single healthcare entity rather than made nationally available regardless of patient location.

33. *See* Health Insurance Portability and Accountability Act § 264 ("Not later than . . . 12 months after the date of the enactment of this Act, the Secretary of Health and Human Services shall submit . . . detailed recommendations on standards with respect to the privacy of individually identifiable health information.").

34. BEYOND THE HIPAA PRIVACY RULE, *supra* note 26, at 64.

35. *See, e.g.*, Health Insurance Reform: Standards for Electronic Transactions, 65 Fed. Reg. 50, 312, 50, 351 (Oct. 16, 2000) (to be codified at 45 C.F.R. pts. 160 & 162). ("As discussed in the proposals, the regulations will provide a consistent and efficient set of rules for the handling and protection of health information. . . . [T]he promulgation of a final privacy standard will enhance public confidence that highly personal and sensitive information is being properly protected, and therefore, it will enhance the public acceptance of increased use of electronic systems.").

36. *See* 45 C.F.R. § 160.203 (2002).

37. 45 C.F.R. §§ 160, 164 (2002). Most health care organizations were required to comply by April 14, 2003. BEYOND THE HIPAA PRIVACY RULE, *supra* note 26, at 64.

38. Ilene N. Moore et al., *Confidentiality and Privacy in Health Care from the Patient's Perspective: Does HIPAA Help?,* 17 HEALTH MATRIX 215, 228 (2007).

coverage, [and] to simplify the administration of health insurance."[39] HHS declared that its "goal is, and has always been, to permit [appropriate data-sharing between covered entities] to occur with little or no restriction"[40] with as much "flexibility" as possible.[41] HIPAA regulatory enforcement has frustrated these goals through its expressive effect.

## II. BRIEF OVERVIEW OF EXPRESSIVE LAW THEORY

Roughly two decades ago, legal theorists began examining ways in which the law communicates and even alters social values.[42] Legal theorists also recognized that the law can shape customs through its effect on social norms in the aggregate.[43] Individuals endorse these customs partly by observing others' actions, even if those behaviors are exhibited in response to laws, and partly by "distorting their public responses in the interest of maintaining social acceptance."[44] This can be particularly true of laws that include immediate sanction. Over extended periods of time, the resulting habit formation directly informs moral education.[45] Laws that include sanctions are especially prone to expressive qualities because the threat of sanction itself encourages altered behavior, and, ultimately, these types of laws most often alter social norms.[46]

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

40. Standards for Privacy of Individually Identifiable Health Information, 67 Fed. Reg. 53,182, 53, 208–9 (Aug. 14, 2002) (to be codified at 45 C.F.R. pts. 160, 164).

41. *Id.*

42. Wittlin, *supra* note 15, at 420 (citing Robert Cooter, *Expressive Law and Economics*, 27 J. LEGAL STUD. 585, 585 (1998)).

43. Daniel L. Chen & Susan Yeh, *Distinguishing Between Custom and Law: Empirical Examples of Endogeneity in Property and First Amendment Precedents*, 21 WM. & MARY BILL RTS. J. 1081, 1081–82 (2013).

44. *Id.* at 1082 (citing Timur Kuran & Cass R. Sunstein, *Availability Cascades and Risk Regulation*, 51 STAN. L. REV. 683 (1999)) (analyzing the channels from perception formation to regulatory policy changes); Edward T. Swaine, *Rational Custom,* 52 DUKE L.J. 559 (2002) (applying rational choice theory to explain the role of custom in international law).

45. Wittlin, *supra* note 15, at 427 (citing H. LAURENCE ROSS, DETERRING THE DRINKING DRIVER 8 (1981), *available at* http://ntl.bts.gov/lib/25000/25500/25588/DOT-HS-805-820.pdf).

46. *See, e.g.*, Dhammika Dharmapala & Richard H. McAdams, *The Condorcet Jury Theorem and the Expressive Function of Law: A Theory of Informative Law*, 5 AM. L. & ECON. REV. 1, 2 (2003); Robert Cooter, *Expressive Law and Economics*, 27 J. LEGAL STUD. 585, 594 (1998).

Theories about how law's "expressive statements"[47] alter behavior and which aspects of law produce expressive effect can be divided into three major categories: (1) theories that the law creates a "meaning account" for pre-established social norms or that the law creates an anticipated action;[48] (2) theories that suggest laws signal existing norms and consequently changes behavior to match the norm;[49] and (3) theories that law can change social norms by altering individual values, which then directly shapes social norms.[50]

In the first group, theorists Cass Sunstein and Lawrence Lessig argue that law can change the social meaning of an action through "social condemnation" or "positive social effects."[51] Lessig cites the historical example of dueling to support his point: a law that prohibited dueling did little to curb the practice because interests in "honor" prevailed, but a law that made a duel participant ineligible for public office more effectively discouraged the practice.[52] The former law added only potential jail time, but the second created what Sunstein calls a "meaning account"[53] by infringing on the duty to serve in one's community and consequently "ambiguated the social meaning of dueling."[54]

The second group of theories, including work by theorist Richard McAdams, suggests that the law signals existing norms.[55] Like Sunstein's "meaning account," this theory recognizes society's interpretation of an act, but this branch of expression theory does not assume laws actively change social meaning and instead argues that "law changes behavior by signaling the underlying attitudes of a community or society."[56] By proposing that laws signal social values,

47. Wittlin, *supra* note 15, at 423.

48. *See, e.g.*, Cass Sunstein, *On the Expressive Function of Law*, 144 U. PA. L. REV. 2021, 2032–33 (1996).

49. *See* Richard H. McAdams, *An Attitudinal Theory of Expressive Law*, 79 OR. L. REV. 339, 340 (2000).

50. *See* Cooter, *supra* note 46, at 586.

51. Wittlin, *supra* note 15, at 424 (citing Lawrence Lessig, *Social Meaning and Social Norms*, 144 U. PA. L. REV. 2181, 2185 (1996)).

52. *Id.*

53. *Id.* at 425 (citing Cass Sunstein, *On the Expressive Function of Law*, 144 U. PA. L. REV. 2021, 2052 (1996)).

54. *Id.* at 424 (citing Lawrence Lessig, *Social Meaning and Social Norms*, 144 U. PA. L. REV. 2181, 2186–87 (1996)).

55. *See* Richard H. McAdams, *An Attitudinal Theory of Expressive Law*, 79 OR. L. REV. 339, 340 (2000).

56. *Id.*

McAdams relies on the presumption that "democratically produced legislative outcomes"—or, at least, those that are well-publicized and created separately from interest group lobbying[57]—"are positively correlated with popular attitudes."[58]

The third category of theories includes Robert Cooter's research regarding a law's expressive function as a way to change behaviors. He argues that the law has two expressive functions: to either "change social norms directly by solving collective action problems" or to "change social norms by shaping individual values."[59] The former is more applicable to public goods laws, like anti-littering laws, rather than laws influencing risky behaviors—for example, failing to adequately protect patient privacy. The theory relies on Cooter's vision of a world with a stable social equilibrium, where a law may shift the equilibrium to a new focal point.[60] When it comes to law's second expressive function—changing social values by changing individual values—Cooter posits "that a rational person will want to change her preferences when the opportunities presented by this observable change in character are superior according to both new preferences and old preferences."[61] Cooter notes that laws with sanctions prompt "character improvement" and ultimately alter internalized values.[62] In the aggregate, reformed individual values build a new social norm,[63] defined as "an obligation backed by a social sanction."[64] Through deterrence efforts (for example, jail time or monetary fines), the state can supplement negative social costs associated with disobeying a social norm.[65] Finally, once an individual has internalized the norm and changed her preferences, there is a personal cost from violating the norm, and, therefore, the public is more likely to observe the norm.[66] Thus,

57. Wittlin, *supra* note 15, at 425 (citing McAdams, *supra* note 55).

58. *Id*.

59. *Id*. (citing Cooter, *supra* note 46, at 586).

60. *Id*. at 425–26 (citing Cooter, *supra* note 46, at 594).

61. *Id*. at 426 (citing Cooter, *supra* note 46, at 600).

62. *See* Cooter, *supra* note 46, at 605.

63. *See id*.; *see also* Chen & Yeh, *supra* note 43, at 1081–82.

64. Robert D. Cooter, *Three Effects of Social Norms on Law: Expression, Deterrence, and Internalization*, 79 OR. L. REV. 1, 5 (2000).

65. *Id*. at 7–8, 15.

66. *Id*. at 7.

expression, deterrence, and internalization of laws change individual preferences, choices, and, ultimately, collective norms.[67]

Cooter's theory is most accurate when applied to laws backed by sanctions. Laws backed by a sanction are more likely to influence individual behavior and consequently social norms; the "sanction itself has expressive force."[68] Accordingly, these results suggest that in the arena of laws backed by sanctions—like HIPAA—Cooter's second theory best explains the outcome: threatened sanctions alone transform behavior and social norms to match the message communicated by the law.

## III. CREATION OF HIPAA CULTURE

Cooter's theory best explains what happened following enactment of the HIPAA statute. The HIPAA statute created a "HIPAA-culture"; the overbroad law and threat of sanctions spawned an inevitably overbroad regulatory privacy regime and effectively convinced patients and providers that the act of sharing PHI is morally problematic.[69] Additionally, steep fines exacerbate the expressive effect of sanctions[70]–and HIPAA fines can be devastatingly high.[71] Sections A and B of this part explain the creation of HIPAA culture, which has arisen from HIPAA violation punishments, public shaming techniques on HHS's "Wall of Shame,"[72] recent Omnibus HIPAA alterations, and resulting pervasive "compliance over

67. *Id*. Incidentally, recently published empirical data confirm the applicability and reality of Cooter's second theory. One recent study that measured the impact of seatbelt laws on seatbelt usage demonstrates that laws alter individual behavior and communicate social norms through that altered behavior. But even without widespread conformance to the law, the mere existence of such a law increased seatbelt usage. Wittlin, *supra* note 15, at 421.

68. *Id*.

69. *See* Yuval Feldman & Janice Nadler, *The Law and Norms of File Sharing*, 43 SAN DIEGO L. REV. 577, 623 (2006).

70. *See* Dan M. Kahan, *What Do Alternative Sanctions Mean?,* 63 U. CHI. L. REV. 591, 593, 623 (1996).

71. These violations will be thoroughly discussed in Section B of this Part. Under the most recent Omnibus HIPAA law, as of September 23, 2013, violations range from $100 to $50,000. The maximum civil penalty for all identical violations in a given year, whether knowing or due to willful, uncorrected neglect, is $1.5 million. *Modifications to HIPAA Rules*, *supra* note 10, at 5583.

72. *Health Information Privacy: Breaches Affecting 500 or More Individuals*, U.S. DEP'T HEALTH & HUM. SERVICES, http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachtool.html (last updated 2014) [hereinafter "WALL OF SHAME"].

security" provider mindset.[73] Section C examines the established HIPAA culture and current state of the HIPAA statute, which demonstrate that the statute's expression, deterrence, and internalization have now changed social norms regarding PHI protections. Section D reviews legitimate privacy considerations.

### *A. A Study of HIPAA Compliance and Patient Complaints: Creation of the HIPAA Culture*

A study conducted by Vanderbilt University Center for Patient and Professional Advocacy investigated patient concerns regarding privacy in health care settings, including whether there has been any improvement in privacy protection since HIPAA implementation.[74] The Vanderbilt study analyzed complaint data from inpatient, outpatient, and emergency departments originating from three geographically distant academic medical centers over a five-year period.[75] The study first revealed that patients' perceptions of privacy protections are a "major factor" in measuring their subjective satisfaction with received healthcare as well as the objective quality of their medical care,[76] in part because patients are likely to provide incomplete medical information if they perceive compromised confidentiality standards.[77] Second, patients complained most about incidental and willful disclosures, followed by "environmental disclosures" and institutional privacy policies.[78] Physicians were mentioned in 20% of privacy complaints[79] while non-physicians were associated with more than 50% of privacy complaints.[80]

Importantly, privacy-related complaints for all institutions increased in frequency during the second observation period (from 2003 to 2005)[81] and rose concurrently with institutional efforts from

73. KROLL ADVISORY SOLUTIONS, 2012 HIMSS ANALYTICS REPORT: SECURITY OF PATIENT DATA 6 (2012), *available at* http://www.csb.uncw.edu/people/cummingsj/classes/MIS534/Articles/Ch6SecurityReport.pdf [hereinafter "HIMSS ANALYTICS REPORT"].

74. Moore et al., *supra* note 38, at 218–19.

75. *Id*. at 235–36.

76. *Id*. at 233.

77. *Id*.

78. *Id*. at 237.

79. *Id*. at 238.

80. *Id*. at 240.

81. *Id*. at 239.

all organizations to better comply with HIPAA requirements.[82] The patient work volume, including procedures and numbers of patients, increased by 21% from the first observation period to the second, but the privacy-related complaints rose more than 140% on a constant workload basis across the board[83] and up to 200% on an absolute basis in at least one institution.[84] The type of complaints and numbers in each category did not vary significantly from one institution to another.[85] Furthermore, the number of privacy-related complaints as compared to other patient complaints rose significantly from the first observational period to the second.[86] These complaint increases, while staggering, may actually be the "tip of the iceberg" in patient privacy anxieties because very few dissatisfied or concerned patients inform the offender of their frustrations, and even fewer register a formal or informal complaint.[87]

The increase in patient privacy complaints from the first observational period to the second, during the first of which the final HIPAA privacy rules were implemented, might have resulted from the expressive effect of the law. Despite the fact that the institutions were more HIPAA compliant, the number of patient privacy complaints rose 140% on a constant workload basis between the first and second observational periods and the ratio of privacy complaints to non-privacy complaints rose dramatically for two of the three institutions.[88] The rise in workload-volume does not adequately explain the disparity.[89]

These numbers may suggest that as patients became more aware of HIPAA's existence between the first and second observational periods in the study, patients also became more fearful of privacy breaches. The author of the Vanderbilt study suggests that the institutions may not have been HIPAA compliant and may have

82. *Id*. at 244.

83. *Id*. at 239–40.

84. *Id*. at 244–45.

85. *Id*. at 245.

86. *Id*. at 244–45.

87. *Id*. at 243 (citing ARTHUR BEST, WHEN CONSUMERS COMPLAIN 114–30 (1977); Ellen Annandale & Kate Hunt, *Accounts of Disagreements with Doctors*, 46 SOC. SCI. & MED. 119, 125 (1998); Mark Schlesinger et al., *Voices Unheard: Barriers to Expressing Dissatisfaction to Health Plans*, 80 MILLBANK Q. 709, 717 (2002) (citing 1988 study that found "as few as 11 percent of American patients complain about the problems they experience").

88. *Id*. at 239–40.

89. *See generally id*.

simply had more legitimate privacy breaches from the first to second observational period.[90] As will later be discussed, HIPAA compliance does not necessarily equate with increased PHI security,[91] but it is extremely unlikely that in efforts to become more HIPAA compliant and better protect patient data, the institutions became *less* compliant and *less* secure. Furthermore, in the second observational period, some patients "complained of behaviors or disclosures that are, in fact, allowed by HIPAA."[92] Though a HIPAA-compliant institution is not necessarily a PHI-secure institution, the institutions in the study nevertheless made efforts to improve in those areas over the period studied. Yet most experienced a dramatic surge in privacy-related patient complaints.[93] This suggests that the confidentiality and privacy issues gained saliency and popularity through dissemination of HIPAA information from providers to patients.[94] Because the HIPAA statute was so poorly understood, even by professionals,[95] it is unlikely that during that time period patients learned their rights directly from the HIPAA statute; nevertheless, the patients' limited exposure to the statute through institutions' privacy notices, HIPAA acknowledgement forms, and provider behavior or commentary changed their understanding of medical privacy from the first to the second observational period.[96] Accordingly, patients likely became more aware of HIPAA's existence, if not its particulars, and their doctors' fears of sanctions for non-compliance; thus, the "HIPAA culture" was born.

### *B. HIPAA Violations and Their Contribution to HIPAA Culture*

Cooter's theory of expressive law demonstrates that laws backed by sanctions have particular expressive force, and threatened

90. *Id*. at 246.

91. HIMSS ANALYTICS REPORT, *supra* note 73, at 6.

92. Moore et al., *supra* note 38, at 248.

93. *Id*. at 244.

94. *Id*. at 245.

95. *Id*. at 248 (citations omitted) ("While patients retain the authority to prohibit disclosures not otherwise excepted, the list of exceptions is so extensive as to eviscerate any common understanding of what it means to be in control of one's medical information."); *id*. at 250–51 ("[Notices of HIPAA privacy practices] have . . . been a common source of unresolved confusion."); *id*. at 255 ("[HHS] must articulate a norm that health care providers and personnel can understand and follow.").

96. *Id*. at 239–40.

sanctions alone influence social norms to match the message communicated by the law.[97] In the context of HIPAA, excessively high monetary penalties have contributed to HIPAA culture by generating justified fear of enormous financial burdens.[98] These concerns are likely enhanced by the "Wall of Shame" and recent updates to the HIPAA statute through the Omnibus HIPAA Act in January 2013.[99] While to some limited degree it is likely that PHI will be better protected by the Omnibus revisions that extend potential liability to business associates, expand the requirements for reportable breaches, and increase HIPAA audits, a recent survey reveals that increased HIPAA compliance does *not* equate to increased PHI protection among health care organizations. In fact, those organizations surveyed consistently prioritize compliance over patient information security.[100] The law and its sanctions have created a pervasive HIPAA culture that favors compliance over privacy. This section will briefly review (1) the HIPAA penalties, (2) the "Wall of Shame," (3) changes to the Omnibus HIPAA law, and (4) recent survey data demonstrating providers' greater interest in HIPAA compliance than PHI security.

*1. The HIPAA penalties*

Violating HIPAA can be extremely costly. The Office of Civil Rights under HHS handles HIPAA complaints and can impose civil penalties for failure to comply.[101] Prior to the Health Information Technology for Economic and Clinical Health (HITECH) Act, HIPAA violations were $100 per unknowing violation with a $25,000 cap.[102] After February 17, 2009, under HITECH, penalties ranged from $100 to $50,000 or more per violation.[103] Each penalty for individual violations was tiered based on the entity's perceived

97. Robert Cooter, *Expressive Law and Economics*, 27 J. LEGAL STUD. 585, 594 (1998).

98. *See generally* Health Information Technology for Economic and Clinical Health (HITECH) Act, Pub. L. No. 111-5, 123 Stat. 226 (2009).

99. WALL OF SHAME, *supra* note 72.

100. HIMSS ANALYTICS REPORT, *supra* note 73.

101. 45 C.F.R. § 160.404 (2013).

102. Patrick Ouellette, *HIPAA Omnibus and HITECH Civil Penalty Changes*, HEALTHIT SECURITY (Jan. 23, 2013), http://healthitsecurity.com/2013/01/23/hipaa-omnibus-and-hitech-civil-penalty-changes/.

103. Health Information Technology for Economic and Clinical Health (HITECH) Act, Pub. L. No. 111-5, 123 Stat. 226 (2009).

culpability with annual caps ranging from $25,000 to $1.5 million.[104] Under the most recent Omnibus HIPAA law, as of September 23, 2013, violations still range from $100 to $50,000 in a tiered fashion, but the maximum civil penalty for all identical violations in a given year, whether knowing or due to willful, uncorrected neglect, is $1.5 million.[105] Each unauthorized PHI disclosure incident can comprise multiple violations.[106] This requires HHS to "count" the violations after a PHI breach based on the "nature and extent of the violation."[107] This may include people affected, time period, level and type of harm, any previous HIPAA violations, nature of the organization at fault, timely reporting, the organization's financial condition, and any other number of factors;[108] thus, the original violation may easily be multiplied up to the $1.5 million cap.[109] The same, single incident may also violate multiple portions of the Security Rule requiring accurate breach prevention.[110] Though the HIPAA statute's substantive requirements have generated confusion in the health community, the statute's penalties are well advertised and widely dreaded among healthcare organizations.[111]

*2. The "Wall of Shame"*

The consequent and prevalent anxiety among providers is further exacerbated by the threat of public humiliation on the HHS "Wall of Shame." In 2009, the Office of Civil Rights started recording incidents of PHI breaches and created the "Wall of Shame," which publicly exposes breaches affecting 500 people or more.[112] In theory, the "Wall of Shame" further incentivizes covered entities and business associates to prioritize patient record confidentiality, but

104. *Id*.

105. *Modifications to HIPAA Rules*, *supra* note 10, at 5583.

106. *Id*. at 5584.

107. 45 C.F.R. § 160.408 (2011).

108. *Id*.

109. *Id*., *see* "HIPAA Final Rule Expands Liability for Violations, Clarifies Penalty Assessment Methodology" (Feb. 22, 2013), http://www.crowell.com/NewsEvents/AlertsNewsletters/all/HIPAA-Final-Rule-Expands-Liability-for-Violations-Clarifies-Penalty-Assessment-Methodology.

110. 45 C.F.R. §§ 164.308–14 (2013).

111. AMA HIPAA Violations, *supra* note 9.

112. WALL OF SHAME, *supra* note 72.

recent studies show that it has not had that effect—again demonstrative of HIPAA culture.[113]

*3. Changes to the Omnibus HIPAA law*

Though the updated Omnibus HIPAA law will likely better protect patient privacy than the prior law by "strengthen[ing] the limitations on the use and disclosure of protected health information" in various arenas,[114] the increased penalties are also likely to exacerbate already-existing provider fears and HIPAA culture. Moreover, under the new law, business associates of covered entities are directly liable for HIPAA compliance.[115] The Omnibus law expanded the definition of "business associate" to include any "subcontractor that creates, receives, maintains, or transmits protected health information,"[116] such as a cloud-service provider.

Under the new Omnibus law, the definition of a "breach" is significantly more expansive as well. Prior to the Omnibus HIPAA rule, a breach was defined as an event that "compromises the security or privacy of the protected health information such that the use or disclosure poses a significant risk of financial, reputational or other harm to the individual."[117] The new rule, however, extends the definition to include even the "risk" of PHI disclosure or impermissible use as identified through a risk assessment approach.[118] This makes required HHS notification for breach more likely.[119] Only when an entity can "demonstrate there is no significant risk of harm" is the entity excused from reporting the breach.[120]

Not only has the scope of violations expanded, but recent reports also show an increase in HIPAA audits, which will likely aggravate

113. *See* HIMSS ANALYTICS REPORT, *supra* note 73.

114. *Modifications to HIPAA Rules*, *supra* note 10, at 5566.

115. *Id*.

116. *Id*. at 5572.

117. *Modifications to HIPAA Rules*, *supra* note 10, at 5639; *see also* DEP'T OF HEALTH & HUMAN SERVS., OFFICE OF CIVIL RIGHTS, *Health Information Privacy*: *Breach Notification Rule*, http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/index.html (follow "Definition of Breach" hyperlink) (last visited October 2, 2014).

118. *Modifications to HIPAA Rules*, *supra* note 10, at 5640.

119. *New Omnibus Rule Released: HIPAA Puts on More Weight*, DWT.COM, http://www.dwt.com/new-omnibus-rule-released-hipaa-puts-on-more-weight-01-23-2013/ (last visited Nov. 14, 2014)

120. *Id*.

compliance fears.[121] The law's changes in penalty and enforcement provisions suggest audits will further increase, which will likely exacerbate the expressive and social effects of HIPAA sanctions and, through that, HIPAA culture.[122] Under the Omnibus rule, HHS no longer must attempt to informally resolve privacy complaints: HHS now has the discretion to determine whether the department will pursue informal resolution before proceeding to the formal penalty assessment process.[123] Furthermore, civil violations are now tiered to correlate the severity of a violation with the nature and circumstances surrounding the incident, which suggests HHS will assess penalties almost automatically unless the potential violator can show that the breach was not due to willful neglect and was "timely" corrected.[124] Under the Omnibus rule, HHS is authorized to share any information gathered from a compliance check with other law enforcement agencies, such as a state attorney general's office.[125] Naturally, these other agencies are free to pursue their own investigations.[126]

*4. Demonstrative survey*

Not surprisingly, with increased threats of monetary sanctions, the "Wall of Shame," and HIPAA audits, healthcare organizations have justifiably reacted with fear of sharing PHI and, in the

121. Jack Anderson, *HIPAA Audits Increase in 2014, Include Business Associates*, COMPLIANCE HELPER (Jan. 9, 2014), http://www.compliancehelper.com/post/2030180-hipaa-audits-increase-in-2014-include; *see also* Marianne Kolbasuk McGee, *HIPAA Audits: More to Come in 2014*, GOVINFO SECURITY (Sept. 23, 2013), http://www.govinfosecurity.com/hipaa-audits-more-to-come-in-2014-a-6090.

122. If HIPAA enforcement directly contributed to increased patient security, these numbers might be encouraging. But, as previously demonstrated, increased compliance does *not* lead to increased PHI protection.

123. *HIPAA Omnibus Final Rule: Enforcement Action Following September 23 Compliance Deadline*, VEDDER PRICE (Sept. 2013), http://www.vedderprice.com/files/Publication/bca4ca87-9723-4ad9-8e95-ba76069b3cab/Presentation/PublicationAttachment/aa4f540a-389e-47cb-8223-07f2e1672bb9/HIPAA%20Omnibus%20Final%20Rule.pdf.

124. Ouellette, *supra* note 101.

125. *Modifications to HIPAA Rules*, *supra* note 10, at 5579.

126. *See* Eric D. Altholz & Christopher Lockman, *Enhanced Penalties and Stiffer Enforcement for HIPAA Violations*, BENEFITS L. UPDATE: EMP. BENEFITS & EXECUTIVE COMPENSATION BLOG (Apr. 7, 2013, 9:28 AM), http://www.employeebenefitsupdate.com/benefits-law-update/2013/4/7/enhanced-penalties-and-stiffer-enforcement-for-hipaa-violati.html.

aggregate, augmented the HIPAA culture. A biannual survey of United States healthcare provider facilities, performed by a "leading risk consulting firm," found that healthcare providers "prioritize *compliance* over *security*."[127] Respondents believe that, even though breach incidents are steadily rising, increased preparations to pass a HIPAA audit correlate to increased data security.[128] The survey results troublingly demonstrate that protecting patient data is not the driving force behind these respondents' security policies and procedures. Rather, the organizations are motivated by compliance interests and ultimately avoiding OCR audit fees.[129] Though organizations actively take steps to ensure PHI security, they "are so focused on meeting compliance requirements that they have little awareness of the *efficacy* of their security programs."[130]

The study revealed, however, that institutional HIPAA compliance does not equate with PHI security: 96% of organizations conducted a formal risk analysis, but 27% still experienced a breach and 18% were unsure whether their organization had experienced a breach in the past twelve months.[131] Additionally, despite the increased privacy training and heighted security policies across nearly all organizations, 45% indicated that "lack of staff attention to policy puts data at risk."[132] Of the 27% of respondents that experienced a breach, only one-quarter of those organizations subsequently updated their organization's "security action plan."[133] However, 73% of respondents said changes in external regulations (for example, HIPAA or HITECH) motivated changes to PHI protection plans.[134]

The data also demonstrate that business associate third-party arrangements dangerously compromise patient PHI, but because business associates were not liable under the HIPPA statute at the time, no efforts were made to secure PHI data held by business associates.[135] Third-party business associates comprised the fastest-

127. HIMSS ANALYTICS REPORT, *supra* note 73, at 6 (emphasis added).

128. *Id*. On a scale from one to seven, with one being "not at all prepared" and seven being "extremely prepared," respondents overall gave themselves a 6.4, as opposed to 6.06 in 2010 and 5.88 in 2008. *Id*.

129. *Id*.

130. *Id*. (emphasis added).

131. *Id*.

132. *Id*.

133. *Id*.

134. *Id*.

135. Before the HIPAA Omnibus update in May 2013, business associates were not

rising source of data breaches (at the time, 18% of breaches).[136] Twenty-eight percent of respondents indicated that sharing PHI with these third parties is the "top item that put patient data at risk,"[137] and the most recent numbers suggest that "out of the 26.8 million individuals whose data has been breached, 48 percent were impacted by breaches involving [business associates]."[138] Despite these numbers, only half of respondents in the healthcare provider survey indicated that they ensure their third-party vendors "conduct a periodic risk analysis to identify security risks and vulnerabilities."[139]

### *C. Current State of HIPAA*

Despite the fact that PHI can now be more secure in HIEs than ever before, record numbers of survey takers indicate increasing fear of privacy hackers and what has become a veritable PHI paranoia derived from HIPAA culture.[140]

In the immediate aftermath of HIPAA, surveys demonstrated that public privacy concerns had decreased—down to 67%[141] from approximately 75% in a pre-HIPAA study.[142] Polls taken in the immediate aftermath of HIPAA are not demonstrative of current feelings regarding health privacy; very limited data sets are available to assess the value of HIPAA in relation to more contemporary fears, including HIEs. Particularly with the increased utilization of health information technology and electronic health records, surveys indicate that the public is increasingly concerned about PHI privacy and security.[143] A 2012 survey by Harris Interactive reported that

liable under HIPAA regulations.

136. HIMSS ANALYTICS REPORT, *supra* note 73, at 6.

137. *Id.*

138. Melissa McCormack, *The Internet Isn't to Blame for HIPAA Breaches*, THE PROFITABLE PRAC.: HELPING YOU GROW A MORE PROFITABLE, EFFICIENT & FULFILLING PRAC. (Sept. 16, 2013), http://profitable-practice.softwareadvice.com/internet-isnt-to-blame-for-hipaa-breaches-0913/.

139. HIMSS ANALYTICS REPORT, *supra* note 73, at 7.

140. FORRESTER RESEARCH, NATIONAL CONSUMER HEALTH PRIVACY SURVEY 2005 (Nov. 2005), *available at* http://www.chcf.org/publications/2005/11/national-consumer-health-privacy-survey-2005.

141. *Id.*

142. *Id.*

143. *Only 26 Percent of Americans Want Electronic Medical Records, Says Xerox Survey*, XEROX (July 31, 2012), http://news.xerox.com/news/Xerox-Surveys-Americans-Electronic-

only 26% of patients wanted their medical records digitally accessible.[144] More than 85% of respondents expressed privacy concern about digital medical records, particularly hackers, lost files, or misused data, up from 82% in 2010.[145] These data demonstrate how little electronic health record systems are understood.

More importantly for purposes of this Comment, these survey data demonstrate that the HIPAA statute's effectiveness has been severely limited by ambiguous guidelines and deference to state laws that can actually be stricter than the federal regulations, doubtlessly adding to the creation of HIPAA culture.[146] HSS originally intended HIPAA privacy practices to promote discussions between patients and providers "related to the use and disclosure of protected health information about him or her"[147]; instead, privacy practices have become a common source of unresolved perplexity. Significant gaps remain in the HIPAA enactment, including differing patient consent protocols nationally and intrastate, misunderstanding regarding "meaningful use," and improving levels of patient involvement in using their health information.[148]

This confusion and frustration associated with enacting HIPAA has transferred to health care consumers as well—and not just because no individual remedy for redress exists for individuals' privacy violated by HIPAA breaches.[149] Approximately 13% of people surveyed in 2005 admit to behaving in various ways meant to protect

Health-Records [hereinafter XEROX 2012] (referencing a Harris Interactive survey from May 11–15, 2012).

144. *Id*. (referencing a Harris Interactive survey from May 11–15, 2012).

145. *See id*. (referencing a Harris Interactive survey from May 11 to 15, 2012); XEROX: A STUDY ABOUT MEDICAL RECORDS (Harris Interactive, 2010), *available at* http://pitchengine.com/xeroxcorporation/xerox-survey-patients-know-little-about-impact-of-electronic-health-records-); *see also* Deborah Peel, *Only 26 Percent of Americans Want Electronic Medical Records, Says Xerox Survey*, PATIENT PRIVACY RIGHTS (July 31, 2012), http://patientprivacyrights.org/2012/07/only-26-percent-of-americans-want-electronic-medical-records-says-xerox-survey/.

146. *See* Deth Sao, Amar Gupta & David A. Gantz, *Interoperable Electronic Health Care Record: A Case for Adoption of a National Standard to Stem the Ongoing Health Care Crisis*, 34 J. LEGAL MED. 55, 62 (2013) (citing 42 U.S.C. § 1320d-2; 63 Fed. Reg. at 43,258; John R. Christiansen, *Legal Speed Bumps on the Road to Health Information Exchange*, J. HEALTH & LIFE SCI. L. 1, 24 (2008)).

147. Moore et al., *supra* note 38, at 250–51 (citing Standards for Privacy of Individually Identifiable Health Information, 67 Fed. Reg. 53,182, 53,201 (Aug. 14, 2002) (to be codified at 45 C.F.R. pts. 160, 164)).

148. Christiansen, *supra* note 146, at 22–23.

149. *Id*. at 23.

their privacy, even at the expense of their own health.[150] These behaviors included, but were not limited to, lying to practitioners about symptoms or circumstances surrounding illness or injury, providing inaccurate or incomplete information, paying for health care services in cash even if covered by insurance, or avoiding care altogether.[151]

### *D. Legitimate Privacy Considerations*

Concern over the privacy paranoia created by HIPAA should be understood neither as a rejection of the importance of privacy nor as a condemnation of HIPAA's goals to protect PHI. Privacy is an essential part of providing and receiving medical care, and HIPAA successfully raised the privacy-protection standards. PHI-sharing technology pre-HIPAA focused "around what was the least disruptive to the physicians [and] nurses"[152] and rights to medical privacy widely varied between states.[153] PHI sharing today abides by national principles of privacy protection, broken only by patient consent.[154]

Additionally, HIPAA enforcement certainly has had some positive outcomes. It created minimum privacy standards, guaranteed an individual's access to personal records[155] and access to an accounting of PHI disclosures for the prior six years, required providers to post a notice of their privacy practices, and allowed individuals to file privacy complaints with their providers and health plans.[156] Covered entities are also required to appoint a privacy officer and provide employee HIPAA training.[157]

The expressive effect of HIPAA and its sanctions is likely exacerbated because of the legitimately sacrosanct nature of medical

150. FORRESTER RESEARCH, *supra* note 140.

151. *Id.*

152. Bill Elmore, *Life Before HIPAA*, TECH DECISION MAKER (Sep. 25, 2006, 10:04 PM), http://www.techrepublic.com/blog/tech-decision-maker/life-before-hipaa.

153. *Fact Sheet 8a: HIPAA Basics: Medical Privacy in the Electronic Age*, PRIVACY RIGHTS CLEARINGHOUSE (revised Feb. 2013), https://www.privacyrights.org/HIPAA-basics-medical-privacy-electronic-age.

154. *Id.*

155. *Id.* Previously, approximately half the states had laws mandating personal access to one's medical records.

156. *Id.*

157. *Id.*

privacy. Hippocrates first described the doctor-patient confidentiality standard unique to medicine: "All that may come to my knowledge in the exercise of my profession . . . which ought not to be spread abroad, I will keep secret and will never reveal."[158] Similarly, the "Principles of Medical Ethics" from the American Medical Association, of which the code version—Code of Medical Ethics—is the "authoritative ethics guide for practicing physicians,"[159] incorporates confidentiality concerns in Section IV, which declares that "[a] physician shall respect the rights of patients, . . . and shall safeguard patient confidences and privacy."[160] Violation of this confidentiality, even if too limited in scope to trigger HIPAA's penalties, can lead to patient embarrassment, social isolation, or health-related discrimination.[161]

Furthermore, with the increase of health information technology, an infringement of medical privacy can have far-reaching effects.[162] The traditional physician control of patient data is simply no longer realistic; today, medical care involves coordination and assistance from multiple services or organizations and often includes multiple non-physician parties.[163] PHI is obtained and processed by employees of the health care system and maintained in electronic format. "The expanding number of those whose jobs provide them with access to medical information increases the risk that individuals will act outside the scope of authorization to obtain information they

158. Moore et al., *supra* note 38, at 219–20.

159. *History of AMA Ethics*, AMERICAN MEDICAL ASSOCIATION, http://www.ama-assn.org/ama/pub/about-ama/our-history/history-ama-ethics.page? (last visited Oct. 2, 2014).

160. *Principles of Medical Ethics*, AMERICAN MEDICAL ASSOCIATION, http://www.ama-assn.org/ama/pub/physician-resources/medical-ethics/code-medical-ethics/principles-medical-ethics.page (last visited Oct. 2, 2014).

161. *See, e.g.*, Tony Francis, *HIPAA Violation Not a Tort . . . But . . .*, MEDSCAPE (Mar. 8, 2012, 9:59 AM), http://boards.medscape.com/forums/?128@@.2a300761!comment=1 (discussing the various concerns with an "invasion of privacy," such as a HIPAA violation).

162. This is even truer with modern advances in genetic research that may exacerbate potential risks to medical privacy. Potentially, genetic information available in an HIE could create a biological "scarlet letter" for insurance companies looking to exclude more expensive customers and consequently erode the patient-physician relationship or even encourage the patient not to seek care. Paul A. Lombardo, *Genetic Confidentiality: What's the Big Secret?,* 3 U. CHI. L. SCH. ROUNDTABLE 589, 595–96 (1996).

163. *See* Christopher R. Smith, *Somebody's Watching Me: Protecting Patient Privacy in Prescription Health Information,* 36 VT. L. REV. 931, 931 (2012) ("In today's ever-expanding world of internet technology and electronic data transmission, patient disclosure of prescription health information is being distributed to a widening circle of entities and individuals, raising serious patient privacy concerns.").

do not legitimately need to perform their work."[164] Health information available through an electronic database could be accessed by others, some of whom are not involved in the patient-based health care process, and transferred elsewhere almost instantaneously.[165] Electronic storage and transfer of PHI between numerous servers and vendors naturally expose data to privacy breaches,[166] and existing laws on both the federal and state levels provide insufficient compliance protocols.[167]

Nevertheless, PHI in electronic record systems can be protected—really protected, and not simply up to HIPAA compliance standards—if the varying risks are "continuously guarded and routinely observed."[168] Properly guarded data sets are significantly safer than paper-based systems, particularly when considering the proportional types of data breaches reported on the Wall of Shame.[169] Since the Wall's creation, as of July 23, 2014, the total number of patients affected by all major breaches was 32,150,360.[170] Forty-eight percent of those breaches arose from theft incidents; eighteen percent were related to unauthorized PHI access; eleven percent stemmed from PHI loss; eight percent of incidents overall were linked to hacking; and only three percent of incidents involved electronic health records.[171] This data suggest at least two things: (1) most data breaches occur because "thieves are not after the information in the laptop, but they're after the laptop," as acknowledged by OCR Senior Health Information Privacy Specialist Rachel Seeger; and (2) the majority of HIPAA breaches could be prevented by putting and storing data *into* electronic form.[172] These numbers reveal that some basic employee training—

164. Moore et al., *supra* note 38, at 225–26.

165. *Id*. at 226.

166. Laura Dunlop, *Electronic Health Records: Interoperability Challenges Patients' Right to Privacy*, 3 SHIDLER J. L. COM. & TECH. 16, ¶ 7 (2007), *available at* http://digital.law.washington.edu/dspace-law/bitstream/handle/1773.1/400/vo13_no4_art16.pdf?sequence=1.

167. Christiansen, *supra* note 146, at 22–24.

168. Moore et al., *supra* note 38, at 227.

169. WALL OF SHAME, *supra* note 72.

170. *HIPAA & Breach Enforcement Statistics for August 2014*, MELAMEDIA, http://www.melamedia.com/HIPAA.Stats.home.html (last visited Oct. 2, 2014)

171. McCormack, *supra* note 138.

172. The five biggest breaches since reporting began on September 1, 2013, reaffirm this conclusion because they are all theft- or loss-related: (1) TRICARE Management Activity, 4,901,432 individuals affected when a military health care provider's business associate "lost"

including encryption, complicated password creation, and theft avoidance techniques—could have prevented the vast majority of major HIPAA violations (i.e., those affecting more than five hundred patient records).[173]

Though hacking occurrences are far from insignificant or impossible,[174] this data reveal that in large measure, breaches are not due to unscrupulous individuals and human error. Hiring an IT team could, in many instances, either prevent hacking incidents entirely or minimize the damage should such hacking occur.

## IV. HIE CREATION AND CHALLENGES TO IMPLEMENTATION

The culture that HIPAA has generated works at cross purposes to the statute's goals of not only protecting privacy but also facilitating cost- and health-effective care through information sharing. Instant sharing of PHI through an HIE between providers—a way to instantaneously transmit patient records without excess delay or cost to any party—has doubtlessly been hindered by HIPAA culture despite widely acknowledged benefits of such information sharing. There is very little disagreement that widespread HIE infrastructure has huge benefits—particularly in terms of cost saving and enhanced patient care—as evidenced by successful HIE implementation in other countries.[175] Admittedly, there are challenges in HIE-building (e.g., making the organizations self-sustainable, securing technological adoption across multiple organizations, adequately protecting PHI, etc.), but the greatest

backup tapes (or they were stolen); (2) Advocate Health Care, over four million affected when four unencrypted computers were stolen; (3) Health Net, Inc., 1,900,000 affected when a business associate misplaced nine servers; (4) NYC Health and Hospitals Corporation's North Bronx Healthcare Network, 1,700,000 affected when unencrypted backup tapes were stolen from a business associate's van; (5) AvMed, Inc, 1,220,000 affected when two laptops were stolen from the facility—the encrypted laptop was recovered and the unencrypted laptop was not. *Id.*

173. *Id.*

174. On the "Wall of Shame," there are forty-four incidents citing "hacking" as the type of breach. Of those forty-four incidents, three involved more than one million potential PHI breaches: 156,000 at the Ankle & Foot Center in Tampa, FL, in 2010; 231,400 at Seacoast Radiology, PA, in 2012; and 780,000 at the Utah Department of Health in 2012. Five breaches exposed 10,000 to 100,000 patient records; ten breaches exposed 5,000 to 10,000 patient records, sixteen breaches exposed 1,000 to 5,000 patient records; and ten breaches exposed 500 to 1,000 patient records. WALL OF SHAME, *supra* note 72.

175. Ariele Yaffee, *Financing the Pulp to Digital Phenomenon*, 7 J. HEALTH & BIOMEDICAL L. 325, 332–33 (2011).

concern by far has been related to medical privacy. In fact, PHI is more secure in an HIE than it ever could be in paper format. The experience of implementing the Houston HIE demonstrates the effects of HIPAA culture: A PHI-sharing paranoia so extensive that, even when presented with a cost-saving, enhanced-care-providing, and PHI-protective solution, the medical community is hesitant to enter a data-exchange system.

### *A. HIEs: Background, Benefits, and Challenges*

An HIE is a "connecting point for an organized, standardized process of data exchange across statewide, regional, [or] local initiatives,"[176] through which electronic health records can be transferred to the appropriate health care provider or organization at the patient's arrival or check-in.[177] HIEs have been vigorously supported by George W. Bush, who in 2004 called for their widespread implementation and use within ten years,[178] as well as "by the Obama Administration as a 'key element' of innovation strategy."[179]

The benefits of HIE systems are widely acknowledged[180] and

176. Health Information Exchange (HIE) Overview, HEALTH IT (updated 2014), http://www.tmhp.com/Pages/HealthIT/HIT_HIE.aspx.

177. Electronic health record, or "EHR," is widely used interchangeably with "EMR" or "electronic medical record" even though the latter technically refers to a computerized patient record maintained within one single healthcare entity. An EMR, by contrast, is made nationally available regardless of patient location. *See* Dunlop, *supra* note 166, ¶¶ 3–4.

178. Kelly Cronin, *Office of the National Coordinator for Health Information Technology* 3, DEP'T HEALTH AND HUMAN SERVS., http://www.deadiversion.usdoj.gov/ecomm/e_rx/mtgs/july2006/kcroninpp.pdf (last visited Oct. 2, 2014).

179. Leslie P. Francis, *When Patients Interact with EHRs: Problems of Privacy and Confidentiality*, 12 HOUS. J. HEALTH L. & POL'Y 171, 171 (2012) (citing THE WHITE HOUSE, CONSUMER DATA PRIVACY IN A NETWORKED WORLD: A FRAMEWORK FOR PROTECTING PRIVACY AND PROMOTING INNOVATION IN THE GLOBAL DIGITAL ECONOMY 20 (2012), *available at* http://www.whitehouse.gov/sites/default/files/privacy-final.pdf).

180. For example, the United States Department of Veterans Affairs (VA) became the best medical provider in the nation in less than a decade, in large part because of its adoption of a comprehensive EMR infrastructure, which provides one hundred percent patient record availability throughout the VA and Department of Defense treatment facilities nationwide (163 hospitals, 800 clinics, and 135 nursing homes, total). The VA EMR system's computerized provider order entry decreased rates of adverse drug events as well as increased prescription accuracy rates to nearly one hundred percent—a remarkable feat, particularly compared to the national error rate of three to eight percent. The system also provides the highest quality of care in the United States for almost any condition as a result of data tracking, and despite national price inflation, VA costs have stabilized—"which is largely attributed to eliminated repetitive lab tests and paperwork." Sao, *supra* note 146, at 55–56.

have been realized in other countries that have enacted similar medical systems.[181] This section will provide a brief overview of some of the significant benefits of HIEs, including healthcare cost reduction and improved medical care through greater patient involvement and enhanced patient tracking.

Administrative healthcare costs represent approximately thirty-one percent of the total healthcare costs in the United States.[182] These administrative costs are approximately thirty to seventy percent higher than in countries equipped with similar mixed private-public health systems.[183] Using electronic health records may result in "$77.8 to $162 billion in cost savings per year in the U.S. by streamlining administrative procedures and eliminating redundant diagnostic tests and paperwork."[184] It seems that data exchange through an HIE would result in even greater savings.

HIE implementation also accelerates information transfer from one provider to another[185] and, as a result, greatly reduces redundant diagnostic testing or paperwork performed as a result of unavailable patient history.[186] HIE implementation provides instant access to a patient's entire medical history, which allows uninterrupted patient treatment[187] through enhanced portability and simultaneous access

181. Yaffee, *supra* note 175. Several other countries have created a nationwide electronic health record infrastructure with reportedly great success. Sao et al., *supra* note 146, at 80–83. Many industrialized nations have widespread HIE infrastructure, with approximately 80% to 100% of healthcare providers utilizing such systems. Yaffee, *supra* note 175, at 332–33. In these countries, including Denmark, New Zealand, and Sweden, communications and electronic health records sharing extend far past single healthcare entities; patient data is appropriately shared among numerous providers to optimize patient health. Sao et al., *supra* note 146, at 55–56. *See* Bradford Gray et al., *Electronic Health Records: An International Perspective on "Meaningful Use"*, 28 COMMONWEALTH FUND 1 (2011), *available at* http://www.commonwealthfund.Org/~/media/Files/Publications/Issue%20Brief/2011/Nov/1565-Gray_electronic_med_records_meaning_use_intl_brief.pdf; Steve Arnold et. al., *Electronic Health Records: A Global Perspective* 5 (2007), http://www.himss.org/content/files/DrArnold20011207EISPresentation WhitePape.

182. LUCIEN WULSIN & ADAM DOUGHERTY, HEALTH INFORMATION TECHNOLOGY-ELECTRONIC HEALTH RECORDS: A PRIMER 1 (2008), *available at* https:// www.library.ca.gov/crb/08/08-013.pdf.

183. *Id.*

184. Sao et al., *supra* note 146, at 58. *See also* Yaffee, *supra* note 175, at 336 (estimating savings of $81 to $162 billion for implementing EMRs).

185. Yaffee, *supra* note 175, at 335.

186. *Id.* at 334–35.

187. *Id.* This is especially necessary during a medical crisis. For example, VA patients' medical records were immediately available following the New Orleans evacuation during

for multiple users.[188] This can help prevent or eliminate some medical record errors[189] typically found on paper records, including mishandled requests, misfiled information, or mislabeling, as well as medical errors associated with difficulties tracking disease patterns, treatment strategies, and prescription use.[190] Enhancing coordinated care efforts among multiple providers generally leads to better health outcomes for patients,[191] even on a global scale through the burgeoning practice of telemedicine, or the exchange of medical data via electronic means.[192] As electronic health records become more accessible to individual patients (through patient health records), patients will have a personal hand in streamlining their own medical care in scheduling appointments, filling prescriptions, and particularly managing chronic illness and disease.[193] Developed HIEs can help individuals control, supervise, and manage their own healthcare or the healthcare of an ailing child or elderly parent.[194]

The widely acclaimed benefits of HIE enactment are reflected in the increase of health exchanges in the United States.[195] A 2013 survey of almost 200 HIEs[196] revealed that health information exchanges have increased 41% since 2008, and 58% of hospitals were exchanging PHI with outside providers.

Hurricane Katrina. Catherine Arnst, *The Best Medical Care in the U.S.*, BLOOMBERG BUSINESSWEEK, July 16, 2006, at 50, *available at* http://www.businessweek.com/stories/2006-07-16/the-best-medical-care-in-the-u-dot-s-dot.

188. Randolph C. Barrows, Jr. & Paul D. Clayton, *Privacy, Confidentiality, and Electronic Medical Records*, 3 J. AM. MED. INFORMATICS ASS'N 139, 146–147 (1996), *available at* http://www.ncbi.nlm.nih.gov/pmc/articles/PMC116296/pdf/0030139.pdf.

189. Nicolas P. Terry & Leslie P. Francis, *Ensuring the Privacy and Confidentiality of Electronic Health Records*, 2007 U. ILL. L. REV. 681, 683 (2007).

190. *See* Amy M. Jurevic, *When Technology and Health Care Collide: Issues with Electronic Medical Records and Electronic Mail*, 66 UMKC L. REV. 809, 810–11 (1998). *See* Terry & Francis, *supra* note 189, at 683.

191. Terry & Francis, *supra* note 189, at 683.

192. Sao et al., *supra* note 146, at 59.

193. Leslie P. Francis, *When Patients Interact with EHRs: Problems of Privacy and Confidentiality*, 12 HOUS. J. HEALTH L. & POL'Y 171, 175–76 (2012).

194. *See id.* at 175–76, 187.

195. *See* EHEALTH INITIATIVE, RESULTS FROM SURVEY ON HEALTH DATA EXCHANGE 2013, at 1 (2013), *available at* http://www.ehidc.org/resource-center/publications/view_document/333.

196. This number included ninety community-based HIEs, forty-five state HIEs, and fifty (Rule 6.2(a)) healthcare delivery organizations. *Id.*

Despite the benefits, however, providers remain hesitant to participate in HIEs.[197] Another 2013 survey of 119 HIEs found that 74% struggled to become financially sustainable, and 66% lacked sufficient funding.[198] The healthcare community has been reluctant to adopt information systems, and several HIE launches have failed, including in Washington, D.C., Minnesota, the Appalachian region (called CareSpark),[199] Kansas,[200] Tennessee,[201] and California.[202] These HIEs encountered similar barriers to implementation. For example, HIE functionality is dependent on complete interoperability between providers; two or more systems must be willing to share and use data that has been exchanged.[203] This can be technically complex—the variety of existing information systems can obstruct data exchange—but does not present an insurmountable barrier.[204] Similarly, HIE implementation costs are not precisely known but likely high, which can be particularly challenging for smaller practices and hospitals.[205] HIEs have failed for numerous reasons, but PHI security remains the greatest concern for the public[206] despite widespread support of HIEs from healthcare policymakers and legislators.[207]

197. Gregg, *supra* note 18.

198. *Id.*; ROBERT WOOD JOHNSON FOUND., *supra* note 18, at 51.

199. Genevieve Morris, et al., *Query-Based Exchange: Key Factors Influencing Success and Failure*, HEALTHIT.GOV 15 (Sept. 30, 2012) (prepared for the Office of the National Coordinator for Health Information Technology), http://www.healthit.gov/sites/default/files/query_based_exchange_ final.pdf.

200. Anthony Brino, *Kansas HIE to Hand Over Authority to the State*, HEALTHCARE IT NEWS (Sept. 20, 2012), http://www.healthcareitnews.com/news/kansas-hie-hand-over-authority-state.

201. Susan D. Hall, *Tennessee HIE Organization Disbands*, FIERCEHEALTHIT.COM (July 10, 2012), http://www.fiercehealthit.com/story/tennessee-hie-organization-disbands-state-opts-direct-project/2012-07-10.

202. John, *RHIO Failure: CalRHIO Goes Belly-up*, CHILMARK RES. (Jan. 18, 2010), http://www.chilmarkresearch.com/2010/01/18/rhio-failure-calrhio-goes-belly-up/.

203. Gregg, *supra* note 18 (discussing the problems of too few participants, and the likely resulting HIE failure, because "HIEs have to be a community effort").

204. *See* Amar Gupta, *Prescription for Change*, WALL ST. J., *available at* http://online.wsj.com/article/SB122426733527345133.html#printMode (last updated Oct. 20, 2008, 12:01 AM).

205. Yaffee, *supra* note 175, at 349.

206. XEROX 2012, *supra* note 143.

207. Sao et al., *supra* note 146, at 57.

### *B. PHI Security in HIEs*

HHS data suggests that traditional record-storing methods are more prone to data breach than electronic formats and that HIEs increase PHI security. As already discussed, since the Wall of Shame began publicly reporting breaches, 48% of breaches arose from theft incidents, and only 8% of incidents were linked to hacking, and only 3% of incidents involved electronic health record systems.[208] Furthermore, unlike paper records, electronic health record systems automatically monitor and record PHI access, including digital "footprints" marking the viewer's identifying information and the portions viewed of the patient record.[209] Encryption prevents document alteration, and classified-viewer settings can prevent unauthorized users from accessing portions of patient data.[210] Off-site storage technologies and vendors provide an additional layer of data security and virtually eliminate data theft if properly stored.[211] These auditing and restrictive tactics are certainly more secure than file cabinets kept in a locked basement, so long as they are periodically updated, encrypted, and complex-password protected. Indeed, such protective measures are not unlike those successfully used in the finance industry.[212]

208. McCormack, *supra* note 138.

209. Leon Rodriguez, *Privacy, Security, and Electronic Health Records*, HEALTH IT BUZZ (Dec. 12, 2011, 10:24 am), http://www.healthit.gov/buzz-blog/privacy-and-security-of-ehrs/privacy-security-electronic-health-records/ ("[I]f your data is seen by someone who should not see it, federal law requires doctors, hospitals, and other health care providers to notify you of a 'breach' of your health information. This requirement helps patients know if something has gone wrong with the protection of their information and helps keep providers accountable.").

210. *See generally CyberSecurity: 10 Best Practices for the Small Health Care Environment*, HEALTHIT.GOV, http://www.healthit.gov/providers-professionals/cybersecurity (last updated Mar. 28, 2014) (discussing some of the methods of device protection and benefits of encryption).

211. John Haughton, *A Perspective On: Cloud-Based Modular EHRs Offer Advantages for Meaningful Use, HIMSS Transforming Health Through IT*, HIMSS (July 26, 2011), http://www.himss.org/News/NewsDetail.aspx?ItemNumber=4052 (demonstrating that cloud-based storage applications have long-protected sensitive information in various data-sensitive industries).

212. This comparison has been widely explored in other scholarship, including in Sao et al., *supra* note 146, at 64–66. To summarize, a financial institution "regularly stores and transfers personal financial information across state and national borders in electronic form" that is comparatively as secure and effective as HIE solutions. *Id.* The finance industry is similarly complex to the HIPAA privacy regime—complete with analogous state and federal requirements—and just as little understood. Despite legal and regulatory inadequacies, however, the finance industry and consumers have accepted the electronic regulation of

In light of comparatively minor privacy concerns for HIEs, the public and healthcare community's reluctance to support HIE implementation can be explained only by the pervasive HIPAA culture. It seems likely that public education regarding these privacy protections would alleviate these worries. In light of increased security, improved care, and greater patient involvement associated with HIE use, the institutional and publicized HIPAA culture–induced fear of PHI sharing between appropriate providers is both unfounded and illogical. To some degree, that paranoia is understandable: it is a worrisome idea that, even theoretically, hundreds or thousands of hospital employees across an HIE network have ready access to millions of patient records. But patient privacy is not only built into the HIE framework through auditing, restrictive entry, and encryption methods; patient privacy is a fundamental tenant of the Hippocratic Oath[213] and the American Medical Association's "Principles of Medical Ethics."[214] Furthermore, in possibly one of the only universally positive outcomes created from HIPAA culture, any employee who knowingly and inappropriately accesses and uses HIE patient records risks severe civil or even criminal penalties.[215] By discouraging HIE use, HIPAA culture and associated "privacy paranoia" costs the healthcare system billions of dollars and severely hinders comprehensive, superior patient care.

### *C. Case Study in Houston, Texas: Greater Houston Healthconnect*

During the summer of 2012, I worked in Houston for the relatively new HIE Greater Houston Healthconnect. Healthconnect launched in late 2011 after receiving a small HITECH grant from the Texas Department of Health and Human Services.[216] The HIE initially garnered support from sixty hospitals—nearly 80% of area

finances to remain competitive through convenience and adequate IT security. *See id*.

213. *Hippocratic Oath: Modern Version, Bioethics*, JOHN HOPKINS SHERIDAN LIBR., http://guides.library.jhu.edu/content.php?pid=23699&sid=190964 (last updated Aug. 28, 2014).

214. *History of AMA Ethics*, *supra* note 159.

215. Health Insurance Portability and Accountability Act (HIPPA) of 1996, 42 U.S.C. § 1320d-5 (2006).

216. Lora Hines, *Sharing Health Info Vital Yet Lacking: Houston's Healthconnect Electronically Connecting Hospitals and Doctors*, HOUS. CHRON., http://www.houstonchronicle.com/news/article/ Sharing-health-info-vital-yet-lacking-4647463.php (last updated July 4, 2013, 9:09 pm).

hospitals[217]—as well as more than 5,300 local physicians.[218] Currently, the Healthconnect HIE covers 20 counties, 14,000 physicians, 133 hospitals, and 7 million potential patients and expects to be entirely self-sustainable by the end of 2014 through participation fees from all participants—including physician offices, hospitals, and federally qualified health centers, which largely serve Medicaid populations.[219] The Texas Medical Center is the largest medical center in the world with a very high density of clinical facilities for science, research, and patient care.[220] Houston is, theoretically, the ideal HIE location.

In addition to the concentrated medical expertise of the area, HIE implementation should be less complicated in Houston than in most other markets because Houston is an "opt-in" consent system.[221] This means that patients have to consciously "opt-in" to the exchange network, as opposed to most other HIE markets, which automatically enroll patients concurrently with providers and require patients to "opt-out" if desired.[222]

Furthermore, unlike some other HIEs, Greater Houston Healthconnect does not have a centralized data repository, which means patient data is not stored in one large, accessible "vat" maintained by the HIE authority.[223] In many centralized HIE models, the HIE provides central authorities (often a state regulating group) with unique patient identifying information and widespread

217. GREATER HOUSTIN HEALTHCONNECT, PRESS KIT 12 (2013) *available at* http://hietexas.org/component/docman/doc_download/671-ghh-press-kit-october-2013?Itemid=.

218. James Byers, *Health Information Organization Changes Name, Announces New CEO*, BUSINESSWIRE.COM (Jan. 31, 2012, 11:32 am), http://www.businesswire.com/news/home/20120131006346/en/Health-Information-Organization-Announces-CEO#.UyoLLBaRE3E.

219. *fastFACTS*, GREATER HOUSTON HEALTHCONNECT, http://ghhconnect.org/index.html#/fast-facts/ (last visited Nov. 11, 2014).

220. *About TMC,* TEXAS MEDICAL CENTER http://www.texasmedicalcenter.org/about-tmc/ (last visited Oct. 2, 2014).

221. *HIE Objectives*, HIETEXAS, http://hietexas.org/resources/index.php?option=com_content&view=article&id=170&Itemid=310 (last visited Aug. 29, 2014).

222. *See* Madelyn Young, *Joining an HIE or RHIO? Navigate the Opt-In/Opt-Out Decision Carefully*, POWER YOUR PRACTICE, http://www.poweryourpractice.com/medical-practice-resources/joining-an-hie-or-rhio-navigate-the-opt-inopt-out-decision-carefully/ (last visited Sept. 2, 2014).

223. Jennifer Bresnick, *Healthconnect HIE Takes Off in Texas with Vendor, Provider Help*, EHR INTELLIGENCE, May 2, 2013, http://ehrintelligence.com/2013/05/02/healthconnect-hie-takes-off-in-texas-with-vendor-provider-help/.

PHI access, or a theoretical "vat" of PHI.[224] Those with requisite authority can access data at any time.[225] Healthconnect, however, uses a federated model,[226] which means that Healthconnect's software vendor maintains patient data in isolated "silos" to separate patient data between healthcare organizations.[227] This federated HIE model stores PHI in remotely located repositories.[228] This means that, with very limited exceptions, no one person has access to all patient records, and no person can access or download all patient records at once. Members of the Healthconnect HIE can retrieve data through the "query and response" model: member organizations send a "query" to the HIE patient registry, which contains an internal patient information "map" searchable by unique patient identifiers, including social security number, name, and other input options.[229] When the query locates the proper medical record, the HIE returns the record's physical location and can request the patient information from the storing organization.[230] The storing organization can then transmit the data via secure e-mail or other web services.[231] The centralized data repository can be more efficient because it allows a single exchange of information but, by incorporating one extra step, the federated model provides extra PHI protection.[232]

HIE implementation has been surprisingly difficult in Houston, despite its concentration of individuals familiar with the current information system's shortcomings and with the potential for financial growth and improved patient care through a community-wide electronic health record system.[233] Experience demonstrates the pervasive HIPAA culture in Houston—arguably the most medically sophisticated city in the world—is actively hindering best-practice

224. *See HIE Technical Informational Overview*, HIMSS.ORG 7 (March 2011), http://www.himss.org/files/HIMSSorg/content/files/HIMSSHIETechnicalOverview.pdf/.

225. *See id*.

226. *HIE Objectives*, *supra* note 221.

227. *See generally* HIMSS, *supra* note 224.

228. *Id*. at 12–13.

229. *See id*.

230. *Id*.

231. *Id*.

232. *See generally id*.

233. *See About TMC*, *supra* note 220.

medicine in the community, and, by extrapolation, throughout the country.

In May 2013, Greater Houston Healthconnect had only twenty-eight contracts with providers and major health systems[234]—the letters of support from hospitals had, in most cases, not yet become contractual relationships. The only effective data exchange was occurring in far southeast Texas, where a few remote hospital systems had signed up for the HIE.[235] Contracting with remote hospitals is understandably less challenging for HIEs; those hospitals have the most to gain, particularly financially, from a regional HIE.[236]

There are some partial explanations unrelated to HIPAA culture for the Houston medical community's hesitancy to install the HIE, but these reasons cannot alone adequately explain Healthconnect's difficulties. From the sales pitch to going "live," patient data exchanges take six to twelve months or more to implement in larger institutions.[237] Implementation involves technical interface installation, which can take from twelve to twenty weeks depending on the complexity of the already-existing interface.[238] Additionally, Houston is a highly competitive medical market, and it is possible administrators may hesitate to share data because they could lose "customers" when they lose their exclusive technological infrastructure.[239]

Still, neither the technological nor unique competitive challenges adequately explain the level of resistance to community HIE

234. Bresnick, *supra* note 223.

235. Greater Houston Healthconnect, *Expansion of Greater Houston Healthconnect will Enhance Coordination of Care Between Patients and Providers*, HEALTHCARE IT NEWS (Mar. 6, 2012), http://www.healthcareitnews.com/press-release/expansion-greater-houston-healthconnect-will-enhance-coordination-care-between-patient.

236. *Benefits for Critical Access Hospitals and Other Small Rural Hospitals*, HEALTHIT.GOV, http://www.healthit.gov/providers-professionals/benefits-critical-access-hospitals-and-other-small-rural-hospitals (last updated May 14, 2014).

237. Bresnick, *supra* note 223.

238. *Id.*

239. *See, e.g.*, Carrie Feibel, *Why Catholic Hospital Chain Wants in on the Houston Market*, HOUS. PUBLIC MEDIA (April 22, 2013, 3:11 PM), http://www.houstonpublicmedia.org/news/1366643466/ (discussing generally hospital market competition in Houston); Deborah White, *Houston 2011 Market Overview*, HEALTHLEADERS INTERSTUDY, http://hl-isy.com/Products-and-Services/Market-Overviews/Southwest/2011/Houston-TX (last visited Sept. 2, 2014) ("Competition is heating up among leading health systems as they build new hospitals and expand in suburban areas and in the Texas Medical Center, the largest medical complex in the world.").

implementation. The medical community in Houston largely supports the HIE, at least in theory, and prominent professionals acknowledge its potential value,[240] but Healthconnect still receives significant pushback as evidenced by the slow HIE implementation. If healthcare organizations were more willing to sign contracts, IT employees could more easily and more quickly move through the technical execution. Furthermore, if organizational hesitancy were simply due to the particular competitive Medical Center environment, every local federally qualified health center ("FQHC") would have immediately signed up for the HIE. FQHCs are generally underfunded and serve indigent, often uninsured or Medicaid-insured patients—of which there are nearly 900,000 in the greater Houston area[241]—and competition is not a concern. Nor have FQHCs been discouraged by the HIE cost; in early HIE stages, many providers receive steeply discounted prices or even entirely waived fees. Still relatively few FQHCs are participating.[242] Finding an employee within a practice or hospital willing to champion the HIE project is a continual challenge for Healthconnect.

The difficulties associated with the Healthconnect HIE implementation demonstrate the negative side effects of HIPAA culture: a public obsessed with PHI protection even at the expense of better, more efficient, less expensive, more PHI-protective care.[243] Even among a health-educated community, doubtlessly aware of the potential benefits of HIEs,[244] the HIPAA requirements and violation

240. Byers, *supra* note 218.

241. *Final Count—Medicaid Enrollment by County—May 2013*, TEX. HEALTH AND HUMAN SERVICES COMM'N, http://www.hhsc.state.tx.us/research/MedicaidEnrollment/ME/201305.html (last accessed Sept. 2, 2014). Greater Houston Healthconnect serves the Colorado, Wharton, Matagorda, Austin, Fort Bend, Harris, Walker, Brazoria, Galevston, Waller, Montgomery, San Jacinto, Liberty, Chambers, Tyler, Hardin, Jefferson, Jasper, Orange, and Newton counties, *fastFACTS*, *supra* note 219, which, according to that chart, total 896,495 Medicaid enrollees. *Final Count—Medicaid Enrollment by County—May 2013*, TEX. HEALTH AND HUMAN SERVICES COMM'N, http://www.hhsc.state.tx.us/research/MedicaidEnrollment/ME/201305.html (last accessed Sept. 2, 2014).

242. Harris County alone has 30 FQHCs. *Greater Houston HEALTHCONNECT*, HARRIS COUNTY HEALTHCARE ALLIANCE, http://www.hchalliance.org/8-site-pages/146-greater-houston-healthconnect.html (last accessed Sept. 2, 2014). In summer 2012 only two FQHCs were in the final stages of HIE connection, though several others were contracted to connect later. GREATER HOUS. HEALTHCONNECT, http://ghhconnect.org/#/connected-providers—-physicians-and-community-health-providers/ (last accessed Sept. 2, 2014).

243. *See, e.g.*, Sao et al., *supra* note 146, at 64–66.

244. *See About TMC*, *supra* note 220.

penalties have educated both patients and providers to resist data-sharing. The negative effects of this HIPAA culture are arguably worsened in a medically saturated market and are hindering best patient care practices.

### *D. Possible Solutions*

Although suggesting fixes for the perception and education problems relating to HIPAA culture privacy paranoia would require a separate article, the very nature of HIE operations demonstrates how solutions could potentially be realized.

As previously discussed, HIEs "have to be a community effort."[245] Many individual hospitals and medical practices utilize their own electronic health record system but are unable to exchange with providers outside that system without a common health information exchange—thereby severely limiting the benefits of hosting electronic data.[246] To provide the best patient care, providers must "'be able to look at the whole [healthcare] community and see every place the patient has been seen' to be able to devise the best course of action for the patient's care."[247] This includes a treating physician's ability to instantaneously extract cumulative patient data and create a treatment plan.[248]

The only way to implement HIEs and create this continuum of patient care is through mass enrollment.[249] More participating providers will drive down the overall cost of participation and increase the value of enrollment through greater quantities of potentially exchanged patient data.[250] Greater enrollment must be encouraged through a whole community effort to reeducate physicians and the general public regarding PHI protection.

Given the unlikelihood of successful legislative reform and in light of the significant benefits of HIEs, a better understanding of

245. Gregg, *supra* note 18.

246. *See, e.g.*, *id.* ("[The Tennessee HIE OnePartner is] a physician-owned HIE that connects more than 700 regional physicians from 14 physician practices. [Individual] practices use a variety of electronic health record platforms and are affiliated with different hospitals, but they are able to find and share patient information on the common exchange.").

247. *Id.*

248. *Id.*

249. *Id.* ("'HIEs are expensive . . . If you're trying to make one for a group of less than 200 or 250 doctors, it's probably prohibitively expensive.'").

250. *Id.*

PHI protection and the increased safety of HIEs over other PHI storage methods would substantially curb HIPAA culture. Widespread enactment of basic privacy training[251]—including encryption, complicated password creation, and theft avoidance techniques—could effectively protect PHI, comply with HIPAA requirements, and encourage increased HIE implementation.[252] Because of the expressive effect of the statute and its sanctions, the best way to effectively counter HIPAA culture without re-writing the statute itself is to contrast that PHI-sharing phobia with educational efforts highlighting the increased protections and advantages of PHI storage and sharing within HIEs.

## V. CONCLUSION

The expressive effects of the HIPAA statute and the associated HHS regulations have resulted in HIPAA culture: a public educated only in privacy paranoia at the cost of better health care. HIPAA culture is associated with hindered patient care, a "compliance" over "PHI protection" mindset among healthcare entities, and millions, if not billions, of lost dollars from repeated tests, wasted administrative time, and poor patient tracking. Given this current mentality, the challenges associated with the Houston HIE implementation are hardly surprising. Though Houston has every indication of potential HIE success—a more protective, federated storage model; a more medically sophisticated population; widespread spoken, if not enacted, support; and an "opt-in" consent requirement—HIPAA culture has significantly slowed HIE enactment and has thereby harmed patient care, both in Houston and, by extrapolation, nationwide.

*Jessica Jardine Wilkes**

251. The statute already requires employee training but does not include recommendations regarding encryption, password complexity, or other basic privacy measures. 45 C.F.R. § 164.530(b), (e) (2013) ("A covered entity must train all members of its workforce on the policies and procedures with respect to protected health information required by this subpart and subpart D of this part, as necessary and appropriate for the members of the workforce to carry out their functions within the covered entity.").

252. *See* McCormack, *supra* note 136.

* J.D., April 2014, J. Reuben Clark Law School, Brigham Young University.