Volume 27 | Issue 1
FALL 2017

LOYOLA UNIVERSITY CHICAGO
AD • MAJOREM • DEI • GLORIAM
1870
SCHOOL *of* LAW

BEAZLEY INSTITUTE FOR HEALTH LAW AND POLICY

Annals OF Health Law

ADVANCE DIRECTIVE

The Student Health Policy and Law Review of
LOYOLA UNIVERSITY CHICAGO SCHOOL *of* LAW

ANNALS OF HEALTH LAW
Advance Directive

THE *STUDENT* HEALTH POLICY AND LAW REVIEW OF
LOYOLA UNIVERSITY CHICAGO SCHOOL OF LAW

BRINGING YOU THE LATEST DEVELOPMENTS IN HEALTH LAW

Beazley Institute for Health Law and Policy

VOLUME 27, STUDENT ISSUE 1 FALL 2017

CONTENTS

ANNALS OF HEALTH LAW
Advance Directive

Editor's Note

The *Annals of Health Law* is proud to present the Nineteenth issue of our online, student-written publication, *Advance Directive*. As has become tradition, this Issue features articles that correspond with our Eleventh Annual Symposium on Health Law & Policy presented by the Beazley Institute for Health Law and Policy and *Annals of Health Law*: 'Privacy, Big Data and the Demands of Providing Quality Patient Care.'

Issues of privacy arise when information is both sensitive or private enough for interested parties to demand privacy and yet valuable or useful enough for others to want or need access. Health information is a classic example. Many categories of health information are considered private—disclosure of health information may open a patient up to anything from public embarrassment to insurance, employment, and other discriminations turning on his or her health status. At the same time health information has incredible value, beyond the patient and his or her doctor. The large volume of information gathered by hospitals and other health care facilities has attracted the attention of Big Data, particularly as electronic medical record systems and network connectivity make the consolidation, transmission, and analysis of this information a viable goal.

However, the law has taken steps to protect patient privacy in some, but not all, circumstances. In the United States especially, health technologies and patient privacy are regulated by a dizzying array of statutes, regulations, and administrative agencies at both the federal and state level. Our authors therefore examine a variety of issues related to the rise of technology and "big data," as well as efforts to increase access, efficiency, and quality and the challenges of security and privacy of patient information.

The Issue begins by looking at the protection of health information at the federal and state level, and examining the way existing regulatory mechanisms could be extended to encourage better safeguards to patient privacy. First, we examine whether the Supreme Court's holding in *National Federation of Independent Business v. Sebelius* creates grounds to tax entities who fail to encrypt sensitive health information. Second, we analyze Illinois' existing privacy protections for stigmatizing health information, and how these might be extended to allow individuals a private cause of action if their information is disclosed. Finally, our authors dig into the provisions of the Health Insurance Portability and Accountability Act ("HIPAA") Privacy Rule to argue for interpretation that is both flexible with regard to information sharing, even as patient information is protected.

The Issue then turns to the matter of emerging technologies in the healthcare space. The technological and digital health market has grown exponentially in the past five years, fueled by the development of network connectivity, increased mobile device adoption, and Big Data investment. Yet technologies like direct-to-consumer genomics, cloud computing, and the use of targeted advertising in healthcare raise issues of patient privacy, quality of care, and liability. Our authors delve deeply into the way these technologies have developed, drawing attention to the role law and regulation have attempted to address such concerns.

Finally, the Issue concludes by examining the interplay between vulnerable populations and the protection or utilization of health information. The stigmas of mental illness can prevent patients from being forthcoming with providers, and receiving necessary care—particularly if patients are aware that psychotherapist-patient privilege is not absolute. However, our authors argue that existing case law provides a balance between fairness and protecting the patient's privacy.

Second, we examine similar concerns surrounding undocumented immigrants receiving health care, particularly as it relates to the implications for treating providers. The issue then concludes with a discussion of privacy during public health crises, examining the need for a more robust right to privacy through the lens of the 2014 Ebola Virus outbreak.

We would like to thank Jordan Donnelly, our Technical Production Editor, because without his knowledge and commitment this Issue would not have been possible. We would like to give special thanks to our *Annals* Editor-in-Chief, Adrienne Testa, for her leadership and support. The Annals Executive Board Members, Christine Bulgozdi and Lauren Batterham, and the Annals Senior Editors, Alex Thompson, Kevin Pasciak, and Lauren Park provided additional invaluable editorial assistance with this Issue. The *Annals* members deserve special recognition for their thoughtful and topical articles and for editing the work of their peers. Lastly, we must thank the Beazley Institute for Health Law and Policy and our faculty advisors, Professor Lawrence Singer, Megan Bess, and Kristin Finn for their guidance and support.

We hope you enjoy our nineteenth issue of *Advance Directive*.

Sincerely,

Sarah Gregory
Advance Directive Editor
Annals of Health Law
Loyola University Chicago School of Law

Collin Rosenbaum
Advance Directive Editor
Annals of Health Law
Loyola University Chicago School of Law

Taxing Covered Entities Who Opt to Not Encrypt ePHI in the Wake of *National Federation of Independent Business v. Sebelius*

Derek Springer

Data breaches are becoming increasingly common in the healthcare industry, with the number of Health Information Privacy Complaints under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") nearly tripling from 2004 to 2015.[1] Part of the reason for this increase in Health Information Privacy Complaints is that the estimated value of an individual's health information is approximately ten dollars, which is ten to twenty times the value of that same individual's credit card number.[2] Another reason complaints are on the rise is that the 2009 Health Information Technology for Economic and Clinical Health Act ("HITECH") implemented a new requirement for covered entities[3] to notify individuals whe n their health information is breached.[4] The most effective way for covered entities to protect sensitive electronic personal health information ("ePHI") is to encrypt sensitive user data.[5] This is not a complete shield

1. Health Information Privacy Complaints Received by Calendar Year, U.S. DEP'T HEALTH & HUMAN SERVS. (Oct. 13, 2016), http://www.hhs.gov/ocr/privacy/hipaa/enforcement/data/complaintsyear.html [https://perma.cc/48AJ-WP4B].

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

3. Covered entities are defined in the HIPAA rules as (1) health plans, (2) health care clearinghouses, and (3) health care providers who electronically transmit any health information in connection with transactions for which HHS has adopted standards.

4. See generally, 45 C.F.R. §§ 164.400-414 (2014).

5. Elizabeth Snell, *Breaking Down HIPAA: Health Data Encryption Requirements*, HEALTH IT SECURITY, https://healthitsecurity.com/news/breaking-down-hipaa-health-data-encryption-requirements (last visited Oct. 8, 2017).

against data breaches[6], as hackers may still use malware that enables them to break through a covered entity's database security. However, encryption is a significant step towards data security.[7]

Perhaps because encryption capabilities at the time of HIPAA's passage in 1996 were not as advanced as they are today, the Security Rule of HIPAA chose to make encryption an addressable implementation specification, as opposed to a mandatory specification.[8] Encryption must be implemented under the addressable implementation standard only if the covered entity decides after conducting a risk assessment that encryption is appropriate in order to safeguard the confidentiality of their ePHI.[9] If the entity decides that encryption is not reasonable and appropriate, it can document that determination and implement an equivalent alternative measure.[10]

Many covered entities confuse the security rule's "addressable"

---

6. *Id*. at 3.

7. *Id.*

8. *See generally*, Health Insurance Accountability and Portability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (codified in scattered sections of 42 U.S.C.) [hereinafter HIPAA]. "HIPAA" also usually refers to the Privacy, Security, Enforcement and Breach Notification Rules promulgated by the Department of Health and Human Services. *Id.* The effectiveness and availability of encryption technology has changed dramatically since HIPAA was originally drafted in 1996. *Id. See also* Barry Shelton & Chris Johnson, *A Brief History of Encryption*, TECH NEWS WORLD (July 19, 2010), http://www.technewsworld.com/story/70437.html. In 1996 data encryption could be achieved by using a Data Encryption Standard (DES) 56-bit algorithm developed by IBM in the 1970's. DES was not nearly as secure as the modern AES standard used today. The modern AES standard supports 128-, 192-, and 256-bit keys in contrast to the relatively short 56-bit DES key. The length of these keys means that brute-force attacks are infeasible, at least for the foreseeable future. *Id. See also* 45 C.F.R. § 164.312(a)(2)(iv); 45 C.F.R § 164.312.(e)(2)(ii).

9. *Is the use of encryption mandatory in the Security Rule?,* U.S. DEP'T HEALTH & HUMAN SERVS., https://www.hhs.gov/hipaa/for-professionals/faq/2001/is-the-use-of-encryption-mandatory-in-the-security-rule/index.html; *see Summary of the HIPAA Security Rule,* U.S. DEP'T HEALTH & HUM. SERVS., https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html. If the standard can otherwise be met, the covered entity may choose not to utilize the implementation specification and then document the rationale for this decision. The Security Rule does not dictate which security measure to use, but does require the covered entity to consider multiple factors, including: the entity's size, software infrastructure, the cost of security measures, and the likelihood of possible impact of potential risks to ePHI. *Id.*

10. *Id*.

encryption provision as being "optional."[11] In 2015, Anthem Inc., the largest U.S. health insurance company, was hacked in a data breach that compromised approximately 80 million people's ePHI.[12] Prior to the breach, Anthem decided to not to encrypt their consumers' ePHI.[13] Experts analyzing the breach say doing so could have prevented the breach.[14]

This article will demonstrate that under the precedent established in *National Federation of Independent Business v. Sebelius* ("*NFIB*"), the federal government could impose a tax on covered entities for failing to encrypt their ePHI.[15] By imposing a federal tax on covered entities that choose not to encrypt their ePHI, the federal government could encourage the encryption of ePHI without arbitrarily making encryption mandatory, which could have the unwanted effect of disadvantaging smaller entities. Such a tax would encourage covered entities to encrypt their ePHI whilst simultaneously raising revenue. In order to prove that this is the best road ahead, Part I of this article will analyze the holding and precedent established by *NFIB*, with a particular eye toward distinguishing the holding in *NFIB* from the Supreme Court's past jurisprudence and precedential taxing and spending cases such as *Bailey v. Drexel Furniture Co*.[16] Next, Part II will discuss private rights of action, the already established route for private citizens to recover for breaches at the state level, and determine whether this could serve as a model for federal regulation. Lastly, Part III will discuss ongoing attempts to pass mandatory data encryption legislation at the federal level and the problems with this proposed legislation, with a particular focus on the legislation

11. Theresa Defino, Lauren Clason, & Jill Brown, *HIPAA and Encryption: 'Addressable' Does Not Mean 'Optional',* 16 REPORT ON PATIENT PRIVACY 8, 8 (2016).

12. Danny Yadron & Melinda Beck, *Health Insurer Anthem Didn't Encrypt Data in Theft,* THE WALL STREET J. (Feb. 5, 2015, 7:26 PM), https://www.wsj.com/articles/investigators-eye-china-in-anthem-hack-1423167560.

13. *Id*.

14. *Id*.

15. Nat'l. Fed'n. of Indep. Bus. v. Sebelius*,* 567 U.S. 519, 539 (2012) [hereinafter *NFIB*].

16. Bailey v. Drexel Furniture Co., 259 U.S. 20, 37 (1922).

drafted by Illinois Representative Bobby Rush in 2015.

I. NATIONAL FEDERATION OF INDEPENDENT BUSINESSES V. SEBELIUS

NFIB held that the provision in the Patient Protection and Affordable Care Act ("ACA") that imposed a penalty on individuals who did not purchase health care was constitutional under the taxing and spending power granted to Congress by the U.S. Constitution.[17] One aspect of the Court's opinion that was controversial was the Court's holding that the ACA's requirement that certain individuals pay a financial penalty for not obtaining health insurance may reasonably be characterized as a tax.[18] Writing for the Court, Chief Justice Roberts reasoned that "[t]he Federal Government does not have the power to *order people* to buy health insurance. . .[but] The Federal Government *does* have the power to *impose a tax* on those without health insurance."[19] Chief Justice Roberts qualified the Court's reasoning by explaining that Congress's power to legislate under the taxing and spending power is very broad.[20] However, Congress's authority under the taxing and spending clause is limited to requiring an individual to pay money into the Federal Treasury.[21] If a tax is properly paid the federal government will not possess the authority to compel or punish individuals subject to the tax.[22]

17. *NFIB*, 567 U.S. at 575; *see also* U.S. CONST. art. I, § 8, cl. 1 (granting Congress the taxing and spending power).

18. *Id*. at 574. Chief Justice Roberts, held that: 1) Anti–Injunction Act did not bar pre-enforcement suit, abrogating *Liberty Univ., Inc. v. Geithner*, 671 F.3d 391; 2) the individual mandate, imposing minimum essential coverage requirement under which certain individuals must purchase and maintain health insurance coverage, exceeded Congress's power under Commerce Clause, abrogating *Thomas More Law Center v. Obama*, 651 F.3d 529, and *Seven–Sky v. Holder*, 661 F.3d 1; 3) the individual mandate was a "tax" that was within Congress's taxing powers; 4) the statutory provision giving Secretary of Health and Human Services (HHS) the authority to penalize States that chose not to participate in Act's expansion of Medicaid program exceeded Congress's power under the Spending Clause; and 5) the penalization provision was severable.

19. *Id*. at 575.

20. *Id*. at 584.

21. *Id.* at 574.

22. *Id.* (pointing out this out not to make light of the severe burden that taxation imposes, but rather to show that a tax leaves an individual with a lawful choice to do or not do a certain act, so long as he is willing to pay a tax levied on that choice.)

Thus, it would be permissible for an individual to pay money into the Federal Treasury in lieu of purchasing mandated health insurance under the ACA.[23] There may be circumstances wherein an individual would rather pay money into the Federal Treasury than purchase health insurance.[24]

The joint dissent in *NFIB* takes direct issue with the majority opinion's classification of the "penalty" in the individual mandate as a "tax."[25] Specifically, Justice Scalia's dissent draws attention to the Court's precedent distinguishing a tax from a penalty, citing that "[a] tax is an enforced contribution to provide for the support of government; a penalty. . .is an exaction imposed by statute as punishment for an unlawful act."[26] Furthermore, the dissent argues that there are structural limits upon federal power, and that the individual mandate threatens the structure of the established constitutional order because *all* private conduct (including failure to act) becomes subject to federal control, effectively destroying the Constitution's division of governmental powers.[27]

Similar to *NFIB*, the Government is in danger of overstepping the Constitution's division of governmental powers by regulating a covered entities failure to act by forcing covered entities to encrypt their ePHI.[28] The current formulation of the "addressable" implementation specification of the

---

23. *Id.*

24. *Id.* Since the penalty is not an exceedingly heavy burden, it was deemed that the penalty was not obviously designed to regulate behavior otherwise beyond federal authority. *Id.*

25. *Id*. at 662 (Scalia, Kennedy, Thomas, and Alito JJ., dissenting).

26. *Id*. (Scalia, Kennedy, Thomas, and Alito JJ., dissenting) (arguing that there is a clear line between a tax and a penalty and that "to say that the Individual Mandate merely imposes a tax is not to interpret the statute but to rewrite it." They also point out that the mandate is referred to as a "penalty" throughout the Act and that the mandate and penalty are located in Title I of the Act, it's operative core, not Title IX, which contains the Act's "Revenue Provisions.")

27. *Id*. at 658 (Scalia, Kennedy, Thomas, and Alito JJ., dissenting) (responding to Justice Ginsburg's argument that Congress needs only a "rational basis" for concluding that the regulated activity substantially affects commerce. Justice Ginsburg argues that the Mandate should be authorized on the basis of the commerce power, not the taxing and spending power)

28. *Id.* (Scalia, Kennedy, Thomas, and Alito JJ., dissenting).

Security Rule of HIPAA does not provide any economic incentive for covered entities to encrypt their ePHI.[29] In truth, the current form of the addressable implementation specification may provide incentive for covered entities to proceed *without* encrypting their data, as many business leaders are willing to risk a large-scale breach in an attempt to reduce overhead by choosing not to encrypt their ePHI.[30] As the law is currently written, the Office for Civil Rights ("OCR") within the U.S. Department of Health and Human Services has the responsibility of enforcing the Privacy and Security Rules with voluntary compliance activities and civil money penalties.[31]

Yet, unlike individuals without health insurance in *NFIB*, covered entities are already in the market and have already consented to being regulated by the OCR.[32] If federal legislation was passed which penalized covered entities for failing to encrypt ePHI, it could be found to be within the taxing and spending power of the federal government as it was articulated in *NFIB.*[33] Extrapolating Chief Justice Roberts's logic throughout *NFIB* and applying it to the HIPAA Security Rule as it applies to covered entities*,* it could be inferred that the federal government *does not* have the power to *order* covered entities to encrypt ePHI.[34] This is because mandatory encryption may lead to an economic situation that disfavors smaller covered entities by forcing entities with relatively little amounts of ePHI to spend exorbitant amounts of money on data encryption.[35] The federal government *does*, however, have the power to impose a tax on covered entities that fail to

29. *See generally supra* note 8.

30. See What is the Difference Between Addressable and Required Implementation Specifications in the Security Rule?, U.S. DEP'T HEALTH & HUMAN SERVS., http://www.hhs.gov/ocr/privacy/hipaa/faq/securityrule/2020.html [https://perma.cc/8QYJ-QEF8] (last reviewed July 26, 2013).

31. U.S. DEP'T HEALTH & HUMAN SERVS., *supra* note 9.

32. *Id*.

33. *See generally, NFIB*, 567 U.S. at 519 et seq.

34. *Id.*

35. *Id*. The high cost of setting up an infrastructure for encryption could be seen as such a heavy burden as to be prohibitive, effectively regulating these smaller entities out of the market. This is discussed at length in Part II of this article.

encrypt their ePHI.[36]

II. DISTINGUISHING NFIB FROM BAILEY V. DREXEL FURNITURE

In *NFIB,* Chief Justice Roberts distinguishes the "tax" in the ACA from the "penalty" in *Bailey v. Drexel Furniture.*[37] In *Drexel Furniture,* the so-called tax on employing child laborers imposed an exceedingly heavy burden—10 percent of a company's net income—on those who employed children.[38] The "penalty" in *Drexel Furniture* was enforced primarily by the Department of Labor, which was the agency responsible for punishing violations of labor laws, not collecting revenue.[39]

The shared responsibility payment contained in the ACA substantially differed from this "penalty" in *Drexel Furniture*.[40] By statute, the tax in the ACA could never be more than the price of insurance.[41] Therefore, it may be a reasonable financial decision to pay the tax rather than purchase insurance, unlike the "prohibitory" financial punishment in *Drexel Furniture*.[42] Furthermore, the Internal Revenue Service ("IRS") collects the payment in the ACA through the normal means of taxation.[43] Thus, the IRS is not allowed to use those means most suggestive of a punitive sanction, such as criminal prosecution.[44] Additionally, the payment is intended to affect

36. *Id*.
37. *Id*. at 566.
38. *Id*. at 565.
39. *Id*.
40. *Id*. ("The payment is not so high that there is really no choice but to buy health insurance; the payment is not limited to willful violations, as penalties for unlawful acts often are; and the payment is collected solely through the IRS through the normal means of taxation.").
41. *Id*. ("In 2016, for example, the penalty will be 2.5 percent of an individual's household income, but no less than $695 and no more than the average yearly premium for insurance that covers 60 percent of the cost of 10 specified services (*e.g.* prescription drugs and hospitalization).").
42. *Id*.; Drexel Furniture Co., 259 U.S. at 36 (reasoning that "there comes a time in the extension of the penalizing features of the so-called tax when it loses its character as such and becomes a mere penalty, with the characteristics of regulation and punishment").
43. *NFIB*, 567 U.S. at 565.
44. *Id.* (noting that in addition, "some individuals who are subject to the mandate are

individual conduct and raise considerable revenue at the same time.[45] Chief Justice Roberts analogizes the individual mandate in *NFIB* to the excise tax on cigarettes, noting that federal and state taxes may compose more than half the retail price of a carton of cigarettes to not only raise more money but also to encourage individuals to quit smoking.[46]

A federal tax on covered entities that make the decision to not encrypt their ePHI would have similar positive effects. Not only would such a tax encourage covered entities to encrypt their ePHI, but it would do so while also providing an alternative for covered entities that cannot encrypt their ePHI in an economically feasible manner whilst simultaneously raising revenue.[47] As data breaches become more frequent and more devastating, it is imperative that the government deals with the issue now. As the Security Rule in HIPAA is currently written, abuses of its implementation specifications are rampant and detracting from the effectiveness of the Security Rule as a whole.[48] A legislative deterrent should ideally be enacted as soon as possible and Chief Justice Roberts' discussion of the individual mandate in *NFIB* provides a great framework as to how such a deterrent can be constitutionally enacted. Many of the problems that the dissent in *NFIB* found with the majority opinion are resolved by the fact that covered entities are already in the market and accordingly subject to regulation.[49] Although private rights of action can provide relief for aggrieved individuals at the state

---

nonetheless exempt from the penalty-for example, those with income below a certain threshold and members of Indian tribes.")

45. *Id*. at 567.

46. *Id*.; *see also* Drexel Furniture Co., 259 U.S. at 36 (explaining that with a commodity or other thing of value the Court "may not be permitted under previous decisions of [the] court to infer solely from its heavy burden that the act intends a prohibition instead of a tax").

47. "Economically feasible" in this context means implementing a tax that would encourage encryption without levying arbitrary penalties, which, as discussed throughout, would place smaller covered entities at a disadvantage and might even force them out of the market.

48. Yadron & Beck, *supra* note 12.

49. *NFIB,* 567 U.S. at 539.

level, a broader regulatory scheme is necessary at the federal level. A tax collected by the IRS from covered entities that choose not to encrypt their ePHI would be an ideal regulatory scheme. By taxing covered entities a percentage of their revenue, such a tax would encourage encryption while not disproportionately affecting smaller covered entities.

III. PRIVATE RIGHTS OF ACTION

Before moving forward with a complex tax bill or a legislative solution, the first question to be considered is whether to create a private right of action under HIPAA. Private rights of action are an important part of many administrative schemes.[50] Although these actions are brought on behalf of a particular individual, that individual acts as a "private attorney general" that serves to vindicate the public interest.[51] As such, they function as an additional enforcement tool while preserving administrative resources.[52] Often, private actions are expressly provided by statute.[53]

A major point of contention over the years is the permissibility of "implied" private rights of action.[54] In general, the Supreme Court has stopped the process of implying private rights of action from a statutory scheme.[55] Instead, the Court now looks for explicit Congressional intent before recognizing a private right of action in a regulatory scheme.[56] Thus, the Court's current jurisprudence stipulates that if Congress did not intend a private right of action then the courts may not imply such a right into the scheme at issue.[57] This is a sharp break with a line of cases that permitted the

50. 7 WESTS'S FED. ADMIN. PRAC. § 8061 (2017).
51. 7 WESTS'S FED. ADMIN. PRAC, *supra* note 50, at § 8061.
52. *Id.*
53. *Id.*
54. *Id.*
55. *Id.*
56. *Id.*
57. Transamerica Mortgage Providers, Inc. v. Lewis 444 U.S. 11, 15 (1979).

implication of private rights of action to further the administrative scheme.[58] For instance, in *Bivens v. Six Unknown Named Agents of Federal Bureau of Narcotics* ("*Bivens*"), the Court ruled that an implied right of action existed for an individual whose Fourth Amendment right of freedom from unreasonable search and seizures was violated by the Federal Bureau of Narcotics.[59] The Court reasoned that Bivens could sue for the violation of the Fourth Amendment itself despite the lack of any federal statute authorizing such a suit.[60] The Court further reasoned that the existence of a remedy for the violation was implied by the importance of the right violated.[61]

In recent years, the Court broke with *Bivens's* precedent and considers the finding of private rights of action where they are not expressly created by Congress to be judicial overreach.[62] Under the current interpretation, Congress must create a private right of action under federal law.[63] HIPAA does not contain an express provision creating a private right of action[64] or any express language conferring privacy rights upon a specific class of individuals.[65] However, HIPAA does assign enforcement of the statute to the Secretary of Health and Human Services.[66] Since Congress specifically delegates the enforcement of HIPAA to the Secretary of Health and Human Services, there is a strong indication that Congress intended to preclude private enforcement.[67] This is because the express provision of one method of enforcing (i.e., a statute) suggests Congress intended to preclude others.[68]

---

58. *See* Cort v. Ash, 422 U.S. 66, 95 (1975).
59. Bivens v. Six Unknown Named Agents of Federal Bureau of Narcotics, 403 U.S. 388, 397 (U.S. 1971).
60. *Bivens*, 403 U.S. at 397.
61. *Id.* at 395.
62. Acara v. Banks, 470 F.3d 569, 571 (2006).
63. *Acara*, 470 F.3d at 571.
64. *Id*.
65. *Id*.
66. *Id*.
67. Alexander v. Sandoval, 532 U.S. 275, 286–87 (2001).
68. *Alexander*, 532 U.S. at 286–87.

Nonetheless, some states, such as Connecticut, have their own privacy laws.[69] HIPAA and its associated regulations do not preempt such claims under state common law.[70] Furthermore, HIPAA and its regulations may inform the standard of care applicable to such claims.[71] A seminal case that held that HIPAA does not preempt state level claims of negligence against insurance companies was the Connecticut case of *Byrne v. Avery Ctr. for Obstetrics & Gynecology* ("*Byrne*").[72] The plaintiff in *Byrne* did not assert a claim for relief premised solely on a violation of HIPAA.[73] Rather, the plaintiff relied on the proposition that common law negligence actions coupled with HIPAA informing the standard of care may complement rather than obstruct HIPAA for preemption purposes.[74]

The fact that private rights of action now exist for privacy breaches at the state level lends further credence to the notion that enforcement mechanisms must evolve at the federal level. For example, the Supreme Court in *Ziglar v. Abbasi* outlines policy reasons for declining to imply private rights of action in federal statutes.[75] The Court in *Ziglar* reasoned that the limited reach of a *Bivens* action informs the determination of whether an implied damages remedy should be recognized.[76] Congress' failure to provide a damages remedy might be more than mere oversight and its silence more than inadvertent.[77] The Court determined in *Ziglar* that Congressional silence is relevant and telling in a scenario where Congress had nearly 16 years to extend the kind of remedies sought by the respondents.[78] Indeed, the policy

69. *See* Byrne v. Avery Ctr. for Obstetrics & Gynecology, 314 Conn. 433, 435 (Conn. 2014).
70. *Byrne*, 314 Conn. At 435.
71. *Id*.
72. *Id.*
73. *Id*. at 445.
74. *Id*.
75. *See generally* Ziglar v. Abbasi, 137 S.Ct. 1843, 1856 (U.S. 2017).
76. *Ziglar*, 137 S.Ct. at 1848.
77. *Id*. at 1849.
78. *Id*.

reason for the Court deferring to the legislature by not implying private rights of action in federal statutes is well supported by state and federal jurisprudence, which discourages judges "legislating from the bench."[79] In regards to HIPAA's Security Rule, the Court further reasoned that Congress declined to extend the kind of remedies sought by the respondents in *Ziglar* by not amending HIPAA to create a private right of action.[80] However, as data breaches and the negligent handling of ePHI by covered entities become more common, the case for a legislative remedy, such as the tax in *NFIB*, against covered entities that fail to encrypt their ePHI continues to gain strength.[81]

IV. ATTEMPTS TO PASS LEGISLATION MAKING DATA ENCRYPTION MANDATORY

While the Supreme Court has developed further jurisprudence regarding taxes and private rights of action, some members of Congress have realized the substantial risks of data breaches in the modern technological age and the value of data encryption. In particular, Illinois Democratic Representative Bobby Rush has been at the forefront of the attempt to pass legislation to reform the HIPAA Security Rule, with one recent attempt coming in the 114th Congress in January of 2015.[82] The Data Accountability and Trust Act ("DATA") proposed to authorize the Federal Trade Commission ("FTC") to promulgate regulations requiring each covered entity engaged in interstate commerce that possesses data containing personal information to establish specified security policies to protect ePHI.[83] Resultantly, according to the DATA, if ePHI is encrypted there shall be a presumption that no reasonable

79. Schweiker v. Chilicky, 487 U.S. 412, 423.
80. Yadron & Beck, *supra* note8.
81. U.S. DEP'T. HEALTH & HUMAN SERVS. *supra* note 1.
82. *See generally* Data Accountability and Trust Act, H.R. 580, 114th Cong. (2015).
83. Data Accountability and Trust Act, *supra* note 82, at § 2.

risk of unlawful conduct exists.[84] The DATA further stipulated that any such presumption might be rebutted by facts demonstrating that the encryption is unlikely to be effective.[85] The DATA mandated that covered entities that violated the act would face liability and be subject to a civil penalty.[86] Finally, under the DATA there would be a maximum total liability of five million dollars for all violations resulting from a single breach of security.[87]

Although Representative Rush's DATA would certainly be a step forward in the realm of data security, there are several facets of ePHI storage that it fails to address. First of all, Representative Rush's bill does not exempt small companies with a low amount of ePHI stored from prohibitive penalties.[88] If his bill were to pass, an insurance company with 15 employees would be expected to meet the same encryption requirements as Anthem with 53,000 employees.[89] Resultantly, that small company would then have to pay potentially catastrophic fines if it failed to meet the DATA's lofty standards.[90] These considerations demonstrate why a tax based on a percentage of a covered entity's revenue is a strong alternative to a civil penalty. Similarly to the Court's reasoning in *Drexel Furniture* that the Department of Labor's proposed tax would be so excessive as to regulate child labor out of existence, the DATA would impose a civil penalty so significant as to make data encryption mandatory, and thus would run the risk of regulating small holders of ePHI out of existence.

Although mandatory data encryption would be a noble undertaking, doing so at the expense of small businesses is not within Congress's interests.

---

84. *Id* at § 3.
85. *Id.*
86. *Id* at § 4. (The penalty would be calculated by multiplying the number of days that the covered entity failed to be in compliance with such section by an amount not greater than eleven thousand dollars.)
87. *Id.*
88. *Id*. at § 3.
89. *Id.*
90. *Id.*

While an exemption could be written into the HIPAA for covered entities that retain less than a statutorily mandated amount of ePHI, it would be more prudent to encourage these smaller companies to securely store data as well. By creating a tax such as 1 percent of revenue per year for entities that choose not to encrypt their ePHI, with that percentage increasing depending on the amount of time an entity chooses not to encrypt their data, Congress would be able to encourage compliance whilst allowing small businesses to forego mandatory encryption in favor of paying the tax. Furthermore, by allowing the IRS to collect this tax, the United States would be able to raise revenue while simultaneously encouraging safe data storage policy.

V. CONCLUSION

Although allowing the FTC to impose mandatory encryption by exacting civil penalties may be a more palatable avenue for legislation, it is clear that the long-term benefits to small business in combination with the possibility of raising revenue makes legislating a tax based off the ruling in *NFIB* a better strategy. Such a tax would not preempt state action, but would provide incentive for businesses to lower their exposure to legislation such as that in *Byrne*. As data security breaches continue to grow, the federal government must act now to ebb the tide of costly litigation whilst preserving an environment of healthy economic competition.

Owning Your Privacy: Why Illinois Should Extend Private Causes of Action to Improper Disclosures of Other Stigmatizing Health Information

Kaleigh Ward

I. INTRODUCTION

Though the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule ensures protected health information (PHI) is not used or disclosed without prior patient authorization,[1] it does not provide patients whose information has been improperly used or disclosed with a private remedy.[2] The only remedy for patients available under HIPAA states that individuals can file a complaint with the Secretary of Health and Human Services through the Office for Civil Rights if they suspect a covered entity has violated the HIPAA Privacy Rule. The Secretary has discretion to investigate or impose fines upon that entity, but the individual harmed is left with no recourse.[3]

However, some laws at the state level provide individuals with private remedies to ensure that patients are awarded damages for improper disclosures of their protected health information.[4] Several Illinois statutes provide patients with a private cause of action for improper disclosures of particularly stigmatizing health information, such as information related to

1. 45 C.F.R. § 164.512(a) (2002).
2. Spencer v. Roche, 755 F. Supp. 2d 250, 271 (2010).
3. 45 C.F.R. § 160.306 (2013); Spencer v. Roche, 755 F. Supp. 2d, at 271.
4. Daniel Oates, *HIPAA Hypocrisy and the Case for Enforcing Federal Privacy Standards Under State Law,* 30 SEATTLE U. L. REV. 745, 763 (2007).

HIV/AIDS and mental health diagnoses.[5] Because Illinois has set a more stringent precedent for protecting stigmatizing health information than the federal government,[6] Illinois should also extend private remedies to cases involving disclosures of other stigmatizing health information, namely, of an individual's Sexually Transmissible Disease infection status. The Sexually Transmissible Disease Control Act (STDCA) already extends privacy provisions beyond the level required by the HIPAA Privacy Rule,[7] but it could be amended to better serve the individuals it protects. Specifically, the STDCA could allow for a private cause of action that mirrors that of the AIDS Confidentiality Act,[8] with numbers adjusted to account for the difference in stigma associated with STD infection, rather than HIV infection. Additionally, in order to ensure the STDCA maintains its goals of extending public health protections,[9] it could be amended to extend exceptions to confidentiality in cases where there is a suspected risk of STD infection with potentially fatal consequences. In addressing these proposed amendments, we will first examine the Health Insurance Portability and Accountability Act of 1996, and then, we will briefly examine individual remedies available at the state level for disclosures of stigmatizing health information.

II. HEALTH INSURANCE PORTABILITY & ACCOUNTABILITY ACT OF 1996

When HIPAA was signed into law on August 21, 1996, the underlying goal was to address the impact that advances in information technology

5. Stephen Weiser, *Sixth Annual Health Law & Policy Colloquium: Diagnosing the Data, December 5, 2006: Transcribed Speech of Stephen Weiser, J.D., L.L.M.*, 16 ANN. HEALTH L. 341, 342-51 (2007); Ill. Found. for Quality Health Care, *Appendix 6 – Confidentiality Protections in Illinois* (2003), http://www.idph.state.il.us/hispc2/resources/Appendix6-Confidentiality.pdf.

6. Weiser, *supra* note 5.

7. 410 ILL. COMP. STAT. § 325/8 (2017).

8. 410 ILL. COMP. STAT. § 305/13 (2017).

9. 410 ILL. COMP. STAT. § 325/2 (2017).

would have on the health care industry.[10] Adding to the new regulations under HIPAA, in 2000, the Department of Health and Human Services issued its final "Standards for Privacy of Individually Identifiable Health Information" (HIPAA Privacy Rule), with which covered entities were expected to comply by April 14, 2003.[11] The HIPAA Privacy Rule set a national standard for an individual's rights to privacy and confidentiality in their health information.[12] HIPAA's privacy provisions state that covered entities may not use or disclose a person's PHI except as permitted or required by the regulations.[13] PHI includes all individually identifiable health information that is maintained or transmitted in any form, including oral statements about medical conditions or treatments.[14] Covered entities under HIPAA include health plans, health clearinghouses, and health care providers that transmit health information electronically in connection with certain transactions.[15] Additionally, the HIPAA Privacy Rule has been extended to business associates of covered entities, so that they must now also comply with The Privacy Rule.[16] Some of the most common permissible uses and disclosures include using or disclosing PHI for treatment, payment, and health care operations.[17] Covered entities may also disclose PHI without a patient's prior authorization in response to a court order, provided that the PHI disclosed does not exceed the bounds of what was expressly required in that order.[18] However, without an applicable exception, HIPAA generally prohibits the use and disclosure of PHI without a patient's prior consent.[19]

---

10. Grace Ko, *Partial Preemption Under the Health Insurance Portability and Accountability Act*, 79 S. SAL. L. REV. 497, 497 (2006).
11. *Id.* at 500.
12. 45 C.F.R. §164.534 (2001); *see also* Ko, *supra* note 10, at 498.
13. 45 C.F.R. § 164.512(a) (2002).
14. 45 C.F.R. § 160.103 (2013).
15. 45 C.F.R. §160.102 (2013).
16. *Id.*; 45 C.F.R. §160.102 (2013).
17. 45 C.F.R. § 160.103 (2013).
18. 45 C.F.R. § 164.512(e)(1)(i) (2002).
19. 45 C.F.R. § 164.508(a) (2002).

Though HIPAA protects an individual's PHI from improper use and disclosure, it provides little in the way of personal remedy for violations of the HIPAA Privacy Rule.[20] The HIPAA Privacy Rule does not give individuals the right to sue.[21] Instead, they must file a complaint with the Secretary of Health and Human Services through the Office for Civil Rights if they suspect a covered entity or business associate is not in compliance.[22] The Secretary has discretion to determine which complaints to further investigate and does so by conducting compliance reviews.[23] HIPAA provides exclusive authority to enforce its provisions with the Department of Health and Human Services (HHS), and any violations of its provisions may result in HHS's imposition of civil penalties or criminal charges.[24] The Office of Civil Rights can impose civil penalties for non-willful, unknowing HIPAA violations ranging from $100 to $50,000 per violation, and at least $50,000 per violation for infringements arising out of willful neglect.[25] Criminal penalties for knowingly disclosing PHI can result in up to 10 years imprisonment and $250,000 in fines.[26] Though a covered entity may face strict penalties for a HIPAA Privacy Rule violation, the individual whose information was improperly used or disclosed is left with no personal remedy or compensation under the federal statutes.

Though HIPAA generally preempts state law under the Supremacy Clause of the United States Constitution,[27] HIPAA contains a preemption exception

20. 45 C.F.R. § 160.306 (2013).
21. *Id.*; Spencer v. Roche, 755 F. Supp. 2d 250, 271 (2010).
22. 45 C.F.R. § 160.306 (2013); Spencer, 755 F. Supp. 2d at 271.
23. 45 C.F.R. § 160.306 (2013); Spencer, 755 F. Supp. 2d at 271.
24. Sconiers v. Cal. Dep't of Soc. Servs., 2007 U.S. Dist LEXIS 95169 1, 11 (2008).
25. 45 C.F.R. § 160.404(b)(2) (2016); Robert Miller & Tegan Schlatter, *Can This Information Be Disclosed? Navigating the Intricacies of HIPAA in Claims Litigation*, 40 THE BRIEF 32, 33 (2011).
26. 42 U.S.C. § 1320d-6 (2009); *see also* Miller & Schlatter, *supra* note 25, at 33.
27. U.S. CONST. art. VI, cl. 2 (establishing that federal law is the supreme law of the land, and further, that if federal and state laws conflict, the federal law must govern, with state law acting as subordinate to the supreme law of the land).

for states that impose higher standards than HIPAA.[28] This exception makes it possible for individuals to raise private causes of action under state law, when available.[29] Specifically, the HIPAA preemption provision allows for state law to preempt HIPAA in certain situations, including when "the provision of State law relates to the privacy of individually identifiable health information and is more stringent than a standard, requirement, or implementation specification adopted under subpart E of part 165 of this subchapter."[30] To fall under this exception, the state law must be contrary to HIPAA, relate to the privacy of PHI, and be more stringent than federal law.[31] In other words, if the state law provides greater privacy protections for the subject of the information than would be available under HIPAA, the state law could preempt an analogous protection under HIPAA.[32] While this provision might make compliance with all applicable regulations more burdensome, it is arguably more favorable to individual subjects of PHI, who may find greater remedies for disclosures of particularly harmful or stigmatizing health information at the state level.[33]

III. PRIVACY IN ILLINOIS

In Illinois, individuals are protected by numerous privacy laws that are more stringent than the HIPAA Privacy Rule, and some of these state laws allow for individuals to raise a private cause of action when their protected health information has been disclosed improperly.[34] Specifically, Illinois law

28. 45 C.F.R. § 160.203(b) (2002); Daniel Oates, *HIPAA Hypocrisy and the Case for Enforcing Federal Privacy Standards Under State Law,* 30 SEATTLE U. L. REV. 745, 763 (2007).

29. Oates, *supra* note 28.

30. 45 C.F.R. § 160.203(b) (2002).

31. *Id*.

32. Ko, *supra* note 10, at 504-05 (explaining that the HIPAA Privacy Rule "constitutes a federal floor of protection rather than a ceiling").

33. *Id.* at 505-06 (describing the main challenges facing covered entities are the obstacles of compliance).

34. Weiser, *supra* note 5.

allows for private causes of action when there has been a prohibited disclosure under the Illinois Insurance Information and Privacy Protection Act, the Mental Health and Developmental Disabilities Confidentiality Act, and the AIDS Confidentiality Act.[35]

While these laws are important in the protections they extend and the remedies they provide, similar remedies need to be available for improper disclosures of other stigmatizing health information, namely sexually transmissible disease (STD) infection. While separate state laws in Illinois specifically protect all three of these areas of health information, private causes of action only exist at the state level for two of these and it does not include improper disclosures of STD infection information.

Most people are unlikely to agree on the level of privacy desired in one's own health information. While some desire complete privacy of all personal data and strict control over who has access to their health information and for what purposes, others see little problem with sharing their health information more freely. However, it can be reasonably assumed that there is more consensus on the desirability of protecting particularly stigmatizing health information from disclosure without prior consent. For example, exposing an embarrassing disease or a mental illness could lead to stigmatization in a variety of ways, both spoken and unspoken.[36] While one could argue that the codification and separation of stigmatizing health conditions further alienates groups affected by such stigma, without the option of a private cause of action for violating the privacy involved in such health information at the state level, those harmed may be left with little recourse for the damage they've incurred.[37]

---

35. *Id.* at 351; Ill. Found. for Quality Health Care, *Appendix 6 – Confidentiality Protections in Illinois* (2003), http://www.idph.state.il.us/hispc2/resources/Appendix6-Confidentiality.pdf.

36. John Hill et al., *Bottom-Up or Top-Down? Removing the Privacy Law Obstacles to Healthcare Reform in the National Healthcare Crisis,* 84 IND. L.J.SUPP. 23, 35 (2009).

37. Miller & Schlatter, *supra* note 25, at 33-34 (listing the remedies that may be available

IV. MENTAL HEALTH PROTECTIONS

The Mental Health and Developmental Disabilities Confidentiality Act (MHDDCA) was enacted with the objective of restricting non-consensual disclosure of mental health records and communications.[38] Specifically, the MHDDCA protects records and communications that concern a recipient of mental health services.[39] Even the fact that a person is a recipient of mental health services is protected under the MHDDCA.[40] This statute has been said to have been enacted to encourage those in need of mental health services to seek treatment and to "prohibit the unduly prejudicial, inflammatory, or stigmatizing use of mental health records."[41] The MHDDCA includes a number of exceptions where disclosure without consent is permitted, including for instance, in cases when a patient's mental condition is "at issue" in a legal proceeding.[42]

Like HIPAA provisions, the MHDDCA allows for non-consensual disclosures of protected mental health information to integrated systems for coordination and management of health care services.[43] It also has extended an exception to the consent requirement, akin to the HIPAA exception, for de-identified records.[44] However, unlike HIPAA, the MHDDCA provides that any person harmed by violation of the MHDDCA can sue for "damages, an injunction, or other appropriate relief.[45] Reasonable attorney's fees and costs may be awarded to the successful plaintiff in any action under this

---

for improper disclosure of PHI).

38. 740 ILL. COMP. STAT § 110/3 (2017); Elinor Hart, *The Illinois Mental Health and Developmental Disabilities Confidentiality Act: Lest We Forget the Search for the Truth,* 41 LOY. U. CHI. L.J. 885, 885 (2010).

39. Hart, *supra* note 38, at 900-01.

40. *Id.* at 900.

41. *Id.* at 937.

42. *Id*. at 892 (meaning the patient's mental condition was central to the dispute being decided, it was directly "at issue").

43. W. Eugene Basanta et al., *Survey of Illinois Law: Health Care Law,* 37 S. ILL. U.L.J. 787, 806 (2013).

44. *Id.* at 807.

45. 740 ILL. COMP. STAT. § 110/15 (2017).

Act."[46] Furthermore, "any person who knowingly and willfully violates the MHDDCA will be guilty of a Class A misdemeanor."[47] The Illinois legislature allows for personal recovery when specific, sensitive health information has been improperly disclosed for purposes outside those that are legally permissible.

V. HIV/AIDS PROTECTIONS

Unlike the HIPAA Privacy Rule, individuals specifically have the right to a private cause of action in Illinois for violation of the AIDS Confidentiality Act (ACA).[48] Specifically, any person harmed under the ACA can recover the following for each violation: for negligent violations, a person may recover liquidated damages of $2,000 or actual damages, whichever is greater, and for intentional or reckless violations a person may recover liquidated damages of $10,000 or actual damages, whichever is greater, plus reasonable attorney fees, and any other relief the court may deem appropriate, including an injunction.[49] In interpreting this statute, the courts have found that punitive damages are not an available remedy under the ACA, reasoning that the statute does not mention this type of damages and that they are generally disfavored at law.[50]

The ACA provides protections and damages that are unavailable to injured parties under HIPAA and at common law.[51] In enacting these protections, the Illinois legislature was motivated to provide additional protections that would promote and ensure the confidentiality of HIV testing.[52] For instance, physicians cannot administer an HIV test without also providing information

46. *Id.*
47. 740 ILL. COMP. STAT. § 110/16 (2017).
48. 410 ILL. COMP. STAT. § 305/13 (2017); Doe v. Chand, 335 Ill. App. 3d 809, 817 (2002).
49. 410 ILL. COMP. STAT. § 305/13 (2017).
50. Doe, 335 Ill. App. 3d at 817.
51. *Id.*
52. *Id.* at 818.

about the meaning of the results, availability of additional testing and of referrals for counseling or further information.[53] Additionally, the ACA prohibits any person from disclosing the identity of anyone who has submitted to an HIV test, and it similarly bars anyone from disclosing the results of another's test that has been revealed to them.[54] Other heightened protections include the requirement that informed consent be provided using a coded system, unlinking the identity of an individual with his or her test result.[55]

Interestingly, when an individual fraudulently alters the results of his or her own HIV test with the intention of releasing those results to a third party, the protections of the ACA no longer apply.[56] Additionally, the ACA does not provide a cause of action for a law enforcement officer who requests a suspect's HIV test results, as may be the case after an arrest where blood was exposed.[57]

VI. STD PROTECTIONS

In enacting the Illinois Sexually Transmissible Disease Control Act (STDCA), the General Assembly was interested in protecting public health from a rising incidence of STDs, which can cause a serious and at times fatal threat to public and individual health.[58] However, at the same time, the General Assembly noted that these diseases, "by their nature, involve sensitive issues of privacy," and intended that "all programs designed to deal

53. 410 ILL. COMP. STAT. 305/5 (2017); Doe v. Chand, 335 Ill. App. 3d at 817.
54. 410 ILL. COMP. STAT. 305/9 (2017); 410 ILL. COMP. STAT. 305/10 (2017).
55. 410 ILL. COMP. STAT. 305/6 (2017); Doe v. Chand, 335 Ill. App. 3d at 817.
56. Glasco v. Marony, 347 Ill. App. 3d 1069, 1075 (2004).
57. Bitner v. Perkin Mem'l Hosp., 317 Ill. App. 3d 935, 938 (2000) (reasoning that while the ACA intends to protect the confidentiality of HIV test results so the public will not be deterred from engaging in testing, the Act does not require that a law enforcement officer receive a suspect's test results. An exception within the act only authorizes disclosure of the results to a law enforcement officer that may have been infected with HIV by a suspect.).
58. 410 ILL. COMP. STAT. § 325/2 (2017).

with these diseases afford patients privacy, confidentiality and dignity."[59] Additionally, the General Assembly noted that it "intends to provide a program that is sufficiently flexible to meet emerging needs, that deals efficiently and effectively with reducing the incidence of sexually transmissible diseases, and provides patients with a secure knowledge that information they provide will remain private and confidential."[60]

Among other things, the STDCA requires that health care providers treating individuals with STDs and labs performing tests for STDs must report the results within two weeks.[61] The STDCA also requires that all records and information held by the Department of Health and its representatives relating to STDs are kept confidential and exempt from inspection and copying under the Freedom of Information Act.[62] Such disclosures of information are also prohibited in court or before any tribunal, board, or agency without the consent of the subject of the information, unless such information is presented statistically and made unidentifiable.[63] Disclosures are also permitted if they are made to medical personnel, state agencies or courts in order to enforce the Act and related rules or when made to persons determined to have been at potential risk of HIV transmission.[64]

While the STDCA protects individuals from having another class of stigmatizing health information revealed without their consent, there is no personal remedy available for someone whose STD infection information has been improperly exposed.[65] Under the STDCA, someone who maliciously or knowingly spreads information about any disease under this act is guilty of a Class A misdemeanor.[66] Additionally, violating other provisions of this Act,

59. *Id.*
60. *Id.*
61. 410 ILL. COMP. STAT. § 325/4 (2017).
62. 410 ILL. COMP. STAT. § 325/8 (2017).
63. *Id.*
64. *Id.*
65. *Id.*
66. 410 ILL. COMP. STAT. § 325/5.5 (2017); 410 ILL. COMP. STAT. § 325/8 (2017).

such as reporting requirements, can also result in Department of Health fines of up to $500 for each violation.[67]

VII. PROPOSED AMENDMENT TO THE STDCA

Though the stigma associated with most STDs is not as severe or as historically significant as the stigma associated with HIV infection, this health information is sensitive and stigmatizing nonetheless, as is reflected in the language of the Act.[68] Because the Act is intended to both protect public health and protect patient privacy in matters that are particularly sensitive and stigmatizing, a two-part amendment to the Act should be proposed that would further both causes.[69] First, in order to extend public health protections, the STDCA could extend its exception to the confidentiality provision that applies in cases of suspected risk of HIV infection to cases of suspected STD infection that carry potentially fatal consequences. Stated differently, the STDCA could allow for disclosures of STD infection, which would otherwise be protected health information under this Act, when there is sufficient reason to believe that a patient has been exposed to an STD that carries potentially fatal consequences, if left untreated. This would allow the government to carry out its goals of protecting the public health and safety in situations when a threat of harm outweighs the need for patient privacy. Second, in order to protect the privacy of stigmatizing health information, the STDCA could be amended to allow for a private cause of action mirroring that of the ACA, but with numbers adjusted to account for the difference in stigma associated with STD infection versus that associated with HIV infection. For instance, for negligent violations of the STDCA, a person could recover liquidated damages of $1,000 or actual damages, whichever is greater, and for intentional or reckless violations a person could recover

67. 410 ILL. COMP. STAT. § 325/4 (2017).
68. 410 ILL. COMP. STAT. § 325/2 (2017).
69. *Id.*

liquidated damages of $5,000 or actual damages, whichever is greater, plus reasonable attorney fees and any other relief the court may deem appropriate.

Potential counterarguments to extending a private cause of action to the STDCA may include concerns about frivolous cases and/or large numbers of such suits. One could argue that, because of the mountain of privacy laws governing health care providers, it is quite easy to find a health care provider in violation of patient privacy, especially in cases of heightened privacy requirements, such as those governing mental health diagnoses, HIV/AIDS infection, and STD infection.[70] In instances like these heightened areas of patient privacy protections, where the risk of violation would necessarily be higher, some may feel the net effect on a person whose privacy has been violated may be small, and is thus unnecessary to protect with a private cause of action. So, in balancing the interests at stake, allowing individuals harmed under this Act to recover personally for improper uses and disclosures of their STD infection status could open the courts up to larger numbers of cases where people are seeking to benefit financially from something that amounts to embarrassment.

While these concerns are not without merit, the Illinois General Assembly has deemed mental health diagnoses and HIV/AIDS to be sufficiently stigmatizing so as to allow for a private cause of action for a violation of the acts that protect these particular health concerns.[71] It does not seem unrealistic to imagine that accidental disclosure of STD test results to a patient's employer, partner, or parent, could also have damaging consequences. And while the stigma associated with STD infection may not amount to the same stigma associated with severe mental illness or to HIV/AIDS infection, the proposed remedy could account for that difference in lowering the available damages to appropriately account for the severity

70. 410 ILL. COMP. STAT. § 305/13 (2017); 410 ILL. COMP. STAT. § 325/2 (2017); 740 ILL. COMP. STAT. § 110/15 (2017).

71. 410 ILL. COMP. STAT. § 305/13 (2017); 740 ILL. COMP. STAT. § 110/15 (2017).

of the disclosure. Furthermore, it seems only appropriate that a patient whose STD infection information has been shared without their knowledge or consent should be able to recover for the resulting harm or injury to their reputation or otherwise, rather than the state recovering that sum.

Another possible counterargument arises from the fact that one of the General Assembly's main stated goals in enacting the STDCA was to protect the public health from the growing rate of STD infection.[72] The argument could be raised that the government has a greater interest in using regulatory compliance to protect the public from infectious disease than it does in preserving a victim's right to profit. However, in the same paragraph that outlined the rising rate of STD infection, the Illinois General Assembly stated the importance of preserving patient privacy in sensitive health information.[73] The proposed amendments to the STDCA would allow for both protection of public health in allowing health care providers to ignore the heightened confidentiality requirements in cases of suspected infection of a disease with fatal consequences, while also allowing those who have been personally harmed by improper disclosures some amount of restitution for the damages they have suffered.

VIII. CONCLUSION

While there are many interests to be balanced in enacting privacy regulations concerning health information, the privacy interests of the individuals whose information is the subject of such regulation cannot be denied. Violations of the HIPAA Privacy Rule carry significant penalties, including fines in the hundreds of thousands of dollars per violation and prison sentences of up to 10 years, and the federal legislation does not allow for individuals whose privacy has been violated to recover for improper

72. 410 ILL. COMP. STAT. § 325/2 (2017).
73. *Id.*

disclosure of their personal information.[74] In order to recover for violations of private health information, individuals must seek redress under available state laws.[75]

While Illinois has admirably sought to protect individuals against improper disclosures of particularly stigmatizing health information, it has limited the availability of private causes of action to only few such statutes, such as the ACA and the MHDDCA.[76] As the State of Illinois has already recognized that personal damages are appropriate in cases of disclosing stigmatizing health information without a subject's consent, the State should extend the same remedy to other legislation that similarly protects against disclosing stigmatizing health information. Namely, Illinois should provide a private cause of action under the Sexually Transmissible Disease Control Act, while adding an exception to non-consensual disclosure in cases of suspected exposure to potentially fatal STDs. In doing this, the State could extend its intended public health protections while having a more consistent approach to providing equitable remedies for persons whose sensitive health information has been disclosed without their consent and without statutory authority.

74. 42 U.S.C. § 1320d-5 (2017); Miller & Schlatter, *supra* note 25, at 33.

75. Oates, *supra* note 28, at 763.

76. Weiser, *supra* note 5, at 351; Ill. Found. for Quality Health Care, *Appendix 6 – Confidentiality Protections in Illinois* (2003), http://www.idph.state.il.us/hispc2/resources/Appendix6-Confidentiality.pdf.

Is This Really Over? 45 C.F.R. § 164.506(c)(4) and Determining When the Physician-Patient Relationship Ends

Allyson N. Thompson

I. INTRODUCTION

In 1996, the United States Congress enacted the Health Insurance Portability and Accountability Act ("HIPAA").[1] In 1999, the United States Department of Health and Human Services ("HHS") released a proposed rule after Congress failed to enact privacy legislation prior to HIPAA's three-year deadline.[2] The final regulation, known as the HIPAA Privacy Rule, was codified in 2000 at 45 C.F.R. § 160-164.[3] The HIPAA Privacy Rule strives to protect individuals' health information through national standards governing covered entities and their business associates.[4] Generally, HIPAA defines protected health information ("PHI") as individually identifiable health information "transmitted by electronic media, maintained in electronic

1. *Summary of the HIPAA Privacy Rule*, U.S. Dept. of Health & Human Servs., https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html.
2. *Id*.
3. Health Insurance Portability and Accountability Act (1996), P. Law 104-191, 110 Stat. 1936.; HIPAA Privacy Rule, 45 C.F.R. § 160, 164.
4. *Covered Entities and Business Associates*, U.S. DEPT. OF HEALTH & HUMAN SERVS., https://www.hhs.gov/hipaa/for-professionals/covered-entities/index.html (last visited June 16, 2017) (defining "covered entities" as certain health care providers, health plans, health care clearinghouses); *Business Associates*, U.S. DEPT. OF HEALTH & HUMAN SERVS., https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/business-associates/index.html (last updated July 26, 2013) (defining "business associate" as "a person or entity [not a member of the covered entity's workforce] that performs certain functions or activities that involve the use or disclosure of protected health information on behalf of, or provides services to, a covered entity").

media, or transmitted or maintained in any other form or medium."[5] However, HIPAA exempts certain types of individually identifiable health information from this definition.[6] Furthermore, although HIPAA generally prohibits disclosure of PHI without patient consent, it provides several exceptions to this ban, including an exception for uses and disclosures of PHI for the purpose of treatment, payment, and health care operations ("TPO").[7]

HHS created this exception for TPO uses and disclosures out of perceived necessity to ensure "individual's access to quality health care or the efficient payment for such health care."[8] One such exception, 45 C.F.R. § 164.506(c)(4), allows covered entities to use and disclose a patient's PHI, without consent, if each entity has or had a relationship with the patient and the PHI pertains to that relationship.[9] The statute's ambiguous language, "pertains to that relationship," fosters dual interpretations. First, regulators and courts can read this provision to require that covered entities must be treating the patient during the same time period to legally share aspects of the patient's PHI with each other. Conversely, this provision can be interpreted more liberally to allow for uses and disclosure of PHI if both

5. HIPAA Privacy Rule, 45 C.F.R. § 160.103.

6. *See id*. (defining individually identifiable information that is exempt from protected health information as information "in education records covered by the Family Educational Rights and Privacy Act", "records described at 20 U.S.C. § 1232g(a)(4)(B)(iv)", "employment records held by a covered entity", "information regarding a person that has been deceased for more than 50 years.").

7. *See* HIPAA Privacy Rule, 45 C.F.R. § 164.512 (providing an exception for uses and disclosures for public benefit purposes); *see also* HIPAA Privacy Rule, 45 C.F.R. § 164.510 (providing an exception for uses and disclosures made with the patient's prior oral consent); *see also* HIPAA Privacy Rule, 45 C.F.R. § 164.506(c)(4) (providing an exceptions for uses and disclosures for treatment, payment, and health care operations); *see also* HIPAA Privacy Rule, 45 C.F.R. § 164.501 (defining the terms "treatment", "payment", and "health care operations").

8. *See* Standards for Privacy of Individually Identifiable Health Information, 67 Fed. Reg. 53182, 53208-09 (Aug. 14, 2002) (to be codified at 45 C.F.R. Parts 160 and 164) ("Given public expectations with respect to the use or disclosure of information for such activities and so as not to interfere with an individual's access to quality health care or the efficient payment for such health care, *the Department's goal is, and has always been, to permit these activities to occur with little or no restriction* [emphasis added].").

9. HIPAA Privacy Rule, 45 C.F.R. § 164.506(c)(4).

entities have or *had* a relationship with the patient at some point in time.

However, courts struggle to determine when a physician-patient relationship terminates, and an increased amount of online medical resources only compounds this issue.[10] In light of this difficulty, the "at some point in time" interpretation, as opposed to the "during the same time period" interpretation, is more practical *and* more closely aligns with HHS's intent.[11] Moreover, the "at some point in time" interpretation more effectively facilitates the treatment and enforcement of HIPAA.[12]

Although 45 C.F.R. § 164.506(c)(4) fosters dual interpretations, it is a blank space in HIPAA interpretation that regulators and courts have largely yet to address. Therefore, moving forward, regulators should proactively address this blank space and courts should similarly be prepared to properly interpret the provision. This article argues that regulators and courts should adopt the "at some point in time" interpretation rather than the "during the same time period" interpretation. In arguing so, Part II reviews the impracticality of the "during the same time period" interpretation. Part II first provides a discussion of patient abandonment cases, which illustrates that courts and physicians struggle to consistently determine when a physician-patient relationship ceases. Part II further reviews the impracticality of the "during the same time period" interpretation by discussing how advancing technology only makes it more challenging to determine the boundaries of the physician-patient relationship.

Part III then explores the legitimacy of the "at some point in time" interpretation. Part III first explores HHS's intent in drafting HIPAA to

10. *See* discussion *infra* Part II.B & C (discussing courts' inconsistent holdings regarding when a patient relationship forms and terminates, as well as the impact of new technology and the internet on the boundaries of the physician-patient relationship).

11. *See* discussion *infra* Part III.A (discussing how HHS' intent in drafting HIPAA more closely aligns with the "at some point in time" interpretation).

12. *See* discussion *infra* Part III.C (discussing how the "at some point in time" interpretation facilitates treatment and enforcement of HIPAA).

restrict uses and disclosures for TPO purposes as minimally as possible. Part III then discusses the statutory safeguards in place to protect PHI, which reduce the need for the more narrow "during the same time period" interpretation. Part III's discussion on the legitimacy of the "at some point in time" interpretation closes with an overview of the utility of this interpretation in facilitating and enforcing 45 C.F.R. § 164.506(c)(4). Finally, Part IV concludes that regulators and courts should adopt the "at some point in time" interpretation, as opposed to the "during the same time period" interpretation, because the former functions as a more proper and effective reading of the HIPAA provision.[13]

II. IMPRACTICALITY OF THE "DURING THE SAME TIME PERIOD" INTERPRETATION: THE PHYSICIAN-PATIENT RELATIONSHIP

The "during the same time period" interpretation lacks practicality due to the difficulty in defining the temporal boundaries of the physician-patient relationship. It is important to understand that covered entities may face a variety of consequences and sanctions for violating HIPAA through improper uses and/or disclosures of PHI. Typically, the government is made aware of HIPAA violations through self-disclosures from the covered entities or covered entities' employees acting as "whistleblowers".[14] As an overview, these consequences typically come in several forms: voluntary compliance, corrective action plans, other settlement agreements, or exclusion from participation in federal health care programs, such as Medicare, Medicaid, Tricare, and Veterans programs.[15] Covered entities will

13. HIPAA Privacy Rule, 45 C.F.R. § 164.506(c)(4).

14. HIPAA Privacy Rule, 45 C.F.R § 164.408 (requiring covered entities and business entities to notify the proper government authority following breaches of PHI); HIPAA Privacy Rule, 45 C.F.R § 164.502(j)(ii) (providing that covered entities' employees, "whistleblowers", can disclose HIPAA violations without fear of retaliation, and providing procedures by which to make such disclosures).

15. *Enforcement Process*, U.S. Dept. of Health & Human Servs., https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/enforcement-

also be held liable for monetary fines and, potentially, criminal charges.[16] However, no private cause of action for HIPAA violations currently exists.[17] Moreover, to date, no covered entity in the form of a hospital has been excluded, largely due to public policy and practicality concerns.[18] Nevertheless, smaller covered entities, such as private practices and home health care providers, face exclusion for HIPAA violations far more frequently.[19]

The difficulty in defining the boundaries of the physician-patient relationship may make these hefty consequences nearly unavoidable if regulators and courts adopt the "during the same time period" interpretation of 45 C.F.R. § 164.506(c)(4). Across jurisdictions, courts fail to consistently determine when a physician-patient relationship exists.[20] This struggle will likely only worsen as increasing amounts of contradictory medical guidance become more readily available on the internet.[21] Therefore, regulators and courts should not adopt the "during the same time period" interpretation, which requires physicians to unreasonably determine the status of theirs and other physicians' relationships with patients prior to using and disclosing PHI for TPO purposes.

---

process/index.html; OFF. OF INSPECTOR GENERAL, DEPT. OF HEALTH & HUMAN SERVS., THE EFFECT OF EXCLUSION FROM PARTICIPATION IN FEDERAL HEALTH CARE PROGRAMS (1999), https://oig.hhs.gov/exclusions/effects_of_exclusion.asp.

16. HIPAA Privacy Rule, 45 C.F.R § 160.402 (providing the basis for civil money penalties for HIPAA violations); *Enforcement Process*, *supra* note 15.

17. Edward Vishnevetsky, *Can a HIPAA Violation Give Rise to a Private Cause of Action*, D CEO HEALTHCARE, May 27, 2014, http://healthcare.dmagazine.com/2014/05/27/can-a-hipaa-violation-give-rise-to-a-private-cause-of-action/.

18. OFF. OF INSPECTOR GENERAL, DEPT. OF HEALTH & HUMAN SERVS., LEIE DOWNLOADABLE DATABASES, https://oig.hhs.gov/exclusions/exclusions_list.asp (providing various downloadable databases, including a list of all excluded entities).

19. *Id*.

20. *See* discussion *infra* Part II.B. (discussing courts' inconsistent holdings regarding when a physician-patient relationship forms and terminates, making it difficult to understand the temporal boundaries of the physician-patient relationship).

21. *See* discussion *infra* Part II.C (discussing courts' inconsistent holdings regarding when a patient relationship forms and terminates, as well as the impact of new technology and the internet on the boundaries of the physician-patient relationship).

A. Formation and Termination of Physician-Patient Relationships

A physician-patient relationship exists when a physician agrees to treat the patient and the patient accepts these services.[22] Typically, this relationship forms when the physician and patient mutually consent to terms, whether explicitly or implicitly.[23] Upon inception, this relationship legally obligates the physician to complete and/or oversee the patient's treatment.[24]

Once formed, the physician-patient relationship can generally terminate in three ways: (1) the parties' mutual consent to termination; (2) the patient revokes the relationship by dismissing the physician; or (3) the physician determines that his or her services are no longer necessary or beneficial and, after providing the patient with reasonable notice, withdraws from treating the patient.[25] Although this rule may seem rather straightforward, medical experts acknowledge the extreme difficulty, if not total impossibility, in determining when a patient becomes a former patient.[26]

---

22. James L. Rigelhaupt, *What constitutes physician–patient relationship for malpractice purpose*, 17 A.L.R.4th 132, §3 (1982) (providing a list of states and cases following this interpretation and noting that courts generally presume a patient's acceptance of a physician's services); *see* AM. MEDICAL ASS'N, PRINCIPLES OF MED. ETHICS 1 (2016), https://www.ama-assn.org/sites/default/files/media-browser/code-of-medical-ethics-chapter-1.pdf (explaining that a physician-patient relationship exists when a physician provides services for a patient's medical needs).

23. *See* AM. MEDICAL ASS'N, *supra* note 22 at 1-2 (stating that the physician-patient relationship may also arise implicitly in emergency care situations, explicitly when a physician provides medical services for a prisoner under court order, or when a physician conducts an independent medical examination of the patient).

24. Angela R. Holder, *Physician's Abandonment of Patient* 3 AM. JUR. 2D § 2 (1974).

25. Tierney v. University of Michigan Regents, 669 N.W.2d 575, 578 (2003) ("The relation of physician and patient, once initiated, continues until it is ended by the consent of the parties or is revoked by the dismissal of the physician, or until the latter's services are no longer needed or he withdraws from the case."); Fortner v. Koch, 261 N.W. 762, 765 (1935) ("When a physician takes charge of a case and is employed to attend a patient, the relation of physician and patient continues until ended by the mutual consent of the parties, or revoked by dismissal of the physician, or the physician determines that his services are no longer beneficial to the patient . . . .").

26. *See* Am. Medical Ass'n, COUNCIL ON ETHICAL & JUD. AFF. REP. 7 – A-04, PHYSICIAN PARTICIPATION IN SOLICITING CONTRIBUTIONS FROM PATIENTS 4 (2004) ("However, determining when a patient becomes a former patient is nearly impossible. Indeed, patients sometimes re-enter a physician's practice after several years, e.g. if a patient experiences a relapse. Moreover, other personal characteristics (whether the patient is healthy, sick, or

B. Inconsistencies in Patient Abandonment Caselaw Due to the Difficulty in Defining the Physician-Patient Relationship

Inconsistencies in patient abandonment caselaw illustrate the aforementioned extreme difficulty in determining when the physician-patient relationship terminates. Patient abandonment serves as a basis for medical malpractice, which takes root in the concepts of fiduciary duty of care and breach of this duty.[27] The American Jurisprudence Proof of Facts defines patient abandonment as "the unilateral severance by the physician of the professional relationship between himself and the patient without reasonable notice at a time when continuing medical attention is still a necessity."[28] Such unilateral severance can arise from an explicit or implied refusal to attend to the patient's needs.[29]

Patient abandonment claims evidence the difficulty in determining when this relationship terminates. Specifically, jurisdictions have reached inconsistent holdings in patient abandonment cases where physicians believed their relationship with the patient ended but the patient successfully argued that the relationship existed. For example, the Supreme Court of Kansas found in *Adams v. Via Christi Regional Med. Ctr.* that giving any degree of medical advice, such as advising a patient to see a doctor the next

---

dying; whether the patient is particularly wealthy) may be at least as relevant and yet as ambiguous.").

27. Angela R. Holder, *supra* note 24 at § 1 ("Abandonment is recognized basis for liability of physician to patient. It is duty of physician in taking charge of case to follow case and to give proper instruction to patient as to his or her future acts and conduct."). The American Jurisprudence Proof of Facts is a legal encyclopedia written by legal professionals and experts in a variety of other fields. It serves as a trusted legal authority and offers an extensive review of a large range of legal topics. THOMSON REUTERS, *American Jurisprudence Proof of Facts*, *3d,* http://legalsolutions.thomsonreuters.com/law-products/Treatises/American-Jurisprudence-Proof-of-Facts-3d/p/100027553 (last visited Nov. 5, 2017).

28. *See* Holder, *supra* note 24 at § 1 (citing three cases: Stohlman v. Davis, 220 NW 248 (1928); Mucci v Houghton, 57 NW 305 (1894); and Groce v. Myers, 29 SE2d 553 (1944)).

29. Sinclair v. Brunson, 180 N.W. 358, 360 (1920) ("Even though the physician does not make any express declaration to the effect that he will not treat the patient in the future, refusal to attend the patient's needs is considered abandonment.").

day, can trigger the formation of a physician-patient relationship and the accompanying duties.[30] In this case, the individual's mother called the physician to explain that her pregnant daughter was experiencing stomach pain.[31] Although the physician did not consider the individual his patient, he recommended the individual see a doctor the following day and made no inquiries into the individual's condition.[32] The individual was taken to the hospital shortly after this phone call and later died due to pregnancy complications.[33]

At trial for the patient abandonment medical malpractice claim, the physician argued that no physician-patient relationship existed between him and the deceased individual.[34] Although the physician had previously been the patient's family physician, he had neither seen, talked to, nor treated the individual in four years.[35] Moreover, the individual responded on a medical form two weeks before her death that she did not have a family physician.[36] Furthermore, the physician reasonably notified his patients that he would be eliminating obstetrical care from his practice.[37] Nevertheless, the court found that, by stating that the individual should see a doctor the following day, the physician provided medical advice and consented to a relationship with the individual.[38] Thus, because a physician-patient relationship existed, the physician's implied refusal to attend to the patient's needs constituted patient abandonment.[39]

A survey of national case law demonstrates jurisdictional inconsistencies in determining whether a physician-patient relationship existed. Unlike

30. Adams v. Via Christi Regional Med. Ctr., 19 P.3d 140 (2001).
31. *Id*. at 134.
32. *Id*. at 132, 140.
33. *Id*. at 135.
34. *Id*. at 132.
35. *Id*. at 140.
36. *Id*. at 134.
37. *Id*.
38. *Id*.
39. *Id*. at 132.

Kansas, the Supreme Court of New York, Appellate Division, First Department defined the physician-patient relationship more narrowly in *Heraud v. Weissman*, holding that a physician's consultation and prognosis did not rise to such a level of medical advice as to trigger a physician-patient relationship. [40] In that case, a surgical physician conducted an initial consultation with the individual, recommended that the individual required immediate retinal surgery, but provided no such surgical care.[41] After experiencing a retinal tear, the individual initiated a medical malpractice claim for patient abandonment against the physician.[42] The court found no sign of a physician-patient relationship because there was no evidence that the physician agreed to care for the individual.[43] However, no such evidence of an agreement to care was provided in Kansas' *Adams* case.[44] To the contrary, that physician recommended that the individual see a different doctor the following day.[45]

Furthermore, the Georgia Court of Appeals held that no physician-patient relationship existed when a defendant-physician examined a woman in the emergency room, prescribed her medicine, answered her phone call later in the evening, listened to her worsening symptoms, and advised her to see him in the morning.[46] While the Supreme Court of Kansas found a recommendation to see "a doctor" sufficient to trigger a physician-patient relationship,[47] and a Michigan Court of Appeals found that a mere telephone call can revive a prior physician-patient relationship,[48] this Georgia Court of Appeals clearly imposes a much stricter standard for the existence of a

40. Heraud v. Weissman, 714 N.Y.S.2d 476, 478 (N.Y. App. Div. 2000).
41. *Id*.
42. *Id*.
43. *Id*.
44. Adams, 19 P.3d at 140.
45. *Id*. at 132.
46. Clanton v. Von Haam, 340 S.E.2d 627, 630-31 (Ga. Ct. App.1986).
47. Adams, 19 P.3d 140 at 136.
48. *Id*. at 627; Weaver v. Board of Regents of the U. of Mich., 506 N.W.2d 264, 264 (Mich. App. 1993).

physician-patient relationship.[49]

Meanwhile, other jurisdictions, like Oregon, contend that a physician-patient relationship exists, even without the physician personally seeing the patient, if the physician knows or reasonably should know that he or she is "diagnosing a patient's condition or treating the patient," as such a diagnosis represents a consent to the relationship.[50] However, an application of this standard would likely have yielded opposite conclusions in the aforementioned cases out of Kansas, New York, Michigan, and Georgia.[51] These cases represent only a small portion of the inconsistencies in defining the physician-patient relationship across jurisdictions.[52]

Reflecting on these cases, the "during the same time period" interpretation would be unworkable and likely result in unavoidable sanctions against covered entities for violating HIPAA.[53] These inconsistent holdings make it difficult for physicians to anticipate liability arising out of a physician-patient relationship. Additionally, considering that whether a physician-patient relationship exists is generally an issue of fact, a physician cannot reasonably guess how a finder of fact would perceive the circumstances of his or her current relationship with the patient when choosing to use or disclose PHI for TPO purposes.[54] Moreover, because courts and physicians can disagree on

49. *See* Clanton, 340 S.E.2d at 630-31.

50. Mead v. Legacy Health System, 283 P.3d 904, 910 (Or. 2012).

51. Adams, 19 P.3d at 132; Heraud, 714 N.Y.S.2d at 478; Clanton, 340 S.E.2d at 627.

52. *See generally* Rigelhaupt, *supra* note 22 (providing an extensive overview of what constitutes a physician-patient relationship for medical malpractice purposes across different jurisdictions).

53. *Top Five Issue in Investigated Cases Closed with Corrective Action, by Calendar Year,* DEPT. OF HEALTH & HUMAN SERVS., https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/data/top-five-issues-investigated-cases-closed-corrective-action-calendar-year/index.html (last visited June 7, 2017) (providing data that, from 2004 to 2015, impermissible uses and disclosures was the number one issue in investigated HIPAA cases closed with a corrective action plan, and the second most investigated issue closed with a corrective action plan in 2003).

54. Raptis–Smith v. St. Joseph's Med. Ctr., 755 N.Y.S.2d 384, 386 (N.Y. App. Div. 2003) (finding that whether a physician-patient relationship existed between an attending radiologist and the patient constituted an issue of fact in a medical malpractice action); Tom v. Sundaresan, 966 N.Y.S.2d 434, 435 (N.Y. App. Div. 2013) (explaining that, unlike the

when a physician-patient relationship currently exists, it is far more reasonable for a physician to determine whether he or she had a relationship with the individual *at some point in time* than whether this relationship continues currently. Thus, the "during the same time period" interpretation lacks practicality because it fails to consider the complexity of the physician-patient relationship. In this way, the broader, "at some point in time" provides a more workable standard because it only requires covered entities to know that they both have or had a relationship with the patient at some point to use and disclose PHI for TPO purposes.[55]

C. Modern Technology and Its Effect on Physician-Patient Relationship Temporal Boundaries

The aforementioned patient abandonment cases illustrate that courts and physicians already struggle to determine when a patient becomes a former patient, and what actions can revive a former physician-patient relationship. The evolution of telemedicine aggravates this struggle and makes it more difficult to decipher when the physician-patient relationship precisely begins or ends.[56] Today, an individual can contact a physician, receive a diagnosis and potentially treatment, and create a physician-patient relationship entirely

---

issue of whether a physician owes a duty of care to a patient, the question of whether a physician-patient relationship exists constitutes an issue of fact).

55. *See* discussion *infra* Part III (further discussing the legitimacy of the "at some point in time" interpretation).

56. *See* WHO, TELEMEDICINE: OPPORTUNITIES AND DEVELOPMENTS IN MEMBER STATES: REPORT ON THE SECOND GLOBAL SURVEY ON EHEALTH 9 (Kai Lashley ed., 2nd vol. 2009), http://www.who.int/goe/publications/goe_telemedicine_2010.pdf (citing WHO, A HEALTH TELEMATICS POLICY IN SUPPORT OF WHO'S HEALTH-FOR-ALL STRATEGY FOR GLOBAL HEALTH DEVELOPMENT (1998)) (defining "telemedicine" as "[t]he delivery of health care services, where distance is a critical factor, by all health care professionals using information and communication technologies for the exchange of valid information for diagnosis, treatment and prevention of disease and injuries, research and evaluation, and for the continuing education of health care providers, all in the interests of advancing the health of individuals and their communities.").

online.[57] Courts continue to disagree regarding how various out-of-office communications affect physician-patient relationships; telemedicine now joins the list of such means of communication available to physicians. Consequently, one could confidently say that the internet and other advances in technology will pose similar, if not far greater, challenges for courts. Although physicians may mitigate liability through express waivers online and click-wrap agreements, courts may struggle to apply to online interactions the general rule that a physician-patient relationship exists where the physician provides a diagnosis and/or treatment.[58] More specifically, in an age where many people never truly "disconnect" from the internet and medical self-help websites are only a click away, courts may face greater struggles in determining when an online physician-patient relationship terminates, and what impact the physician truly had on the individual's medical outcome.[59] Consequently, courts and regulators should consider telemedicine's impact on the temporal boundaries of the physician-patient relationship when interpreting 45 C.F.R. § 164.506(c)(4).[60] Such consideration would make it clear that physicians cannot be reasonably expected to accurately determine whether their relationships with the patient overlapped prior to uses and disclosures for TPO purposes, as the "during the same time period" interpretation requires. Therefore, courts and regulators should recognize that telemedicine further adds to the impracticality of the "during the same time period" interpretation of 45 C.F.R. § 164.506(c)(4).

57. John D. Blum, *Internet Medicine and the Evolving Legal Status of the Physician-Patient Relationship*, 24 J. LEGAL MED. 413, 414 (2013).

58. *Id*. at 439.

59. *Id*. at 415 (citing Lee Rainie & Susannah Fox, *The Online Health Care Revolution*, PEW RESEARCH CENTER, Nov. 26, 2000, http://www.pewinternet.org/2000/11/26/the-online-health-care-revolution/) ("More than 52 million adults in the United States have searched the World Wide Web for health and medical information.").

60. *See* HIPAA Privacy Rule, 45 C.F.R. § 164.506(c)(4).

III. THE LEGITIMACY OF THE "AT SOME POINT IN TIME" INTERPRETATION

As described above, regulators and courts should adopt the "at some point in time" interpretation of 45 C.F.R. § 164.506(c)(4) for several reasons. First, the "at some point in time" interpretation more accurately reflects the drafters' intent.[61] Second, safeguards in place adequately protect individuals' rights to privacy regarding their PHI. Third, the broader, "at some point in time" interpretation facilitates treatment and enforcement of HIPAA.

A. HIPAA'S Original Intent

The "at some point in time" interpretation more accurately reflects HHS's original intent in drafting HIPAA.[62] HHS was clear in its intent to restrict uses and disclosures regarding TPO as minimally as possible.[63] In theory, the "at some point in time" interpretation fosters a more minimal restriction to disclosures for TPO purposes than the "during the same time period" interpretation because the former provides a standard that covered entities can more easily satisfy. Consequently, some who advocate for stringently limiting uses and disclosures of PHI may argue that the "at some point in time" interpretation allows for too high a volume of PHI uses and disclosures and, thus, violates the minimum necessary standard, which provides that covered entities should make *reasonable* efforts to limit uses and disclosures to the those minimally necessary to accomplish their goal.[64]

---

61. *See* Standards for Privacy of Individually Identifiable Health Information, *supra* note 8, at 53183 ("[HHS's modifications to the HIPAA Privacy Rule] reflected a continuing commitment on the part of the Department to strong privacy protections for medical records *and the belief that privacy is most effectively protected by requirements that are not exceptionally difficult to implement* [emphasis added].").

62. *See id*.

63. *Id*. at 53182, 53208-09.

64. HIPAA Privacy Rule, 45 C.F.R. § 164.502(b); *See* David Humiston, *Will Your State Privacy Law Be superseded by HIPAA?*, MANAGED CARE MAGAZINE, May 2002, https://www.managedcaremag.com/archives/2002/5/will-your-states-privacy-law-be-superseded-hipaa (defining "more stringent" state laws as those that restrict or prohibit uses

However, the minimum necessary standard expressly does not apply to uses and disclosures for treatment purposes.[65] Although the standard applies to uses and disclosures for payment and health care operations, this article argues that the "at some point in time" interpretation is, in fact, minimally necessary based upon HHS's intent in drafting HIPAA.[66] Specifically, permitting uses and disclosures for TPO purposes only if each covered entity has or had a simultaneous relationship with the patient would *unreasonably*, severely restrict these activities and, therefore, impinge on HHS's goal to permit disclosures for TPO purposes to occur with little or no restriction. Conversely, the "at some point in time" interpretation more *reasonably* restricts such activities and, thus, more accurately reflects HHS's emphasis on the necessity of these activities for an efficient and high-quality health care system.

B. Current Safeguards Protect Individuals' Rights to Privacy Regarding PHI

---

and disclosures that are proper under HIPAA). Although this article does not directly discuss 45 C.F.R. § 164.506(c)(4), it provides examples of states that utilize several more and less stringent provisions regarding PHI than HIPAA. Generally, when a state provides more stringent provisions than HIPAA and the provisions are not contrary to HIPAA, its provisions will take effect over HIPAA. Conversely, when a state's provisions are less stringent, HIPAA preempts the state's provisions. For example, New York and Illinois generally provide parallel or more stringent provisions than HIPAA. However, California provides parallel or less stringent provisions than HIPAA, except regarding liability, for which California provides a private cause of action for violations of its medical information privacy laws. Nevertheless, the article purports that HIPAA provides more stringent provisions than most states. Ultimately, advocates of these more stringent state provisions would likely similarly argue that the "during the same time period", as compared to the "at some point in time", interpretation of 45 C.F.R. § 164.506(c)(4) more properly limits the time frame for uses and disclosures of PHI and likely reduces the volume of disclosed PHI. *See id.*

65. 45 C.F.R. § 164.502(b).

66. DEPT. OF HEALTH & HUMAN SERVS., DISCLOSURES FOR TREATMENT, PAYMENT, AND HEALTH CARE OPERATIONS (2003), https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/sharingfortpo.pdf (explaining that the minimum necessary standard applies to uses and disclosures of PHI for payment and health care operations and, therefore, covered entities must establish policies and procedures that *reasonably* limit such uses and disclosures [emphasis added]).

The "at some point in time" interpretation does not unreasonably infringe upon the privacy and security of PHI because current safeguards adequately protect PHI.[67] According to 45 C.F.R. § 164.522(a), individuals can request restrictions on how a covered entity will use and disclose their PHI for TPO purposes.[68] Although the statute does not require covered entities to agree to such restrictions, the entity must abide by any restrictions to which it agrees.[69] Thus, this safeguard allows individuals to express their desire for privacy and, if the covered entity does not respect these wishes, choose to not use that covered entity because it will not agree to their terms. Likewise, it holds entities accountable for any such agreements they choose to make. The statute further safeguards an individual's right to privacy by requiring health plans to "accommodate an individual's reasonable request for confidential communications, if the individual clearly states that not doing so could endanger him or her."[70] Therefore, current HIPAA safeguards protect individuals by preserving their right to request privacy restrictions on uses and disclosures of PHI for TPO, and by demanding that health plans abide by these requests when safety requires.

C. Facilitation of Treatment and Enforcement

The "at some point in time" interpretation facilitates treatment and enforcement of HIPAA provisions by establishing a clear test for what constitutes a violation of 45 C.F.R. § 164.506(c)(4).[71] Regarding treatment facilitation, when proposing modifications to the HIPAA Privacy Rule, HHS

67. *See* HIPAA Privacy Rule, 45 C.F.R. § 164.522(a); *see also* HIPAA Privacy Rule, 45 C.F.R. § 164.522(b).
68. 45 C.F.R. § 164.522(a).
69. *Id*.
70. 45 C.F.R. § 164.522(b).
71. *See* Standards for Privacy of Individually Identifiable Health Information, *supra* note 8, at 53186 ("The purpose of the [TPO] exclusions . . . is to facilitate those communications that enhance the individual's access to quality health care."); HIPAA Privacy Rule, 45 C.F.R. § 164.506(c)(4).

acknowledged that "a health care provider cannot treat a patient without being able to use and disclose his or her protected health information for treatment purposes."[72] Recognizing the necessity of uses and disclosures of PHI for treatment, the "at some point in time" interpretation allows covered entities to exchange PHI more freely and, thereby, facilitates treatment.

More specifically, by reducing the restrictions on uses and disclosures, physicians may more readily share and obtain PHI to facilitate treatment and improve the continuity of care.[73] For example, when changing physicians, the "at some point in time" interpretation permits the new physician to contact the prior physician and discuss the patient's PHI for treatment purposes. This allows the new physician to develop a more complete understanding of how to best treat the patient and deliver seamless services.[74] Thus, by permitting uses and disclosures of PHI for treatment purposes, the "at some point in time" interpretation facilitates treatment, reduces fragmentation of care, and enhances the quality of care along with patient safety.[75]

Similarly, the "at some point in time" interpretation would likely facilitate enforcement of HIPAA. Under § 160.402 of the HIPAA Privacy Rule, the Secretary of HHS will impose monetary fines upon any covered entity or

---

72. Standards for Privacy of Individually Identifiable Health Information, 67 Fed. Reg. 14776, 14778 (proposed Mar. 27, 2002) (codified at 45 C.F.R. Parts 160 and 164).

73. *Continuity of Care, Definition of,* AM. ACAD. OF FAM. PHYSICIANS (2015), http://www.aafp.org/about/policies/all/definition-care.html (defining "continuity of care" as the "process by which the patient and his/her physician-led care team are cooperatively involved in ongoing health care management toward the shared goal of high quality, cost-effective medical care.").

74. Martin Gulliford et al., *Continuity of Care in the United States*, 11 J. OF HEALTH SERVS. RES. & POL'Y 248–50 (2006), http://journals.sagepub.com/doi/10.1258/135581906778476490 ("For providers . . ., the contrasting ideal [for continuity of care] is the delivery of a 'seamless service' through integration, coordination and the sharing of information between different providers. As patients' health care needs can now only rarely be met by a single professional, multidimensional models of continuity have had to be developed to accommodate the possibility of achieving both ideals simultaneously.").

75. *Continuity of Care, Definition of*, *supra* note 73 ("[C]ontinuity of care] reduces fragmentation of care and thus improves patient safety and quality of care.").

business associate who violates any HIPAA provision.[76] The regulations obligate covered entities to disclose such violations, as well.[77] The "at some point in time" interpretation facilitates such disclosures and enforcement because it provides both covered entities and the government with a clear test as to what constitutes a violation of § 164.506(c)(4). Under this interpretation, a covered entity violates the provision by sharing PHI with a covered entity who at no point in time had a relationship with the patient or by sharing PHI that does not pertain to that relationship.[78] With so clear a test, covered entities can more effectively audit and monitor their operations, educate their employees on proper uses and disclosures, and understand when their conduct is improper and, hence, requires disclosure to the government.[79] Congruently, the "at some point in time" interpretation's clear test eases the government's burden of determining whether a violation occurred because the government does not have to determine whether the entities had simultaneous relationships with the patient. Therefore, the simplicity of the "at some point in time" interpretation enhances both treatment and enforcement of 45 C.F.R. § 164.506(c)(4).

IV. CONCLUSION

Regulators and courts alike should adopt the "at some point in time" interpretation, rather than the "during the same time period" interpretation, of 45 C.F.R. § 164.506(c)(4). This provision functions far more efficiently

76. HIPAA Privacy Rule, 45 C.F.R. § 160.402.

77. HIPAA Privacy Rule 45 C.F.R. § 164.408 ("A covered entity shall, following the discovery of a breach of unsecured protected health information as provided in § 164.404(a)(2), notify the Secretary.").

78. HIPAA Privacy Rule, 45 C.F.R. § 164.506(c)(4).

79. OFF. OF INSPECTOR GENERAL, DEPT. OF HEALTH & HUMAN SERVS. *Health Care Compliance Program Tips*, HEALTH CARE FRAUD PREVENTION & ENFORCEMENT ACTION TEAM PROVIDER COMPLIANCE TRAINING, visitedhttps://oig.hhs.gov/compliance/provider-compliance-training/files/compliance101tips508.pdf (last visited Nov. 5, 2017) (providing the seven fundamental elements of an effective compliance program, including conducting internal auditing and monitoring, effective training and education, and responding promptly to discovered regulatory violations, which includes disclosure to the government).

if it allows covered entities to use and disclose PHI for TPO proposes if each entity has or had a relationship with the patient at some point in time. Likewise, the "at some point in time" interpretation recognizes the complexity of the physician-patient relationship, including the impact of telemedicine, and removes the need for covered entities and courts to decipher whether the entities had simultaneous relationships with the patient. Further, the "at some point in time" interpretation continues to preserve the privacy of PHI while accurately reflecting the Department of Health and Human Services' intent in drafting HIPAA. Ultimately, in fostering treatment and enforcement of this HIPAA provision, the "at some point in time" interpretation of 45 C.F.R. § 164.506(c)(4) encourages a superior quality of care and more efficient health care system.

Consumers Left up a Genetic Data Creek without a Paddle

John Meyer

I. INTRODUCTION

In a world with ever increasing accuracy in genome testing and interpretation, where businesses sell private services increasingly similar to medical diagnosis, what is a consumer to do with the data? Companies now offer consumers the ability to have their genetic code processed and transformed into data which is compared to known genetic traits to provide the customer with information about themselves.[1] Originally, these tests, sold directly to consumers, tested for ancestry and genetic traits such as hair loss; however, tests now include information regarding wellness, genetic health risks, and carrier status.[2] This information ranges from suggestions on how to most effectively deal with weight to your likelihood of developing non-curable diseases like Alzheimer's.[3]

Recently, the Food and Drug Administration's (FDA) decision to grant regulatory approval of such products has given the data not only federal

1. *How is Genetic Testing Done?*, U.S. NAT'L LIBR. MED. (Nov. 28, 2017), https://ghr.nlm.nih.gov/primer/testing/procedure ("For example, a procedure called a buccal smear uses a small brush or cotton swab to collect a sample of cells from the inside surface of the cheek. The sample is sent to a laboratory where technicians look for specific changes in chromosomes, DNA, or proteins, depending on the suspected disorder.").

2. *Health + Ancestry*, 23ANDME, https://www.23andme.com/dna-health-ancestry/ (last visited Dec. 2, 2017).

3. *See Genetic Weight*, 23ANDME, https://permalinks.23andme.com/pdf/samplereport_wellness.pdf (last visited Dec. 2, 2017); *Late-Onset Alzheimer's Disease*, 23ANDME, https://permalinks.23andme.com/pdf/samplereport_geneticheath.pdf (last visited Dec. 2, 2017).

approval but also a significant stamp of authenticity consumers may rely on to their detriment.[4] Despite the data's authenticity, consumers may still lack the scientific literacy to interpret what the companies provide.[5] It is unclear to exactly what degree these data providers are responsible for ensuring consumer understanding, seeing as, according to the FDA, they are not actually providing a diagnosis.[6] With the receipt of this medically relevant data, consumers are often guided to their doctors for advice.[7] However, most doctors are trained to diagnose patients and lack an appropriate background to effectively analyze genetic risk factors.[8]

In order to prevent possible harm when discussing the risk of serious future medical conditions, it is important that consumers develop a proper understanding of their results. Companies that offer genetic services can further ensure proper understanding by referring or giving their customers access to health care providers with a specialty in communicating genetic risk factors – rather than a primary care physician. However, even if companies provide customers with sufficient information, a thin waiver of liability should not be sufficient to absolve them of potential harms associated with a consumer's failure to properly comprehend the implications of their results which could result in injuries such as panic and harmful self-treatment. Courts should give customers the opportunity to seek remedy for injuries that

4. *FDA Allows Marketing of First Direct-to-Consumer Tests*, U.S. FOOD & DRUG ADMIN., https://www.fda.gov/newsevents/newsroom/pressannouncements/ucm551185.htm (last updated Apr. 7, 2017) [hereinafter *FDA Allows*].

5. David Dobbs, *The Case for Selective Paternalism in Genetic Testing*, NEURON CULTURE (Jan. 14, 2013), http://daviddobbs.net/smoothpebbles/the-case-for-paternalism-in-genetic-testing/.

6. *23andMe Service Options*, 23ANDME, https://customercare.23andme.com/hc/en-us/articles/202908020-23andMe-Service-Options (last visited Sept. 29, 2017) ("This data has undergone a general quality review however only a subset of markers have been individually validated for accuracy. The data from 23andMe's Browse Raw Data feature is suitable only for research, educational, and informational use and not for medical, diagnostic or other use.").

7. Richard R. Sharp, *Addressing Gaps in Physician Education Using Personal Genomic Testing*, 13 GENETICS IN MED. 8, 750-51 (2011).

8. *Id.* (". . .practicing physicians are likely to encounter patients wishing to discuss genetic test results with which those physicians have very limited familiarity").

arise from serious misunderstanding of FDA approved data provided by companies.

II. HISTORY OF DIRECT-TO-CONSUMER GENOMICS

Traditionally, medical professionals would be the facilitators of genetic testing to ensure patients had a proper source for information and advice, but now testing kits are available to everyone to collect a DNA sample and send it to a lab for testing. These testing kits are referred to as Direct-to-Consumer (DTC) Genomics.[9] One of the most well-known providers of DTC genomic tests is 23andMe.[10] In 2007, 23andMe released its first Personal Genome Service with the mission to "help people access, understand and benefit from the human genome" where they would compare a customer's genetic data to known genetic markers and provide information on ancestry or other characteristics.[11] As years passed, their collection of consumer genetic data rapidly increased, allowing them to develop many new studies of genetic markers regarding disease and physical characteristics.[12] Unfortunately for consumers, genetic risk factors that measure predisposition are not a simple determination, as the development of a specific genetic condition is often dependent on much more than the information a DTC Genomic test can provide, hence the high level of concern associated with misunderstanding.[13]

---

9. *What is Direct-to-Consumer Testing?*, U.S. NAT'L LIBR. MED. (Sept. 26, 2017), https://ghr.nlm.nih.gov/primer/testing/directtoconsumer.

10. Sarah Schmidt, *9 Leading Companies in Direct-to-Consumer Genetic Testing,* MARKETRESEARCH.COM (Apr. 6, 2016), http://blog.marketresearch.com/9-leading-companies-in-direct-to-consumer-genetic-testing.

11. *23andMe About Us*, 23ANDME, https://mediacenter.23andme.com/company/about-us/ (last visited Sept. 29, 2017).

12. *Id.* ("23andMe has more than 2,000,000 genotyped customers. More than 85 percent of our customers have opted-in to participate in our research. [T]he company has collected 600 million phenotypic data points. To date, 23andMe has published more than 75 peer-reviewed studies in scientific journals.").

13. *What Does it Mean to Have a Genetic Predisposition to a Disease?*, U.S. NAT'L LIBR. MED. (Nov. 28, 2017), https://ghr.nlm.nih.gov/primer/mutationsanddisorders/predisposition ("A genetic predisposition (sometimes also called genetic susceptibility) is an increased likelihood of developing a particular disease based on a person's genetic makeup. In people with a genetic

The FDA became officially involved in 2013 when it issued a formal warning letter to 23andMe for failing to obtain proper regulatory approval required under the Federal Food, Drug, and Cosmetic Act (FDCA) on a genetic risk assessment of breast cancer that produced data the FDA considered similar in nature to a diagnosis.[14] Along with a number of violated regulations requiring 23andMe to stop marketing their product, the letter also mentioned a strong concern for consumers' well-being, a role the people, through Congress, have entrusted to the FDA since its inception.[15] In 1906, Congress passed the Food and Drugs Act to protect consumers from products that were improperly labeled or substandard.[16] Congress enacted the FDCA's current format in 1938 after public outrage due to the increasing number of deaths from untested products on the market.[17] Finally, in 1976 Congress passed the Medical Device Amendments which grant the FDA the authority to regulate all in vitro Diagnostic Devices (IVDs) to ensure "the reasonable safety and effectiveness of these tests; that they are accurate,

predisposition, the risk of disease can depend on multiple factors in addition to an identified genetic change. These include other genetic factors (sometimes called modifiers) as well as lifestyle and environmental factors.").

14. Alberto Gutierrez, *23andMe, Inc. 11/22/13,* U.S. FOOD & DRUG ADMIN., https://www.fda.gov/ICECI/EnforcementActions/WarningLetters/2013/ucm376296.htm (last updated Mar. 28, 2014); *see also* FEDERAL FOOD, DRUG, AND COSMETIC ACT OF 1938 § 201(h), 21 U.S.C. § 321(h) (2011) ("The term "device" . . . means an instrument, apparatus, implement, machine, contrivance, implant, in vitro reagent, or other similar or related article, including any component, part, or accessory, which is— . . . (2) intended for use in the diagnosis of disease or other conditions, or in the cure, mitigation, treatment, or prevention of disease, in man or other animals . . .").

15. Gutierrez, *supra* note 14 ("Some of the uses for which PGS is intended are particularly concerning, such as assessments for BRCA-related genetic risk and drug responses (e.g., warfarin sensitivity, clopidogrel response, and 5-fluorouracil toxicity) because of the potential health consequences that could result from false positive or false negative assessments for high-risk indications such as these.").

16. *How Did the Federal Food, Drug, and Cosmetic Act Come About?*, U.S. FOOD & DRUG ADMIN., https://www.fda.gov/AboutFDA/Transparency/Basics/ucm214416.htm (last visited Oct. 29, 2017).

17. *Id.* ("The tipping point came in 1937, when an untested pharmaceutical killed scores of patients, including many children, as soon as it went on the market. The enactment of the 1938 Food, Drug, and Cosmetic Act tightened controls over drugs and food, included new consumer protection against unlawful cosmetics and medical devices, and enhanced the government's ability to enforce the law.").

reliable, and clinically meaningful."[18]

Less than a year later,[19] 23andMe met the FDA's regulatory concerns by agreeing to suspend the production of genetic health data.[20] The FDA remained relatively quiet until April of 2017 when it announced its approval of ten DTC genetic risk assessments with implemented special controls to ensure accuracy and reliability of data.[21] It is also a requirement that any data used for medical purposes has to be delivered in a way that its consumers can properly comprehend.[22] The FDA determines consumer comprehension

18. Jeffrey Shuren, *Examining the Regulation of Diagnostic Tests and Laboratory Operations*, U.S. FOOD & DRUG ADMIN. (Nov. 17 2015), https://www.fda.gov/NewsEvents/Testimony/ucm473922.htm ("[T]he central features of FDA's framework for devices, including IVDs, are a system of device classification that tailors regulation to device risk; a transparent review standard that accounts for the benefits and risks to patients, and range of regulatory controls that together provide a reasonable assurance of safety and effectiveness; and an adaptive but scientifically grounded evidentiary standard of valid scientific evidence. Patients have benefited from this regulatory model, which has enabled FDA to respond to innovation in rapidly emerging technologies. . .while ensuring tests used to make treatment decisions for patients are accurate and reliable.").

19. Alberto Gutierrez, *23andMe, Inc. – Close Out Letter 3/25/14*, U.S. FOOD & DRUG ADMIN., https://www.fda.gov/iceci/enforcementactions/warningletters/ucm391016.htm (last updated Mar. 28, 2014) [hereinafter *Close Out Letter]* ("Your firm's response to our Warning Letter appears to be adequate. This letter does not relieve you or your firm from the responsibility of taking all necessary steps to assure sustained compliance with the Federal Food, Drug, and Cosmetic Act and its implementing regulations or with other relevant legal authority.").

20. Grant Brunner, *23andMe Halts Health-Based DNA Analysis After FDA Crackdown*, EXTREME TECH (Dec. 6, 2013), https://www.extremetech.com/extreme/172248-23andme-halts-health-based-dna-analysis-after-fda-crackdown.

21. *FDA Allows*, *supra* note 4 ("Parkinson's disease, a nervous system disorder impacting movement; Late-onset Alzheimer's disease, a progressive brain disorder that destroys memory and thinking skills; Celiac disease, a disorder resulting in the inability to digest gluten; Alpha-1 antitrypsin deficiency, a disorder that raises the risk of lung and liver disease; Early-onset primary dystonia, a movement disorder involving involuntary muscle contractions and other uncontrolled movements; Factor XI deficiency, a blood clotting disorder; Gaucher disease type 1, an organ and tissue disorder; Glucose-6-Phosphate Dehydrogenase deficiency, also known as G6PD, a red blood cell condition; Hereditary hemochromatosis, an iron overload disorder; and Hereditary thrombophilia, a blood clot disorder.").

22. *Id.* ("The FDA requires the results of all DTC tests used for medical purposes be communicated in a way that consumers can understand and use."); *see also Learn More About 23andMe's New Genetic Health Risk Reports*, 23ANDME (May 19, 2017), https://blog.23andme.com/health-traits/learn-23andmes-new-genetic-health-risk-reports/ ("Each report is broken into a similar structure that includes your results, an explanation of what they mean, an overview of the condition, other factors that may influence risk, suggested next steps, and additional resources. This is all done in clear and easy to understand language, and the reports are structured in a way that allows you to go deeper

based on evidence submitted by the manufacturer.[23] In the case of 23andMe, the government relied on a consumer comprehension study administered by 23andMe, which tested the thoroughness of the frequently asked questions page, and the opt-in page consumers are required to agree to prior to receiving results for more severe diseases.[24]

In a recent review of several studies on the link between communicated risk and behavior changes, researchers concluded that, similar to other examples of risks such as smoking and weight gain, genetic risk factors will not have a significant impact on society.[25] While these sources have claimed that genetic health data does not actually impact the choices people make, it is too early to draw that conclusion in such a fast-growing market.[26] There are currently over 1,000 genetic tests used to find various genetic conditions by identifying mutations and other variations in a person's DNA.[27] The rising popularity of DTC genomics is closely associated with a rise in care for personal health.[28] This means that the consumers purchasing the tests may

---

into different sections to learn more if you wish.").

23. *Evaluation of Automatic Class III Designation*, U.S. FOOD & DRUG ADMIN., https://www.accessdata.fda.gov/cdrh_docs/reviews/den160026.pdf (last updated May 02, 2017).

24. *Id.*

25. Timothy Caulfield, *The Limits of Personalized Medicine*, ATLANTIC (Mar. 16, 2016), https://www.theatlantic.com/health/archive/2016/03/does-knowing-personal-health-risks-change-behavior/473991/ (stating that other possible conflicting impacts include creating a sense that good health requires overwhelmingly complicated processes or that other public health initiatives are no longer important).

26. Muin J Khoury, *Does Genetic Risk Information Improve Healthy Behavior?*, CTRS. DISEASE CONTROL & PREVENTION (Apr. 11, 2016), https://blogs.cdc.gov/genomics/2016/04/11/does-genetic-risk/.

27. *What is Genetic Testing?*, U.S. NAT'L LIBR. MED. (Sept. 26, 2017), https://ghr.nlm.nih.gov/primer/testing/genetictesting ("Molecular genetic tests (or gene tests) study single genes or short lengths of DNA to identify variations or mutations that lead to a genetic disorder. Chromosomal genetic tests analyze whole chromosomes or long lengths of DNA to see if there are large genetic changes, such as an extra copy of a chromosome, that cause a genetic condition. Biochemical genetic tests study the amount or activity level of proteins; abnormalities in either can indicate changes to the DNA that result in a genetic disorder.").

28. Muin J Khoury, *Direct to Consumer Genetic Testing and Public Health Education*, CTRS. DISEASE CONTROL & PREVENTION (Mar. 8, 2016), https://blogs.cdc.gov/genomics/2016/03/08/direct-to-consumer/ ("In an age of easily accessible and sometimes confusing health information on the Internet, consumers are

intend to use them for some medical benefit which could lead to unexpected and possibly harmful results.[29] In fact, 23andMe suggests that the data they provide will benefit customers by allowing them to become their own best medical advocate.[30]

In addition to testing for genetic conditions, there are other types of genomic testing that have a large potential impact on the health of consumers.[31] Pharmogenetics, which is an established and quickly evolving field, hopes to use genetic testing to not only help consumers find medications that will have the most effect on a specific individual, but it also presents the future possibility of customizable drugs.[32] Other DTC genomic services claim that for $1000 a year they can use genomic data about the bacteria in your stomach to create personalized nutrition plans to maximize health.[33] The major concern is that consumers might take the data into their

fascinated with genomics and its possibilities for improving health. As we are bombarded by news of the latest scientific discoveries of "the gene for disease X," it may be tempting to think that genomic information is always useful and does not cause harm, even when there is no available scientific evidence. As we look to consider genetic testing as a way to improve health, we need all the credible help we can get.").

29. Muin J Khoury, *Direct to Consumer Genetic Testing: Think Before You Spit, 2017 Edition!*, CTRS. FOR DISEASE CONTROL & PREVENTION (Apr. 18, 2017), https://blogs.cdc.gov/genomics/2017/04/18/direct-to-consumer-2/.

30. *Health + Ancestry*, *supra* note 2 ("These reports provide you with more insights to be the best possible advocate – for you.").

31. *Genetic Testing: How it is Used for Healthcare*, NAT'L INSTITUTES HEALTH, https://www.report.nih.gov/NIHfactsheets/Pdfs/GeneticTesting-HowItIsUsedForHealthcare(NHGRI).pdf (last visited Nov. 19, 2017) (stating that uses of genetic testing include: diagnostic testing, predictive and pre-symptomatic genetic testing, carrier testing, prenatal testing, pre-implantation genetic testing, newborn screening, pharmacogenetic testing, and research genetic testing).

32. Shannon Manzi, *Can Genetic Testing Help Determine the Best Medications for You?*, HARV. HEALTH PUB. (Dec. 16, 2016), https://www.health.harvard.edu/blog/can-genetic-testing-help-determine-the-best-medications-for-you-2016121610888 ("One of the things your genes direct is the production of enzymes required to break down (or metabolize) the drugs you take. These enzymes influence how effective a drug might be for you and how likely you are to experience negative side effects.").

33. Kevin Loria, *Companies are Trying to Use Your DNA and Bacteria to Give You Personalized Diet Advice*, BUS. INSIDER (Jun. 11, 2017), http://www.businessinsider.com/personalized-nutrition-dietary-advice-dna-test-microbiome-2017-6 (stating that many professionals when asked about the validity of such a test claimed that it was beyond current scientific understanding. When asked for proof, Naveen Jain, founder of Viome, said it would take at least six months).

own hands, making drastic lifestyle changes or relying on unregulated false results to self-manage their health, including medications, to their detriment.[34]

III. THIRD PARTY RESOURCES

In addition to the FDA approved data, the consumer receives what 23andMe refers to as the customer's "raw" genetic data.[35] 23andMe does not interpret this raw data but it contains genetic code not evaluated for accuracy.[36] Without much direction on what to do with this data, consumers have developed a whole host of third party online resources and interpretation materials.[37] An easy-to-find resource are online blogs, many of which have disclaimers stating that peer reviewed articles are the foundation of their material; however, the author is not a doctor and consumers should not rely on the information for medical purposes.[38] Promethease, an online application that interprets raw genetic data provided by services like 23andMe to consumers, requires the consumer to accept multiple, liability-releasing terms and conditions before viewing the webpage and directs the consumer to an online forum for answers to any questions.[39] However, other

34. Gutierrez, *supra* note 14 ("The risk of serious injury or death is known to be high when patients are either non-compliant or not properly dosed; combined with the risk that a direct-to-consumer test result may be used by a patient to self-manage, serious concerns are raised if test results are not adequately understood by patients or if incorrect test results are reported.").

35. *Accessing and Downloading Your Raw Data*, 23ANDME, https://customercare.23andme.com/hc/en-us/articles/212196868-Accessing-and-Downloading-Your-Raw-Data (last visited Sept. 29, 2017).

36. *Id.*

37. *What to do with Your 23andMe Raw Data*, GENETIC LIFEHACKS, http://www.geneticlifehacks.com/23andme-raw-data/ (last updated Mar. 2017) (stating that StrateGene, LiveWella, and Nutrahacker are all third party resources that allow you to pay a fee ranging from $20 to $85 in order to gain access to services that compare your genetic data to existing reports. The sites have various sources of information ranging from other consumers interested in genetics to external resources to professional, others simply recommend talking to a doctor).

38. *About*, GENETIC LIFEHACKS, http://www.geneticlifehacks.com/about/ (last visited Sept. 29, 2017).

39. *Promethease*, PROMETHEASE, https://www.promethease.com/ (last visited Sept. 29,

applications clarify that the FDA does not regulate them because they are not providing information intended for diagnostic purposes.[40] The one aspect that most of these resources have in common is a waiver of liability that directs the consumer to consult a doctor about any concerns that arise from the information they provide.[41]

IV. PRIMARY CARE PHYSICIANS

A 2016 study polled users of DTC genomic services and found that only 27% discussed their results with their primary care physician (PCP) and of this percentage, only 35% felt "very satisfied" with that encounter.[42] While the number of consumers that have followed the advice of DTC genomic providers and sought the advice of a medical professional is not huge, researchers expect it to increase as consumers find more ways in which their genomic data may have an impact on their health.[43] Dissatisfaction with PCPs is linked to a list of factors, including: doctors not knowing what to do with the data, not being interested in discussing it, or clients' often-unreasonable expectations of what the data may be able to tell them when the source suggests that a medical doctor should be consulted.[44] It has been proposed

---

2017).

40. *Disclaimer*, NEUROLOGICAL RES. INST., https://knowyourgenetics.com/ (last visited Sept. 29, 2017); *see also* Justin Petrone, *Consumer Genomics Third-Party Tool Makers Look to Develop Services While Keeping User-Friendly Focus*, GENOMEWEB (Oct. 15, 2015), https://www.genomeweb.com/informatics/consumer-genomics-third-party-tool-makers-look-develop-services-while-keeping-user (Quote from Greg Lennon, geneticist and co-founder of Promethease, saying, "Keep in mind that we don't do assays of any sort; Promethease is a literature retrieval system. . .[w]e are trying to connect people as efficiently as possible to what the literature says about those genotypes.").

41. *Id.*; *see also About*, *supra* note 38 ("Disclaimer: Not a doctor! Anything you read here is for informational purposes only. Go talk to your own doctor if you need recommendations or help with anything."); *see also Promethease*, *supra* note 39 ("Before you may use Promethease to retrieve information about the human genome, you must read and agree to the following statements. Please read each statement and check the box next to each one and then click 'I Agree'.").

42. Cathelijne H. van der Wouden et al., *Consumer Perceptions of Interactions with Primary Care Providers After Direct-to-Consumer Personal Genomic Testing*, 164 ANN. INTERNAL MED. 8, 513-22 (2016).

43. *Id.*

44. *Id.* ("These beliefs may originate from various sources (such as company marketing,

that doctors should receive a form of participatory training in medical school regarding genetic tests in order to better understand the experience and results, thus allowing them to better help their patients.[45]

All of this is not to suggest that DTC genomics have no place in medicine, as there have been – and will continue to be – numerous breakthroughs that lead to life changing diagnoses.[46] When dealing with what Dr. Robert B. Darnell, a physician at The Rockefeller University and a founding director of the New York Genome Center, calls the "diagnostic odyssey," a physician well-versed in genomics may be able to rely on DTC genomics in order to effectively determine the best course of treatment.[47] However, there are concerns that relying on genomics may send doctors off on a different odyssey, attempting to navigate through incidental findings in search of those most immediately relevant for diagnosis.[48] Only one thing is clear, consulting your primary care physician may not provide sufficiently reliable results worthy of allowing a DTC genomics provider to avoid liability through a simple waiver.

V. PROPER UNDERSTANDING OF GENOMICS

While everyone should have access to their own genetic information, the results could be devastating without appropriate knowledge and resources

media reports on genetic testing and genealogy, or science education programs) and may or may not be accurate, but they nonetheless contribute to the context in which results are discussed between consumers and PCPs.").

45. Sharp, *supra* note 7, at 750 ("A participatory approach to genetic education is also supported by data showing the effectiveness of interactive forms of medical education, especially pedagogical approaches that use some form of personal involvement.").

46. Rob Preston, *How Genomics Can Lead Doctors to 'Knowing Ahead of Time'*, FORBES (Mar. 30, 2017), https://www.forbes.com/sites/oracle/2017/03/30/how-genomics-can-lead-doctors-to-knowing-ahead-of-time/#12abe3b77da5.

47. *Id.*

48. Bonnie Rochman, *What Your Doctor Isn't Telling You About Your DNA*, TIME (Oct. 25, 2012), http://healthland.time.com/2012/10/25/what-your-doctor-isnt-telling-you-about-your-dna/ ("Dr. Wylie Burke, a geneticist who chairs the Department of Bioethics and Humanities at UW: 'If we open the door to a test that has no clear, well-defined purpose, that is a recipe for unnecessary medical care. Instead, we could say, here are the 1,000 mutations we should check in everyone.'").

available that a simple webpage may not be able to provide.[49] Possibly the most well-equipped group to deal with this issue are genetic counselors who help clients deal with genetic disorders.[50] Typically, they have a master's degree in genetic counseling from an accredited program and are required to pass a board examination.[51] Often, doctors recommend that patients see a genetic counselor when they have concerns about the possibility of a genetic disorder, resulting from either concerning symptoms or a family history.[52]

Genetic counselors work with patients all the way through the process, which includes learning the family history, the decision to have tests, and continued emotional support, especially after the patient receives their results.[53] If someone was seriously concerned about their results from a DTC genomic test, and neither the provider nor the consumer's doctor were able to fully address their concern, it might already be too late for a genetic counselor to handle the situation to the best of their ability.[54] Conducting tests can be an incredibly difficult and emotional decision and it is possible that a genetic counselor would suggest that an individual not undergo genetic testing due to the potential impacts of the results.[55] Normally, a genetic counselor's clientele seek help due to more than simple intellectual curiosity – the patients are seeing a genetic counselor based on a physician's

49. Dobbs, *supra* note 5 ("The desire to use web-based tools to analyze their own DNA sequence is vanishingly rareFalsewe worry about the effect of getting this information may have on the people who live where the sky is blue and the sun is yellow.").

50. *About Genetic Counselors*, NAT'L SOC'Y GENETIC COUNSELORS, http://www.nsgc.org/page/frequently-asked-questions-students (last visited Sept. 29, 2017).

51. *Id.* (stating that an increasing number of states are also in the process of developing laws and professional licensure as a method of regulation in a growing field).

52. *Id.* ("Genetic counselors are specialists. That means that [they] work with a patient's health care provider as a part of a patient's complete care. [They] always communicate what testing is done and what these results mean.").

53. *Id.*

54. Dobbs, *supra* note 5.

55. *About Genetic Counselors*, *supra* note 50 ("Often [genetic counselors] are in a position to help individuals decide what level of information is right for them. In other situations, individuals must make decisions regarding their medical and/or pregnancy care as a result of genetic testing, and the choices can be difficult to navigate.").

recommendation.[56] While the potential of DTC genomics excites many genetic counselors, they also express concerns about consumers' attempts to interpret the information without professional guidance.[57] Even when looking at the list of 23andMe tests that the FDA approved, there are complications, including additional known genes related to the diseases not being tested and the tests' inability to account for family history.[58]

Genetic counselors seem to be the best equipped at dealing with genomic information and 23andMe even mentions the benefit of consulting with a genetic counselor several times on their website.[59] However, 23andMe could further embrace what has become a growing field.[60] Rather than placing a significant amount of important information in front of customers or referring to genetic counselors in the abstract, 23andMe could provide access to genetic counselors that work with the site in order to make sure customers are adequately grasping the information prior to purchasing. In fact, 23andMe is hiring genetic counselors as Medical Affairs Liaisons.[61] Unfortunately the description of this position leaves unclear exactly how much impact this will

56. Dobbs, *supra* note 5 (". . .my experience is with people who come for assessment or testing because they were concerned about something specific – or more likely, because some doctor told them they should – and not out of intellectual curiosity.").

57. Mary E. Freivogel, *FDA Approved 23andMe At-Home Genetic Tests*, NAT'L SOC'Y GENETIC COUNSELORS (Apr. 12, 2017), https://www.nsgc.org/p/bl/et/blogaid=898 ("[Q]uestions you might want to ask yourself before undergoing direct-to-consumer genetic testing are: Would I be comfortable knowing that I'm likely to get a disease that I can't do anything to prevent, and that can't be cured or treated if I do get it? Am I ready to share what I learn with my relatives, since the genetic test results might also provide information about their health risks? Do I have concerns about other diseases NOT included in this particular genetic test?").

58. *Id.*

59. *Learn More About 23andMe's New Genetic Health Risk Reports*, 23ANDMEBLOG (May 19, 2017), https://blog.23andme.com/health-traits/learn-23andmes-new-genetic-health-risk-reports/ ("While 23andMe Genetic Health Risk reports do not diagnose diseases or conditions, they do include potentially important information that you could use to help be more proactive about your health and engage in your own wellness. . .Genetic counselors in particular are well-suited to help people who have questions about genetic risks and genetic testing.").

60. *About Genetic Counselors*, *supra* note 50 ("Genetics is a rapidly expanding field and therefore the demand is growing quickly.").

61. *Medical Science Liaison - Genetic Counselor*, 23ANDME, https://www.23andme.com/en-int/careers/oPB85fwn/ (last visited Nov. 19, 2017).

have on consumers as direct support to customers is only one of their many job requirements.[62] While the cost of bringing on a team of genetic counselors to directly work with clients could be significant, as leaders in a booming industry, 23andMe should reasonably expect increasing costs associated with development and improvement of their business model. The genetic counselors 23andMe could provide would not even be required to deal with the full scope of genetic counselor duties. Specifically, the counselors would work on the front end to ensure anyone with additional questions or hesitations has the help they need. If after receiving their genetic risk factors clients had additional concerns, they would have an established relationship with a genetic counselor. Additionally, 23andMe could contract with the genetic counselors to provide their services through 23andMe to customers for an additional fee. As the study of the human genome continues to develop, allowing more opportunities for DTC services, genetic counselors could play an essential role in helping consumers keep up. This could be a great opportunity that would benefit both industries. However, just because someone can provide answers, should 23andMe be able to avoid liability?

VI. SOLUTION: ENFORCING LIABILITY

The waiver of liability used by 23andMe closely resembles what has been coined a "wrap agreement."[63] A wrap agreement is most commonly associated with "sales of computer software, hardware, and Internet transactions."[64] They represent a waiver of liability attached to a product or

62. *Id.* (Working with customer care specialists to provide direct and indirect support to customers and healthcare providers with advanced health product inquiries).

63. *Terms of Service*, 23ANDME, https://www.23andme.com/about/tos/ (last visited Nov. 19, 2017) ("You may not use the Services if you do not accept the TOS. You can accept the TOS by (1) clicking to accept or agree to the TOS, where this option is made available to you by 23andMe for any Service; or by (2) actually using the Services. In this case, you acknowledge and agree that 23andMe will treat your use of the Services as acceptance of the TOS from that point onwards.").

64. MONIQUE C.M. LEAHY, 150 AM. JURIS. TRIALS 383 § 2 (2017).

service.[65] There are various types of wrap agreements implemented by 23andMe, including click-wrap, where a consumer must check a box, and browse-wrap where the consumer consents just by using the website.[66] Courts have often been hesitant to accept wrap agreements, but there do seem to be some underlying trends in what is adequate.[67] Generally, wrap agreements are accepted when the consumer has notice of the agreement, the site is designed in a way so as to promote the examination of the clearly available terms of service, and the terms of service are not hidden at the bottom of a web page.[68] 23andMe's wrap agreement likely meets these standards; however, their wrap agreement has implications beyond its web-based services.[69]

Allowing 23andMe to waive liability approaches the realm of caveat emptor, also known as "buyer beware," where a consumer takes on full responsibility for their purchase.[70] However, in *Canterbury v. Spence*, the Court mentioned it was unreasonable to require a patient to seek information that the provider has a duty to disclose because caveat emptor is not the standard when dealing with medical services.[71] While DTC genomic tests do not qualify as diagnostic for FDA standards, they certainly should qualify as medical services because they provide risk factors for various diseases.[72]

If an injured party tried to make a claim of medical malpractice for

---

65. *Id.*
66. *Terms of Service*, *supra* note 63.
67. Berkson v. Gogo LLC, 97 F. Supp. 3d 359, 401 (E.D.N.Y. 2015).
68. *Id.*
69. *Terms of Service*, *supra* note 63 ("Once you obtain your Genetic Information, the knowledge is irrevocable. You should not assume that any information we may be able to provide to you, whether now or as genetic research advances, will be welcome or positive.").
70. *Caveat emptor*, BLACK'S LAW DICTIONARY (10th ed. 2014).
71. Canterbury v. Spence, 464 F.2d 772, 783 n. 36 (D.C. Cir. 1972).
72. *FDA Allows*, *supra* note 4 ("The [Genetic Health Risk] tests are intended to provide genetic risk information to consumers, but the tests cannot determine a person's overall risk of developing a disease or condition. In addition to the presence of certain genetic variants, there are many factors that contribute to the development of a health condition, including environmental and lifestyle factors.").

misdiagnosis, they would likely have difficulty proving that the duty of the company to a consumer is similar to that of a doctor to a patient, that a risk factor is significantly comparable to a diagnosis, or that the proper care was not used in processing the results.[73] Intentional infliction of emotional distress also appears to have too high a standard for a plaintiff to succeed as it requires extreme and outrageous behavior unlikely to come from a business.[74] However, if there is a potential for physical harm, prospects may look better following a claim for negligent infliction of emotional harm.[75] As previously mentioned, the FDA had legitimate concerns about the potential for self-treatment in reliance on DTC genomic test results, and this self-treatment could lead to physical harm whether it is related to diet, activity, or medication.[76] The use of a wrap agreement in the context of waiving liability for a medical service is problematic in regards to consumer protections and should therefore not function as a proper bar to liability. If a situation of real physical injury were to take place, the court should grant the consumer an opportunity to litigate.

VII. CONCLUSION

DTC genetic tests are an incredible advancement in the understanding of

73. 70 C.J.S. PHYSICIANS AND SURGEONS § 95 (2017) ("A physician, surgeon, or other health-care provider is liable for a failure, due to a lack of the requisite skill or care, to diagnose correctly the nature of the ailment, with resulting injury or detriment to the patient, but a health-care provider is not liable for a mistake in diagnosis if he or she uses the proper degree of skill and care.").

74. RESTATEMENT (THIRD) OF TORTS § 46 (AM. LAW INST. 2012) ("An actor who by extreme and outrageous conduct intentionally or recklessly causes severe emotional harm to another is subject to liability for that emotional harm and, if the emotional harm causes bodily harm, also for the bodily harm.").

75. RESTATEMENT (THIRD) OF TORTS § 47 (AM. LAW INST. 2012) ("An actor whose negligent conduct causes serious emotional harm to another is subject to liability to the other if the conduct: (a) places the other in danger of immediate bodily harm and the emotional harm results from the danger. . .").

76. Gutierrez, *supra* note 14 ("The risk of serious injury or death is known to be high when patients are either non-compliant or not properly dosed; combined with the risk that a direct-to-consumer test result may be used by a patient to self-manage, serious concerns are raised if test results are not adequately understood by patients or if incorrect test results are reported.").

genetic disorders and genetics in general. However, it is problematic for a business to be able to both obtain FDA approval and avoid liability simply by suggesting that if a customer has concerns, they should consult a medical provider because the company does not intend for the medical services they provide to be diagnostic. Often, doctors do not receive training on how to deal with this kind of risk factor analysis and are unable to provide patients with the reassurances they desire. This ability to skirt liability creates a void of consumer protections where companies refer consumers to a possible dead end with nowhere else to turn. Genetic counselors are much more prepared for this responsibility but the average DTC genomics customer would be unlikely to seek a genetic counselor's help prior to receiving results. Regardless, genetic counselors should not replace doctors as a shield for companies to hide behind. These companies provide not only a product on the market but also a medical tool that has the potential to cause serious concerns for their consumers. As the market continues to develop, both courts and the FDA should hold companies responsible for the foreseeable harm resulting from their product.

Cloud-Based EHR: Demonstrating Meaningful Use and Interoperability for 2018

Timothy Gaffud

I. INTRODUCTION

"Meaningful use" of electronic health records ("EHR") has demonstrated to improve cost, efficiency, and quality of health care.[1] Accordingly, the federal government implemented a nationwide effort to promote the adoption and utilization of EHR by creating the Medicare and Medicaid Meaningful Use EHR Incentive Programs ("Meaningful Use Programs") for eligible providers – specific hospitals and clinicians.[2] The Meaningful Use Programs are divided into three stages to provide flexibility in determining requirements for achieving "meaningful use" over time.[3] One reason for this progressive structure is to give providers who may experience delays in implementing meaningful EHR systems, whether due to higher training needs or other unforeseen circumstances, the opportunity to participate in the incentive programs when they are ready to do so later on.[4] Another reason for the gradual approach is to create appropriate requirements for future EHR meaningful use based on the advancement of technology and transformation of provider practice experience.[5]

1. Jenny Carroll & Daniel O. Carroll, *Electronic Health Records*, 299 N.J. LAW 55, 55 (2016).
2. *See* Medicare & Medicaid Programs; Electronic Health Record Incentive Program, 75 Fed. Reg. 44313, 44321 (July 28, 2010) [hereinafter, EHR Incentive Program] (describing the HITECH act and its Medicare and Medicaid meaningful use incentive program to eligible hospitals and providers).
3. *Id.*
4. *Id*. at 44320.
5. *Id.* at 44321.

Participation to the Meaningful Use Programs was voluntary at first and providers received substantial incentive payments in the first five years.[6] No penalties were imposed then, but since 2015, program participants who fail to meet "meaningful use" based on the respective objectives and measures when they joined the program are subject to significant reductions in Medicare payments.[7]

At any stage, the cost of adopting standard EHR systems that meet the requirements is high and can range from tens of thousands of dollars to several million.[8] Nevertheless, the federal government believes that the long-term benefits of the Meaningful Use Programs outweigh the upfront costs.[9] By 2018, all eligible providers must meet eight requirements under Stage 3 of the Meaningful Use Programs, regardless of when the providers joined.[10] Those who are at risk of being non-compliant or who have been non-compliant, whether due to inadequacy of the provider's current EHR system or complete lack thereof, have no choice but to invest in purchasing a new system or in upgrading a current one.[11]

Unfortunately, some providers simply can't afford to adopt traditional on-premise EHR systems, the standard system.[12] For those who have already

6. Medicare & Medicaid Programs; Electronic Health Record Incentive Program – Stage 3 and Modifications to Meaningful Use in 2015 Through 2017; Final Rule, 80 Fed. Reg. 62761, 62930 (Oct. 16, 2015) [hereinafter, EHR Stage 3].

7. *Id.*

8. *See id.* at 62935 (describing costs of EHR adoption for both eligible professionals and hospitals); *see also 8 Epic EHR Implementations with the biggest price tags in 2015*, BECKER'S HEALTH IT & CIO REV. (Jul. 1, 2015), https://www.beckershospitalreview.com/healthcare-information-technology/8-epic-ehr-implementations-with-the-biggest-price-tags-in-2015.html (enumerating a list of hospital systems that have spent a substantial amount of money to implement EHR systems, dedicated to installing software, hardware, data conversion, and additional personnel).

9. *Id.* at 62929.

10. *Id.* at 62766.

11. *See generally* Nicolas Terry, *Information Technology's Failure to Disrupt Heath Care*, 13 NEV. L. J. 722, 737 (2013) ("According to 2012 survey, while almost 35% of acute care hospitals had adopted EMRs by 2011, only 8.8% had comprehensive systems.").

12. *See* Rachel Arndt, *Internet-Based EHRs Gaining Some Customers but Still a Small Segment*, MODERN HEALTHCARE (Aug. 7, 2017), http://www.modernhealthcare.com/article/20170807/TRANSFORMATION02/170809936

implemented traditional EHR systems and plan to continue using them after purchasing upgrades may find themselves passing the system's staggering costs on to their patients.[13] Financial pressures stemming from the shift to value-based health care, reduced provider revenue, and the need to do more work necessitate innovations that bring economic, operational, and functional advantages.[14] At its core, the flexibility to adapt and innovate is what the federal government intended in the first place to achieve successful electronic exchange of health information.[15] Given that implementing traditional EHR systems carry extensive costs to providers, and potentially to patients as well, it seems counterintuitive to continue to adopt such systems if one of the main drivers of EHR utilization was to reduce health care cost.[16]

(stating that a 14-bed critical-access hospital doesn't have the money to implement a traditional EHR system or client-server based system – can't afford the software nor afford to hire IT employees) [hereinafter, *Internet-Based EHRs*]; *see also* Greg Slabodkin, *Epic Shift: Demand for Cloud EHR Service is Soaring*, HEALTH DATA MGMT. (Feb. 1, 2016, 05:45 AM), https://www.healthdatamanagement.com/news/epic-shift-demand-for-cloud-ehr-service-is-soaring (stating that a shift of focus to cloud-based EHRs because of increased cost pressures on providers and low productivity and return on investment from on-premise systems).

13. *See* Zina Moukheiber, *The Staggering Cost of an Epic Electronic Health Record Might Not Be Worth It*, FORBES (Jun. 18, 2012, 07:59 AM), https://www.forbes.com/sites/zinamoukheiber/2012/06/18/the-staggering-cost-of-an-epic-electronic-health-record-might-not-be-worth-it/#3c7f7af46d35 (claiming that due to increased capital spending by hospitals from adopting EHR systems, considering the changes in rules and reimbursements, will cause hospitals to pass on the "cost of their pricey EHRs" to their patients).

14. *See* CLOUD STANDARDS CUSTOMER COUNCIL, IMPACT OF CLOUD COMPUTING ON HEALTHCARE VERSION 2.0 7 (2017) (introducing, first, "cost pressures stemming from the need to do more and higher quality work with fewer and fewer and more costly resources and also reduced revenue. Expectations for better outcomes, higher quality treatment and more value from the health care services provided increase the need for point-of-care access to medical data and the parallel evolution and adoption of mobile devices" and, then, explaining how health care providers are utilizing the economic, operational, and functional advantages of a cloud technology to meet that need).

15. *See* American Recovery and Reinvestment Act, H.R. 1, 111th Cong. 3013 (2009) [hereinafter ARRA] (stating the discretionary power of the Secretary who shall evaluate the state activities under HITECH and, "in the determination of the Secretary, will lead towards the greatest improvement in quality of care, decrease in costs, and the most effective authorized and secure electronic exchange of health information.").

16. *See generally* EHR Incentive Program, *supra* note 2, at 44327 ("There are significant gains that meaningful use can achieve . . . significant other benefits such as engaging patients more fully in decisions affecting their health and reducing costs through increased efficiency of care.").

In effect, it seems apparent that providers need to adopt more feasible non-traditional EHR systems to achieve "meaningful use" in the future.

Cloud computing offers, among other things, reduced expenses, enhanced usability, and decreased infrastructure needs as compared to traditional on-premise systems.[17] Taking EHR to the cloud and developing a "meaningful use" system there is the innovation that health care reform needs.[18] This article proposes that adopting a cloud-based EHR system is not only a more feasible option for eligible providers looking to achieve EHR meaningful use for 2018, but it is the only option to advance interoperability and exchange under the "meaningful use" requirements of Stage 3. First, this article presents the legislation that gives authority to the Meaningful Use Programs. Second, this article shows how a cloud-based EHR system is more feasible than a traditional EHR system by distinguishing the two systems. Third, this article illustrates how a cloud-based EHR system meets all eight objectives of the Meaningful Use Programs in Stage 3 to demonstrate full compliance for 2018 and, additionally, how the requirements of the Meaningful Use Programs cultivated the environment that leaves cloud-based systems as the only option to achieve EHR interoperability and exchange.

II. HITECH AND THE MEANINGFUL USE PROGRAMS

The HITECH Act was enacted as part of the American Recovery and Reinvestment Act of 2009 to achieve health care reform by implementing a nationwide infrastructure that utilized health information technology –

17. *See* Douglas R. Richmond, *Confidentiality Problems for Lawyers in Today's Digital Era*, 33 ENERGY & MIN. L. INST. 183, 196 (2012) ("Cloud computing may be desirable because it offers substantial cost savings, ease of use, constant service, mobility, and reduced infrastructure and management needs.").

18. *See generally* CLOUD STANDARDS CUSTOMER COUNCIL, *supra* note 14, at 4 (presenting that the rising demand for health care services, the focus on preventative health care, the need for health care delivery transformation, the impact of regulation on financial risks, and the influence of digitalization all influence the role of IT and, by association, the role of cloud computing in health care).

EHR.[19] The HITECH Act created the Meaningful Use Programs that set out to provide $27 billion in incentives for eligible providers to promote the adoption and meaningful use of EHR by these providers.[20] As of August 2017, more than 639,300 eligible providers are registered in the Meaningful Use Programs.[21]

The Meaningful Use Programs are divided into three stages – each stage having a set of objectives designed for specific goals. In 2011, Stage 1 laid the foundation of the "meaningful use" infrastructure by focusing on the electronic capture and use of EHR.[22] In 2012 to 2014, Stage 2 looked to improve coordination between provider-to-provider and provider-to-patient relationships by demanding the utilization and exchange of EHR.[23]

In 2015, the programs entered their final stage.[24] Stage 3 consolidates all eligible providers into a single set of requirements by 2018, simplifying the programs and setting a sustainable long-term foundation for the programs' future.[25] This stage is designed to meet three policy objectives – to standardize quality improvement efforts, to improve access and quality of healthcare while reducing cost, and to promote interoperability and health information exchange.[26]

The eight objectives and measures must be met by all eligible providers,

19. Jenny Carroll & Daniel O. Carroll, *Electronic Health Records*, 299 N.J. LAW 55, 55 (2016).

20. ARRA, *supra* note 15, at 13001.

21. *Data and Program Reports*, CMS.Gov, https://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/DataAndReports.html (last updated Oct. 11, 2017).

22. EHR Stage 3, *supra* note 6, at 62765.

23. Medicare & Medicaid Programs; Electronic Health Record Incentive Program – Stage 2; Health Information Technology; Standards, Implementation Specifications, and Certification Criteria for Electronic Health Record Technology, 2014 Edition; Revisions to the Permanent Certification Program for Health Information Technology, 77 Fed. Reg. 53967, 53973 [hereinafter, EHR Stage 2].

24. EHR Stage 3, *supra* note 6, at 62765.

25. *Id.*

26. *Id*. at 62766.

regardless of when they joined the Meaningful Use Programs.[27] Six of the eight can be organized into two categories – one for clinical effectiveness and safety, and one for health information exchange.[28] Clinical effectiveness and safety are measured in terms of computerized provider order entry ("CPOE") and electronic prescribing.[29] On the other hand, health information exchange is measured in terms of patient electronic access, coordination of care through patient engagement, health information exchange during transfer of care, and public health and clinical data registry reporting.[30] The two uncategorized goals are measured in terms of protecting patient information and implementing decision support interventions on high-priority health conditions.[31]

III. CLOUD-BASED SYSTEM V. TRADITIONAL SYSTEM

A *cloud* is an internet-based infrastructure that provides computation, software, data access, and data storage on remote servers owned and maintained by a vendor.[32] A cloud-based system offers substantial economic benefits over a traditional system.[33] Unlike a traditional system, a cloud-based system does not require on-premise hardware, and accordingly, the substantial upfront expenses from such hardware are non-existent.[34] A cloud-based system may only require a monthly subscription fee to the

27. *Id.* at 62772-73.
28. *Id.* at 62,772.
29. *Id.*
30. *Id.*
31. *See id.* at 62826 (providing a table that lists "Protect Patient Health Information" and "Clinical Decision Support" as two of the eight objectives).
32. Richmond, *supra* note 17, at 196.
33. *Internet-Based EHRs*, *supra* note 12.
34. Larry Combs, *Cloud-Based Computing in the Forecast*, 105 J. AM. WATER WORKS ASS'N 60, 60 (2013); *see also* CLOUD STANDARDS CUSTOMER COUNCIL, *supra* note 14, at 5 ("Cloud computing provides an IT infrastructure that allows . . . entities . . . to leverage improved computing capabilities at lower initial capital outlays than previously required by purchase or long-term licensing.").

vendor in order to operate.[35] Furthermore, a traditional system requires constant dedication of time and resources to refine and improve the utilization of the system – dedication "far beyond its installation and go-live."[36] Thus, the traditional system demands significantly more resources in both its initial installation and subsequent up-keep. While there are options for cutting costs in a traditional system by adopting a "slimmed-down" version of its platform, the usability and interoperability shortcomings of the traditional system may remain unaddressed.[37]

A cloud-based system provides functional and operational benefits beyond cost-savings.[38] First, because all data in the cloud can be accessed from any location where internet is available,[39] a cloud-based system boasts remote capabilities that a traditional system does not, and cannot, provide.[40] A traditional system, on the other hand, requires a hardware server installed in a physical location to store data and process software and limits the user's access to that in-house location.[41] Second, because of the cloud-based system's remote capability, the cloud vendor can access, configure, update, and secure data externally – allowing for more efficient responses during

35. *Internet-Based EHRs*, *supra* note 12.

36. Dale Sanders, *Epic EMR Adoption, Utilization, and Cos*t, HEALTHCARE INFORMATICS (Apr. 23, 2009) https://www.healthcare-informatics.com/blogs/dale/epic-emr-adoption-utilization-and-cost; *see also Internet-Based EHRs*, *supra* note 12 (suggesting that the expenses of employing an internal staff to manage traditional EHR systems is unaffordable).

37. *See* Shaun Sutner, *New Epic EHR Systems to Carry Lower Prices, Aimed at Smaller Hospitals,* SEARCHHEALTHIT (Mar. 1, 2017) http://searchhealthit.techtarget.com/news/450414132/New-Epic-EHR-systems-to-carry-lower-prices-aimed-at-smaller-hospitals ("While potential users who have long wanted to look at an Epic EHR but couldn't afford it will soon have the opportunity . . . Epic should also now refocus on improving usability and interoperability.").

38. CLOUD STANDARDS CUSTOMER COUNCIL, *supra* note 14, at 7.

39. *Id.* at 8.

40. *See* Salbodkin, *supra* note 12 (listing distinguishing factors of cloud-based EHR from in-house EHR which includes financial savings, ease of implementation, auto-scalability, compatibility with disparate healthcare systems, and remote accessibility).

41. Aiden Spencer, *Differences Between Cloud-Based and Regular EHRs*, AM. J. MANAGED CARE (Feb. 10, 2017), http://www.ajmc.com/contributor/aiden-spencer/2017/02/differences-between-cloud-based-and-regular-ehrs?p=2.

software updates, data security issues, and general system configuration.[42] Unlike the cloud-based system, updating and maintaining the traditional system is complicated, time-consuming, and costly.[43]

While a cloud-based system is intangible, it is not less comprehensive in service than a traditional system.[44] Data analysis, design, development, and implementation can all be performed in the cloud.[45] Considering that a cloud-based system provides comprehensive data use at lower cost, increased functionality, and enhanced efficiency, choosing a cloud-based system over the traditional system for data storage and utilization not only becomes a more feasible option, but, ultimately, becomes the right decision. Various industries took notice of the cloud's benefits and adopted cloud-based systems in their respective practices – e-learning, water management, car-sharing, retail, hospitality, and social networking.[46] The cloud transformed organizations for the better and it became a fundamental means for businesses to be able to keep up with change.[47]

---

42. *See* Combs, *supra* note 34, at 62 (claiming that the cloud provides uptime reliability, enhanced data back-up, and continuous service even during power outage or natural disaster).

43. Spencer, *supra* note 41.

44. Frank Pasquale & Tara Adams Ragone, The Future of HIPAA in the Cloud 7 (June 30, 2013) (white paper) (on file with Seton Hall Center for Health & Pharmaceutical Law & Policy) (describing the sensitive issues that cloud-based systems are capable of handling such as patient account management, patient management, HIPAA compliance, patient portals, appointment scheduling, and meaningful use requirements).

45. *See* Ghazal Riahi, *E-Learning Systems Based on Cloud Computing: A Review*, 62 PROCEDIA COMPUT. SCI. 352, 354 (2015) (listing four areas in which the cloud improves efficiency and decreases cost).

46. *See* Narinder Singh, *US Healthcare – The Cloud Computing Sequel, Part 1*, DIGINOMICA (May 11, 2016), https://diginomica.com/2016/05/11/us-healthcare%E2%80%8A-%E2%80%8Athe-cloud-computing-sequel-part-1 (claiming that cloud technology redefined business industries – Apple, Google, Facebook, Amazon, Uber, and Airbnb); *see also* Riahi, *supra* note 45, at 352 (illustrating the impact of cloud on efficiency and cost in e-learning); *see also* Combs, *supra* note 34, at 60 (illustrating comprehensive utility of cloud-based system in water management);

47. Singh, *supra* note 46.

IV. CLOUD-BASED EHR: STAGE 3 AND INTEROPERABILITY

A. Cloud-Based EHR System Demonstrates Meaningful Use for 2018

By 2018, all eligible hospitals and clinicians must meet objectives and measures in eight areas – Computerized Provider Order Entry, Electronic Prescribing, Patient Electronic Access, Implement Decision Support Interventions on High-Priority Health Conditions, Coordination of Care through Patient Engagement, Health Information Exchange, Public Health and Clinical Data Registry Reporting, and Protect Patient Information.[48] A cloud-based system easily addresses these requirements.

Because the system stores EHR online, rather than in a single on-premise location, the patient and provider can access health information electronically at any location where a computer and an internet connection is available.[49] Furthermore, a cloud-based EHR system is adaptable to mobile devices and other portable platforms and, as a result, the means of accessing EHR becomes more convenient through mobility.[50] An article in *Clinical Diabetes and Endocrinology* demonstrates how enhanced access and ease of use effectively engages patients in the coordination of their care – giving diabetic patients the ability to store, view, and transmit their data online using mobile devices.[51] The article recognizes that technologies that are familiar and easily navigable to patients promote self-engagement in their care and lead to

48. EHR Stage 3, *supra* note 6, at 62772-73.

49. *See* Rachel Z. Arndt, *Will Epic's New Record-Sharing Data Tool Solve Interoperability Challenges?*, MOD. HEALTHCARE (Sep. 16, 2017) http://www.modernhealthcare.com/article/20170916/NEWS/170919908 [hereinafter *Epic's New Record-Sharing Data Tool*] (stating that a web-based medical record tool allows patients and providers to access records through a web browser, only requiring a computer and internet access).

50. CLOUD STANDARDS CUSTOMER COUNCIL, *supra* note 14, at 8.

51. Viral N. Shah & Satish K. Garg, *Managing Diabetes in the Digital Age*, 1 CLINICAL DIABETES & ENDOCRINOLOGY 1, 3 (2015) (presenting various web-based diabetes mobile apps that provide online electronic logs where blood glucose data can be entered, saved, printed later, and emailed to providers).

positive results.[52] The article's finding is promising as it may be applied to other conditions as well.

A Cloud-based EHR system enhances data access and sharing among various levels of health care.[53] Both physician and patient can access current medications, laboratory results, diagnostic imaging, and other provider ordered entries. An article in *Infection Control and Hospital Epidemiology* reveals that a cloud-based EHR system provides tools that result in more complete health information and less medical discrepancies.[54] A self-reporting tool prompts patients to answer questions using pre-made answers that help reveal contraindications.[55] In certain events, the self-reporting tool urges patients to elaborate with further details and becomes another opportunity to collect more patient information.[56] By capturing complete data on an accessible cloud-based system, the patient can be properly linked to specific identifiers (e.g., lot numbers, expiration dates, vaccine names, manufacturers) and elements that enhance the risk of medical discrepancies such as illegible documentation and erroneous recording are eliminated.[57] Data completeness is crucial during transitions of care as it prevents gaps in patient information that may bring severe risks if actual contraindications are

52. *Id.* at 2

53. *See* JOHN HASKEW ET AL., IMPLEMENTATION OF A CLOUD-BASED ELECTRONIC MEDICAL RECORD TO REDUCE THE GAPS IN THE HIV TREATMENT CONTINUUM IN RURAL KENYA 1, 3 (Aug. 7, 2015) (describing the cloud-based model as an infrastructure where data is centrally hosted, rather than by individual clinic, which enhances data access and sharing at different levels of health care).

54. *See* Monica Salazar et al., *Web Based EHR Improve Data Completeness and Reduce Medical Discrepancies in Employee Vaccination Programs*, 33 INFECTION CONTROL & HOSP. EPIDEMIOLOGY 84, 86 (2012) (finding that healthcare workers provided more complete information regarding their eligibility to receive flu vaccine when they used self-administered, Web-based EHR and, as a result, reduced medical discrepancies).

55. *Id.* at 85 (the electronic forms available pertained to consent to vaccination, contraindications, and declination).

56. *See generally id.* (illustrating the mechanism for when the employee refuses to get vaccinated – prompting the employee to provide his or her reason for declining, educating them on the importance of worker vaccination, and allowing time to change his or her mind before the employee submits the declination form).

57. *Id.* at 85-86.

not captured.[58]

The accuracy of the EHR appropriately activates built-in alerts and clinical decision support features, upon identifying contraindications, and recommendations for better clinical options are subsequently introduced.[59] The complete data allows for efficient tracking and evaluation of clinical performance and outcomes, making it possible for government agencies to quickly analyze trends and formulate the best practice recommendations that appear in the clinical decision support features.[60] At a local scale, at least, this type of mechanism is effective in identifying specific high-risk patients that require immediate clinical treatment.[61] As a result, it enhances the providers' response and utilization of computerized order entry and electronic prescribing as the providers are alerted to give timely medical intervention when such necessity is identified.[62] A cloud-based EHR system provides practical benefits that improve the quality of health care delivery at various levels.

A cloud-based EHR system is equipped with various safeguards that adequately protects patient information. Although the cloud-based system lacks physical structure, it is fortified with heavy encryption protocols that are "almost impossible" to crack.[63] Furthermore, the system is subject to

58. *See* Salazar, *supra* note 54, at 84 (stating that an employee previously experienced severe adverse reaction to a vaccine, a contraindication, but was still given the vaccine due to medical discrepancy).

59. *See id.* at 86 (stating that alerts highlight contraindications and display the best vaccination choices for each individual based on government agency recommendations).

60. *See id.* ("EHRs facilitate efficient tracking of participation, program performance, and vaccination outcomes . . . completion of state-mandated reporting were greatly expedited by real-time electronic data capture").

61. *See* HASKEW ET AL., *supra* note 53, at 8 (reporting that implementation of cloud-based EHR in an HIV study helped identify patients who met the criteria for treatment eligibility).

62. *See id.* (effective identification of eligible HIV patients allowed for timely treatment of those patients).

63. Willie Mata, *Is Cloud Safe for Healthcare Information?* CTR. TECH'S (June 15, 2015) https://centretechnologies.com/is-cloud-safe-for-healthcare-information.

stringent security monitoring by the vendor's IT team at all times.[64] Next, the system is not susceptible to damage by natural disaster due to its non-physical infrastructure.[65] Additionally, the stored EHR is routinely backed-up, ensuring that the data is up-to-date and preserved.[66] Lastly, the federal government extended substantial privacy and security liability to non-clinical corporations that manage patient information such as cloud vendors.[67] Since cloud vendors are liable for managing EHR, they a have significant incentive to ensure that the EHR is in fact well-protected.

B. Stage 3 Requires Cloud-Based EHR System for Interoperability

Although the Meaningful Use Programs effectuated widespread EHR adoption,[68] EHR interoperability and exchange continue to be inadequate.[69] Critics argue that the requirements of the programs are fixated on defining the correct use of EHR, rather than advancing its interoperability and exchange.[70] The number of EHR exchanges that do take place are limited to narrow networks – within the local area or between organizations that share common EHR system vendors.[71] This limitation is attributed to the EHR

64. *See id.* (claiming that patient data is being delegated to an experienced IT team that is devoted to the security of the cloud "24/7").

65. *Id.*

66. *See* Combs, *supra* note 34, at 62 (claiming that data back-up redundancy and disaster recovery capabilities of cloud-based systems are far beyond those found in typical IT departments).

67. OFFICE OF THE NAT'L COORDINATOR OF HEALTH INFO. TECH., CONNECTING HEALTH AND CARE FOR THE NATION: A SHARED NATIONWIDE INTEROPERABILITY ROADMAP DRAFT VERSION 1.0 13 (2015) (stating that business associates that perform functions involving patient information are required to follow HIPAA Privacy and Security Rules that seek to protect patient privacy).

68. *See* Kalle Deyette, *HITECH ACT: Building an Infrastructure for Health Information Organizations and a New Health Care Delivery System*, 8 ST. LOUIS U. J. HEALTH L. & POL'Y 375, 413 (2015) (claiming that over 200,000 Medicare EHR Incentive Program participants are utilizing EHR).

69. *See* Julia Adler-Milstein, *Moving Past the EHR Interoperability Blame Game*, NEJM CATALYST (Jul. 18, 2017), https://catalyst.nejm.org/ehr-interoperability-blame-game/ ("The substantial increase in electronic health record across the nation has not led to health data that can easily follow a patient across care settings.").

70. Deyette, *supra* note 68, at 415-16.

71. *Id.* at 416.

itself and its lack of standardization, inhibiting interoperability on a larger scale due to lack of universal compatibility.[72]

Adopting a standardized EHR system would most likely solve the issue of incompatibility between separate and distinct EHR systems.[73] One way to achieve standardization is through the use of a universal language that provides a means for distinct EHR systems to exchange data without having to entirely alter their EHR format.[74] Another way is to form a centralized health information exchange that is regulated by a health information organization which utilizes a uniform EHR format.[75] Unfortunately, neither forms of standardization are feasible due to the high costs associated in implementing the systems, the privacy and security risks associated, and the impracticalities of each model.[76]

No stage of the Meaningful Use Programs explicitly defines a standard that easily establishes universal EHR interoperability and exchange. Stages 1 and 2 were merely preparatory stages, building the EHR database and learning how to effectively implement EHR into clinical practice.[77] Their requirements did not demand for disparate systems to actually interact. Stage 1 and 2 requirements did not expose the traditional system's major

72. *See id.* (quoting an ONC-report, "[e]lectronic health information is not yet sufficiently standardized to allow seamless interoperability . . . . ").

73. Terry, *supra* note 11, at 744.

74. *Id.*

75. *See* Deyette, *supra* note 68, at 380 (describing the HIO as a formal organization that oversees and governs health information exchanged between all stakeholders within health care according to a national standard).

76. *See id.* at 420 (listing the barriers for HIO: privacy and security concerns, substantial expense to implement, and difficulty for providers to integrate the model in clinical practice); *see also* Terry, *supra* note 11, at 744 (explaining that the universal language model failed because: it did not provide a coherent roadmap for short term implementation; it set-off security and privacy alarms; and its model was difficult to apply to available EMRs)

77. *See* EHR Incentive Program, *supra* note 2 at 44321 (stating that Stage 1 focuses on capturing and tracking health information to create the foundation for later years, but that data for coordination of care can be structured or unstructured); *see also* EHR Stage 2, *supra* note 23, at 53973 (increasing demands for electronic prescribing requirements but only an "expectation that providers will electronically transmit patient care summaries").

shortcoming – limiting EHR interoperability and exchange to narrow networks due to unstandardized formatting.[78] Perhaps, the biggest mistake of the Meaningful Use Programs was that its progressive approach to defining "meaningful use" failed to require a universal standard in the early stages, consequently resulting in the disparate EHR systems of today.

Stage 3 demands actual interoperability and exchange, unlike the earlier stages.[79] Its requirements make traditional EHR system obsolete and noncompliant – requiring beyond the capabilities of the traditional systems because such systems are limited in providing EHR access and sharing.[80] The subsequent upgrades that traditional systems need to achieve meaningful use are no longer feasible for providers and patients.[81] Stage 3's success in advancing interoperability and exchange will depend on the infrastructure that it seeks to establish now.

Whether by fate or design, Stage 3 requires the adoption of the cloud-based EHR not just because it is the best choice moving forward, but it is the only choice to achieve standardization for interoperability and exchange under its requirements. Other forms of standardized innovations are not feasible. A cloud is a virtual infrastructure, uninhibited by physical constraints. It is secure and achieves "meaningful use." A cloud-based system is accessible, functional, and adaptable – an appropriate foundation to foster EHR interoperability and exchange. Similar to the methods of Stage 1, capturing EHR into the cloud is the first step to reach standardization. This transition is, at the very least, a step closer to the goals of national exchange and integration of EHR by taking EHR to an infrastructure that promotes

78. *See generally* Terry, *supra* note 11, at 745 (claiming that "too much patient data is trapped by the proprietary formats used in current-generation EMRs").

79. EHR Stage 3, *supra* note 6, at 62770.

80. *See* Haskew, *supra* note 53, at 3 (removing a local infrastructure enhances data access and sharing).

81. *See* Singh, *supra* note 46 (claiming that even minor software updates for client-based systems is time consuming and decreases productivity).

standardization through accessibility, functionality, and adaptability.

VI. CONCLUSION

A cloud-based EHR system provides cost, functional, and operational advantages over traditional EHR systems. A cloud-based EHR system addresses all eight requirements of the Meaningful Use Programs for 2018. Eligible providers who are looking to implement new EHR systems or upgrade a current one should consider cloud-based services, especially if they are unable to invest substantial expenses upfront. Cloud-based EHR systems are not less comprehensive than traditional systems and they offer complete patient information protection. Cloud-based systems promotes standardization through accessibility, functionality, and adaptability. Under the requirements of Stage 3, a cloud-based EHR system becomes the only feasible solution today to achieve EHR interoperability and exchange. Moving forward, adopting a cloud-based EHR system becomes the right choice for eligible providers not only looking to meet the demonstrate "meaningful use" for 2018, but also to advance interoperability and exchange.

Targeted Advertising in the Healthcare Industry: Predicted Privacy Concerns

Lianne Foley

I. INTRODUCTION

In September 2017, the Attorney General of Massachusetts settled its suit against Massachusetts-based advertising company, Copley Advertising, LLC, for violating state consumer protection laws.[1] Copley had created a "geofence" around Massachusetts reproductive health facilities, tracking consumers' physical location and disclosing that location to third-party advertisers. Geofence technology constructs a perimeter around a pre-determined area and signals a mobile device to take an action once inside the perimeter, through the device's mobile application ("app").[2] The Attorney General alleged that targeting the consumer with potentially unwanted advertising based on inferences about his or her private, sensitive, and intimate medical or physical condition—all without the consumer's knowing consent—constituted a breach of Massachusetts's "Unfair Methods of Competition or Deceptive Acts or Practices" law.[3] Copley constructed the geofence on behalf of a third party, Bethany Christian Services, a global

1. *AG Reaches Settlement with Advertising Company Prohibiting 'Geofencing' Around Mass. Healthcare Facilities,* ATT'Y GEN. OF MASS., (Sept. 28, 2017), http://www.mass.gov/ago/news-and-updates/press-releases/2017/2017-04-04-copley-advertising-geofencing.html [hereinafter *Att'y Gen. of Mass.'Geofencing'*].

2. Bradley Ryba, *iHeartGeo-Fencing?: The Section 114 Exemption That Illustrates Why Full Sound Recording Rights Are the Sine Qua Non For a Vibrant Music Industry*, 20 MARQ. ITELL. PROP. L. REV. 33, 35 (2016).

3. *Massachusetts AG Fences off Geofencing Ad Campaign*, MANATT, PHELPS, & PHILLIPS, (Sept. 28, 2017), https://www.manatt.com/Insights/Newsletters/Advertising-Law/Massachusetts-AG-Fences-off-Geofencing-Ad-Campaign; *see* MASS. GEN. LAWS ch. 93A, §2 (2017).

pregnancy counseling and adoption service.[4] Copley was hired to create a geofence around medical facilities, including women's reproductive clinics, not only in Franklin, Massachusetts but also in New York City; Columbus, Ohio; Richmond, Virginia; St. Louis, Missouri; and Pittsburgh, Pennsylvania.[5] The purpose of geofencing was to target "abortion-minded women" as they sat in waiting rooms at health clinics.[6] The advertising techniques included text such as "Pregnancy Help," "You Have Choices," and "You're Not Alone."[7] If the consumer clicked on such advertisement, he or she would be directed to a webpage that featured abortion alternatives and access to a live web chat with a "pregnancy support specialist."[8] Ultimately, Copley and the Attorney General of Massachusetts agreed to a settlement.[9]

This article endeavors to explain how targeted advertising, and geofencing in particular, will negatively affect privacy of the consumers in the healthcare industry. Specifically, Part II of this paper will explain the various geological technologies, followed by Part III which will compare the Copley Settlement to another geofencing case, *United States of America v. InMobi Ltd*. Lastly, Part IV will demonstration the negative impact of targeted advertising and geofencing in the Healthcare industry.

II. THE GEOS: LOCATION, FENCING & TARGETING

Prior to modern technology, healthcare advertisers had to reach patients through traditional means like radio, television, and newspaper ads. However, internet usage is a commonality of modern life. Almost every time an individual uses the Internet, his or her user identity is traced, and by

4. *Id.*
5. Assurance of Discontinuance, *Commonweatlh v. Copley Advert., LLC & John F. Flynn*, at 3 (Mass. Sup. Ct. filed on Apr. 4, 2017) [hereinafter *Copley Advert. Settlement*].
6. *Att'y Gen. of Mass.'Geofencing*,' *supra* note 1.
7. *Id*.
8. *Id.*
9. *Id.*

extension, his or her basic privacy is violated.[10] Geolocation technologies can pin-point an internet user's location by locating his or her own computer or wireless device.[11] Specifically, satellite technology allows a service provider (e.g., Comcast, or AT&T) to read the internet user's Internet Protocol (IP) address to track their location.[12] According to experts, geolocation accuracy is 85 to 98 percent at the state level and over 99 percent at the national level.[13] Geolocation's potential for accuracy has fostered high usage for advertising.[14] Specifically, "target advertising," helps advertisers "deliver their persuasive message to audiences who are most likely to be interested."[15] Geofencing allows advertisers to send messages to smartphone users once that smartphone has entered a specific geographical location.[16] In essence, geofencing is a virtual "fence," created around a specific location and activated when an individual enters into the "fenced" in area with a phone or another internet capable device.[17] Once an individual enters the geofenced location, advertisers display an ad on an open app or web browser.[18] The advertisement is geared specially to that location and the user's habits.[19]

Consumers are rarely aware that their installed apps may disclose their

10. Kevin F. King, *Personal Jurisdiction, Internet Commerce, and Privacy: The Pervasive Legal Consequences of Modern Geolocation Technologies*, 21 ALB. L.J. SCI. & TECH. 61, 115-16 (2011); *see also,* BOUVIER'S LAW DICTIONARY: PRIVACY (Desk ed. 2012) (defining privacy as a condition in which a person is free from the observation and knowledge of others).

11. *Id*. at 66.

12. Ryan Mura, *Geolocation and Targeted Advertising: Making the Case for Heightened Protections to Address Growing Privacy Concerns,* 9 BUFF. INTELL. PROP. L.J. 77, 77 (2013).

13. Kevin F. King, *Geolocation and Federalism on the Internet: Cutting Internet Gambling's Gordian Knot*, 11 COLUM. SCI. & TECH. L. REV. 41, 59 (2010).

14. *See* Mura *supra* note 12.

15. *Id*. at 80.

16. Valerie Morris, *The Basic Rules for Geofencing in Advertising*, *Data-Dynamix: Digital Marking Experts* (Sept. 8, 2017, 5:00 PM), http://www.data-dynamix.com/the-basic-rules-for-geofencing-in-advertising/.

17. *Att'y Gen. of Mass. 'Geofencing'*, *supra* note 1.

18. *Id.*

19. *Id.*

location information for unrelated uses, like targeted advertising.[20] Targeted advertising becomes particularly worrisome among apps connected to the healthcare industry. Health-based apps were some of the highest downloaded in 2016.[21] Many health-based apps transmit unencrypted information over unsecure network connections.[22] Health information is a person's most sensitive personal data,[23] and individuals are entitled to ensure the privacy of that information remains. The privacy of one's health data is inextricably linked with individual dignity.[24] The continuation of downloads of health-based apps at a high frequency, combined with the power of target advertising, may collectively result in deceptive geofences which risk individuals' personal privacy.

III. GEOFENCED DECEPTION: TWO SCENARIOS

In the aforementioned 2017 suit, *Commonwealth of Massachusetts, In the Matter of Copley Advertising, LLC, & John F. Flynn,* the Attorney General of Massachusetts alleged that Copley Advertising violated the Massachusetts Consumer Protection Act.[25] One year prior, in *U.S. v. InMobi Pte Ltd.*, the Federal Trade Commission ("FTC") alleged that the Singapore-based advertisement company, InMobi Pte. Ltd., violated the Children's Online Privacy Protection Act (COPPA) as well as Section 5(a) of the FTC Act, which prohibits unfair and deceptive acts or practices in or affecting

20. *Id.*

21. Jennifer Elias, *In 2016, Users Will Trust Health Apps More Than Their Doctors*, FORBES (Oct. 1, 2017), https://www.forbes.com/sites/jenniferelias/2015/12/31/in-2016-users-will-trust-health-apps-more-than-their-doctors/#47ae4aa67eb6.

22. Ann Carrns, *Free Apps for Nearly Every Health Problem but What About Privacy*, N.Y. TIMES (Sept. 11, 2013) http://www.nytimes.com/2013/09/12/your-money/free-apps-for-nearly-every-health-problem-but-what-about-privacy.html.

23. Elias, *supra* note 21.

24. Sharyl J. Nass, Laura A. Levit, & Lawrence O. Gostin, BEYOND THE HIPPA PRIVACY RULE; ENHANCING PRIVACY, IMPROVING HEALTH THROUGH RESEARCH, 15 (2009) https://www.ncbi.nlm.nih.gov/books/NBK9578/.

25. *See* G.L. c. 93A, §2; *see also Copley Advert. Settlement*, *supra* note 5, at 1.

commerce.[26] In both cases, geofencing was used by the respondent to target consumers, and both petitioners alleged that this form of advertising constituted unfair methods of competition or deceptive acts or practices.[27]

A. Commonwealth of Massachusetts, In the Matter of Copley Advertising, LLC, & JohnF. Flynn

Copley Advertising, LLC ("Copley Advertising" and "Copley") is a mobile marketing advertisement company that contracts with third parties to provide geofencing technology and advertising services.[28] In fact, Copley's main revenue stream is in creating geofences.[29] In establishing a geofence, Copley begins by selecting a location.[30] Examples include retail stores and automobile dealerships.[31] John Flynn, CEO of Copley Advertising, explained the process:

> "[Copley Advertising] can set up a mobile geofence around any area.[32] Once a consumer has entered the geofenced location, Copley then tags the ID of all smartphones.[33] After a smartphone has been tagged, Copley Advertising will determine the smartphone user's demographics, e.g., age, gender, and lifestyle habits.[34]

Examples of "lifestyle habits" include general profiles like "skiers" and

26. U.S. v. InMobi Pte Ltd., No. 3:16-cv-03474 (N.D. Cal. 2016) [hereinafter *InMobi*]; *see also* Federal Trade Commission Act, 15 U.S.C §45(a) (2017).

27. *Copley Advert. Settlement*, *supra* note 4, at 1 (stating that the MA Consumer Protection Act, section 2, entitled Unfair Methods of Competition or Deceptive Acts or Practices had been violated; *InMobi*, *supra* note 25, at 2. (stating that InMobi had violated Section 5(a) of the FTC Act, which prohibits unfair and deceptive acts or practices in or affecting commerce).

28. COPLEY ADVERTISING, http://copleyadvertising.com (Oct. 28, 2017); *See also Copley Advert. Settlement supra* note 5, at 5.

29. *Id*.

30. *Mobile Geo-Fencing: What is it?,* COPLEY ADVERTISING (Oct. 28, 2017), http://hubs.ly/H045RM00.

31. *Id*.

32. *Id.*

33. *See* COPLEY ADVERTISING, *supra* note 28.

34. *Id*.

"soccer moms."[35] In addition to identifying a user's demographics and lifestyle habits, once an ID for a user's smartphone has been created, Copley Advertising places the ID of in a retargeting folder for future marketing campaigns.[36] The user is then served the targeted advertisement that correlates with that particular geofenced location.[37] The advertisement can be on display on certain of the consumer's mobile applications for up to thirty days.[38]

In 2015, Copley contracted with Bethany Christian Services, a global pregnancy counseling and adoption agency, and RealOptions, a network of crisis pregnancy centers.[39] Copley agreed to provide geofencing technology and advertisements to "abortion minded women" on behalf of Bethany Christian Services and RealOptions.[40] The geofence encompassed women who were close to or within the waiting room of women's reproductive health clinics.[41] The advertisements sent to these women included text such as "Pregnancy Help," "You Have Choices," and "You're Not Alone."[42] Furthermore, once these women's Smartphone device had been tagged, Copley continued to push these advertisements on these women for thirty days after.[43]

The Attorney General of Massachusetts alleged that Copley Advertising violated the Consumer Protection Act due to the unfair and deceptive nature of the geofencing conduct.[44] She noted that consumers were not aware that their geolocation was being used by third party advertisers to "infer the

35. *Id*.
36. *Id.*
37. *Id.*
38. *Copley Advert. Settlement*, *supra* note 4.
39. *Id.*
40. *Id*.
41. *Id.*
42. *Id.*
43. *Id*. at 4.
44. *Id.*

consumer's physical or mental health status or medical treatment for the purpose of serving tailored advertisements."[45] The Attorney General of Massachusetts appraised such actions to be an invasion of a consumer's privacy because it intrudes upon an individual's health or medical affairs.[46] Consumer protection laws, like those in Massachusetts, purport to ensure that individuals are free from unfair and deceptive trade practices.[47]

Massachusetts consumer protection laws define "unfair" practices as those that "cause or are likely to cause substantial injury to consumer which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition.[48] When a consumer has entered into a geofence, they rarely realize that they have entered an area specifically established to target their phone and retrieve information about their person.[49] Once targeted, they can be sent any type of advertisement that has been created for that location. While it may be beneficial for consumers to share the data on their cell phones in a retail market (e.g. at a shopping mall) to ensure that they are getting the best deals[50], it is an unfair practice for advertisers to encroach upon individual's cellphone in a medical setting. Individuals are entailed to keeping their personal medical information private.

B. United States of America v. InMobi Pte Ltd.

In a similar case, the FTC alleged that InMobi deceptively tracked the locations of hundreds of millions of consumers, including children, without

45. *Id.* at 4.
46. *Id*.
47. William A. Lovett, *Louisiana Civil Code of 1808: State Deceptive Trade Practice Legislation*, 46 TUL. L. REV. 724, 724 (1972) (stating that 80% of the nation's population is governed by some kind of consumer protection statute that made "deceptive acts or practices" unlawful).
48. 15 U.S.C. §45(n) (2017).
49. *Att'y Gen. of Mass.'Geofencing*,' *supra* note 1.
50. Lauryn Chamberlain, *GeoMarketing 101: What is Geofencing?,* GEOMARKETING FROM YEXT (Nov. 14, 2017) http://www.geomarketing.com/about.

their knowledge or consent, through geotargeted advertising.[51] InMobi is a Singapore-based advertisement company that conducts substantial business in the United States, in part, via U.S.-based websites.[52] InMobi provides an advertising platform for mobile application developers and advertisers.[53] Its products consist of three variations of software that advertisers can use to locate a consumers.[54] Using InMobi's software, application developers can maximize their profits by allowing third party advertisers to advertise to consumers through banner ads, interstitial ads, and native ads.[55] Advertisers are then capable of targeting consumers across all of the mobile applications that have integrated the InMobi software.[56]

The allegations against InMobi emerged out of a database in which InMobi collected consumer information.[57] From that database, InMobi was capable of pin-pointing a consumer's location, even when consumers had turned off location collection on their devices.[58] This was possible due to InMobi collecting the Wi-Fi network information.[59] InMobi's software was able to track a consumer's location and serve geo-targeted ads, regardless of the application developer's intent with regard to privacy or the user's preference

51. Press Release, Federal Trade Comm'n, Mobile Advertising Network InMobi Settles FTC Charges it Tracked Hundreds of Millions of Consumers; Locations Without Permission (Jun. 22, 2016) (on file at https://www.ftc.gov/news-events/press-releases/2016/06/mobile-advertising-network-inmobi-settles-ftc-charges-it-tracked) [hereinafter Federal Trade Comm'n Press Release].

52. *InMobi*, *supra* note 25, at 3.

53. *Id.*

54. See *InMobi*, *supra* note 25, at 4, explaining the three types of products as the "Now" targeting suite, the "Conditional" targeting suite and the "Psychographic" targeting suite. The "Now" product lets advertisers to target consumers at their current location. The "Conditional" suite gives advertisers to the power to target consumers who satisfy certain conditions, like visiting a certain location at a certain time. The "psychographic" gives advertisers the capability to target consumers based on their location for up to the last two months. "For example, an advertiser may target consumers who live in affluent neighborhoods and, during the last two-month period, have visited luxury auto dealership."

55. *Id.* at 3.

56. *Id.*

57. Federal Trade Comm'n Press Release, *supra* note 51.

58. *Id*.

59. *Id.*

too not be tracked.[60] InMobi then fed this information into its geocoder database, and could infer the consumer's location, which allowed InMobi to continue to send geo-targeted ads.[61]

InMobi also used the same advertising techniques on children by collecting information from apps intended for children, violating the Children's Online Privacy Protection Act ("COPPA").[62] COPPA requires that applications directed towards children must obtain a parent's or guardian's consent in order to collect their child's data.[63] InMobi failed to do obtain the requisite consent, and therefore, the court found that it was in violation of COPPA.[64] Ultimately, InMobi was forced to stop using their software and had to pay fines for each violation of the COPPA Rule.[65] InMobi, accepted thee fines and both the FTC and InMobi agreed to a settle.[66]

IV. CONSUMER PROTECTION LAWS MUST PROTECT CONSUMERS OF THE HEALTHCARE INDUSTRY AGAINST GEOFENCING

In both the *InMobi* and *Copley Advertising* settlements, the advertisement companies were alleged to have used deceptive measures to target consumers.[67] In *Copley*, it was Massachusetts' consumer laws that were being violated, while in *InMobi* it was federal consumer laws.[68] The geotargeted advertising Copley Advertising used was alleged to have deceptively encroached upon a consumer's private health or medical affairs.[69]

As advertisers gain access about individuals through targeted advertising,

60. *InMobi*, *supra* note 25, at 6.
61. *Id.*
62. *Id.*
63. *Id.*
64. *Id.*
65. *Id.* at 16.
66. *Id.*
67. COPLEY ADVERTISING, *supra* note 28.
68. *Id.*
69. *Copley Advert. Settlement, supra* note 5, at 4.

significant health privacy concerns arise.[70] Privacy in the healthcare industry is taken very seriously, and has been since Congress passed the Health Insurance Portability and Accountability Act ("HIPAA"), which laid the groundwork for the Department of Health and Human Services ("HHS") to adopt the HIPAA Privacy and Security Rules. HIPAA gives HHS's Office for Civil Rights ("OCR") the power to penalize the unauthorized disclosure of protected health information ("PHI").[71] Those governed by HIPAA are called "covered entities."[72] Healthcare providers are responsible for ensuring that their patient's healthcare records remain confidential.[73] This includes ensuring that a patent's personal health information is protected if a healthcare provider chooses to utilize healthcare apps in conjunction with the patient's care.[74] Additional legislation has been implemented to ensure the safety of a patent's personal health information: namely, the Health Information Technology for Economic and Clinical Health Act (HITECH Act).[75] The HITECH Act establishes guidelines for any person that creates, maintains or has access to patient health records.[76] Its purpose is to ensure that each patient's health information is secured and protected,| in addition to promoting a more effective marketplace, greater competition, greater systems analysis, increased consumer choice and improved outcomes in health care

70. Courtney A. Barclay, *Implementation and Administration of the Broadband Stimulus Act: Protecting Consumers by Tracking Advertisers Under the National Broadband Plan*, 19 MEDIA L. & POL'Y 57, 66 (2009).

71. Roger Hsieh, *Improving HIPAA Enforcement and Protecting Patient Privacy in a Digital Healthcare Environment*, 46 LOY. U. CHI. L.J. 175, 177-78 (2014).

72. Health Insurance Portability and Accountability Act (HIPAA), 42 U.S.C. §1320d-1 et seq. (2017) (clarifying that covered entities include health plans, health care clearinghouses, and any other health provider who transmits health information).

73. Christina M. Mares, *To Cover or Not To Cover? The Relationship Between the Apple Watch and HIPAA*, 18 DEPAUL J. HEALTH CARE L. 159, 166 (2016).

74. *Id.* at 165.

75. *See generally* Ranjit Janardhanan, *Uncle Sam Knows What's In Your Medicine Cabinet: The Security and Privacy Protection of Health Records Under the HITECH Act*, 30 J. MARSHALL J. INFO. TECH. & PRIVACY L. 667 (2014).

76. *Id*.

services.[77]

Neither HIPAA nor its regulations reference potential privacy issues regarding geofencing and its power to target advertisements. Although HIPAA governs the interchange between providers and patients,[78] it does not extend to the interaction between *advertisers* and *consumers* as implicated by geofencing. Furthermore, HIPAA and the HITECH Act would only apply to geofencing practices if the geofencing data constituted protected health information ("PHI"). However, the data used to *create* a geofence is not PHI. Therefore, to prevent geo-targeting of healthcare facilities, HIPAA and/or the HITECH Act should adopt amendments that prohibit advertisers from collecting geo-location data while patients are located near a healthcare facility or protecting healthcare apps from targeted ads.

At the federal level, the Federal Trade Commission Act was passed by Congress to prevent persons, partnerships, or corporations from using unfair methods of competition in commerce.[79] Section 5(a) of the Federal Trade Commission Act is what *InMobi* was accused of violating.[80] Section 5(a) of the Federal Trade Commission Act provides ". . .unfair or deceptive acts or practices in or affecting commerce, are hereby declared unlawful."[81] Though *Copley Advertising* involved the violation of a state law (the Massachusetts Consumer Protection Act), the state law's language is virtually the same to the Federal Trade Commission Act.[82]

When applying this law to the act of geofencing consumers and serving them with geo-targeted advertisement, Congress has expressly rejected

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

78. *Id*. at 166.

79. Federal Trade Commission Act, 15 U.S.C. §45 (2017).

80. *InMobi*, *supra* note 26, at 3.

81. Federal Trade Commission Act, *supra* note 79.

82. *Att'y Gen. of Mass.'Geofencing*,' *supra* note 1 (clarifying the Massachusetts Consumer Protection Act states "unfair methods of competition and unfair or deceptive acts or practices in the conduct of any trade or commerce are hereby declared unlawful).

enumeration of specific unfair practices.[83] Congress reasoned that the term "unfair" should remain as a flexible concept because no matter how many unfair practices it could lists, there would always be others.[84] When consumers are unaware that their data is being used by a third party, it is clear that the consumer is not given an equal bargaining stance in the market. Geofencing invades a person's smartphone often without the consent of the user, and uses an individual's identity for the sole purpose of targeting them for a particular product or service. The intrusive nature of geofencing and the ability for advertisers to use geo fencing as a marketing tool needs to be more strictly regulated. It is not enough that marketing agencies have violated a provision of the Federal Trade Commission Act or a State Consumer Protection Laws. Geofencing must be kept away from health-related industries as this is where an individual deserves to have the highest level of privacy.

The market for the geofencing industry is expected to grow from $542.7 million to $1,825.3 million by 2022 at a compound annual growth rate of 27.5%.[85] Based on geofencings' predicted growth, it is not surprising that geofencing has been labeled as one of the trendiest modes of advertising for 2018.[86] Geofencing in the healthcare industry is predicted to hold the largest market share of the geofencing market.[87] In order to avert consumer

83. *See* David Bender, *The FTC, Unfair Practices, & Cybersecurity: Two Steps Forward and Two Steps Back*, 2 PRIVACY & CYBERSECURITY L. REPORT 105 (Apr. 2016).

84. *Id*.

85. *Geofencing Mark by Component (Solution and Services), Geofencing Type (Fixed and Mobile), Organization Size, Vertical (Transportation & Logistics, Government & Defense, Retail, Healthcare & Life Science, and Region- Global Forecast to 2022,* MARKETS & MARKETS (Sept. 2016), https://www.marketsandmarkets.com/Market-Reports/geofencing-market-209129830.html.

86. Rougeyar Parry, *10 Marketing Trends to Think About for 2018*, HUFFINGTON POST (Aug. 16, 2017, 05:07 PM), https://www.huffingtonpost.com/entry/10-marketing-trends-to-think-about-for-2018_us_5994b288e4b055243ea1357c.

87. Rony Deluycia, *Geofencing Market to Cross US 2,387 Million by 2023 Propelling at 27% CAGR*, MILTECH PR DISTRIBUTION (Dec. 1, 2017 03:20 AM), https://www.openpr.com/news/840294/Geofencing-Market-to-Cross-USD-2-387-Million-by-2023-Propelling-at-27-CAGR.html

deception of those patients who could find themselves located within a perimeters of a geofenced healthcare location, precautions need to be taken in order to protect the dignity of one's information. At the federal level, the current enforcement of protecting consumers from deceptive advertising rests with the Federal Trade Commission.[88] As seen in *InMobi*, the FTC has carved out an exception for protecting children's privacy.[89] Since geofencing is predicted to become one of the most used tools in digital advertising, the FTC should create limits on its use in order to prevent the Copley turmoil that it had created for the women who were innocently waiting in a women's health center. To allow a third party to entrap a patient's phone while seeking medical services, and without that individual's knowledge, in order for an advertising company to inundate that patient with custom advertisements runs counter to the purpose of the FTC's mission of keeping consumers free from deception.[90]

88. Federal Trade Commission Act, *supra* note 79.

89. *InMobi*, *supra* note 26, at 6 (explaining the Children's Online Privacy Protection Act is meant to protect children's private information while online).

90. *About the FTC*, FED. TRADE COMM'N, https://www.ftc.gov/about-ftc (last visited Dec. 3, 2017) (stating that Federal Trade Commission's mission is "Work[ing] to protect consumers by preventing anticompetitive, deceptive, and unfair business practices, enhancing informed consumer choice and public understanding of the competitive process, and accomplishing this without unduly burdening legitimate business activity").

The Importance of the Garden-Variety Exception to Mental Health Privilege Waivers in Protecting Patient Privacy

Emma Garl Smith

I. INTRODUCTION

Mental health treatment providers in America are vital, considering nearly one fifth of the country suffers from a mental illness.[1] Providers who offer mental health services rely on full disclosure by patients;[2] if patients withhold information from providers, they may not receive the full benefits of treatment.[3] Unfortunately, both public and self-assigned stigmas often accompany mental illnesses, such as the notion that all people with mental illness are dangerous or incompetent.[4] For this reason, patient privacy is necessary, as the disclosure of mental health treatment records may not just have a chilling-effect on patient candidness during therapy, but could also make therapy less effective,[5] and cause embarrassment, shame and stigma.[6]

1. SUBSTANCE ABUSE & MENTAL HEALTH SERVS. ADMIN., CTR. BEHAVIORAL HEALTH STATISTICS & QUALITY, NAT'L SURVEY DRUG USE & HEALTH, TABLE 8.2B, 2506 (2015).

2. Daniel M. Buroker, *The Psychotherapist-Patient Privilege and Post-Jaffee Confusion*, 89 IOWA L. REV. 1373, 1374 (2004) ("Confidentiality is essential to the psychotherapist-patient relationship." Referencing PSYCHIATRY 50 (Allan Tasman et al. eds., 1997)).

3. *Id.* ("The psychotherapist-patient relationship inspires such honesty because the patient is motivated to provide useful information to the psychotherapist so that the psychotherapist will be able to make the most accurate diagnosis and render the best therapy possible.").

4. Patrick Corrigan, *How Stigma Interferes With Mental Health Care*, 59 AM. PSYCHOLOGIST 614, 617–18 (2004).

5. Jaffee v. Redmond, 518 U.S. 1, 10 (1996) ("[T]he mere possibility of disclosure may impede development of the confidential relationship necessary for successful treatment.").

6. Corrigan, supra note 4, at 618.

In turn, this can influence whether an individual will seek treatment,[7] or can decrease the likelihood of ongoing participation in that treatment.[8] The potential disclosure of mental health records can decrease the effectiveness of therapy to such an extent that those records may lose their probative value as evidence in a court proceeding.[9] For this reason, the commonly known doctor-patient confidentiality in court proceedings applies to mental health providers and their patients.[10]

However, the confidentiality of mental health records is not absolute.[11] Challenges to privilege laws arise when one side needs mental health records to make their case and they beseech the court to make those records available to them.[12] Federal Rule of Evidence 501 is the brief but definitive rule that dictates what relationships between a party and other people are protected from the discovery process.[13] Courts interpret claims of privilege based on "reason and experience," unless the Constitution, federal statutes or the Supreme Court articulate otherwise.[14] This rule is further qualified by rejected Federal Rule of Evidence 504, the psychotherapist-patient

7. *Id.* at 617; Otto K. Wahl, *Mental Health Consumers' Experience of Stigma*, 25 SCHIZOPHRENIA BULL., 467, 470 (1999).

8. Corrigan, *supra* note 4, at 618.

9. Jaffee, 518 U.S at 12 (referencing American Psychological Association, Ethical Principles of Psychologists and Code of Conduct, Standard 5.01 (Dec. 1992), National Federation of Societies for Clinical Social Work, Code of Ethics V(a) (May 1988), and the American Counseling Association, Code of Ethics and Standards of Practice A.3.a (effective July 1995)).

10. Paul W. Mosher & Peter P. Swire, *The Ethical And Legal Implications of Jaffee v. Redmond and the HIPAA Medical Privacy Rule For Psychotherapy and General Psychiatry*, 25 PSYCHIATRY CLIN. N. AM. 575, 575 (2002).

11. Jaffee, 518 U.S. at 9–10.

12. Sherry L. Talton, *Court Construes Exception to Psychotherapist-Patient Privilege*, LITIG. NEWS (Oct. 10, 2009), http://apps.americanbar.org/litigation/litigationnews/top_stories/psychotherapist-patient-privilege-connecticut.html.

13. Fed. R. Evid. 501.

14. *Id.* (stating the common law—as interpreted by United States courts in the light of reason and experience—governs a claim of privilege unless any of the following provides otherwise: the United States Constitution; a federal statute; or rules prescribed by the Supreme Court.)

privilege,[15] and the subsequent "patient-litigant exception" found in section 504(d)(3),[16] which is frequently applied by courts.[17] This rule protects the confidentiality of mental health records in order to protect the benefit that patients receive from mental health providers and treatment.[18] Section 504(d)(3) comes into play when a party to a lawsuit "bases a claim or defense on her mental or emotional condition."[19]

In the 2015 case of *Fagen v. Grand View University*, the court's usage of the "garden-variety exception" prevented the defense from accessing private mental health records as long as the damages claimed in the case were based merely on the mental or emotional injury that an average person might experience due to the cause of action.[20] However, this exception would not apply if the damages sought were for extreme mental or emotional injury, such as mental disability resulting from the cause of action.[21] Some perceive

15. Rejected Fed. R. Evid. 504 ("General Rule of Privilege. A patient has a privilege refuse to disclose and to prevent any other person from disclosing confidential communications, made for the purposes of diagnosis or treatment of his mental or emotional condition, including drug addiction, among himself, his psychotherapist, or persons who are participating in the diagnosis or treatment under the direction of the psychotherapist, including members of the patient's family.").

16. Melissa Lee Nelken, *The Limits of Privilege: The Developing Scope of Federal Psychotherapist-Patient Privilege Law*, 20 REV. LITIG. 1, 20 (2000) (citing Jack B. Weinstein & Margaret A. Berger, *Weinstein's Federal Evidence* § 504.07(7) (2d ed. 1997)); Rejected Fed. R. Evid. 504(d)(3) ("Condition an Element of Claim or Defense. There is no privilege under this rule as to communications relevant to an issue of the mental or emotional condition of the patient in any proceeding in which he relies upon the condition as an element of his claim or defense, or, after the patient's death, in any proceeding in which any party relies upon the condition as an element of his claim or defense."); Anne Bowen Poulin, *The Psychotherapist-Patient Privilege After Jaffee V. Redmond: Where Do We Go From Here?*, 76 WASH. U. L. Q. 1341, 1342 (1998) (explaining the history of rejected Rule 504: "When the Court promulgated rules of evidence, culminating in 1975 with the statutory adoption of the Federal Rules of Evidence, the Court also proposed rules to govern the federal law of privilege. While retaining most of the other proposed rules of evidence with some modifications, Congress deleted the proposed rules pertaining to privilege. Instead, Congress adopted a single rule addressing privilege. . . rule 501.").

17. Nelken, *supra* note 16, at 20.

18. *Id.* at 6; Mosher & Swire, *supra* note 10, at 576.

19. Nelken, *supra* note 16.

20. Fagen v. Grand View Univ., 861 N.W.2d 825, 837 (Iowa 2015).

21. *Id.* at 835 ("Before the court can require Fagen to sign a waiver for the anger-management counseling records Iddings seeks, Iddings must advance some good faith factual basis demonstrating how the records are reasonably calculated to lead to admissible evidence germane to mental pain and suffering that any normal person would have

this holding to contravene *Jaffee v. Redmond*, in which the United States Supreme Court, nineteen years prior, first agreed with all fifty states that an absolute patient-psychotherapist privilege existed.[22] This is because the *Fagen* holding gives a judge discretion over whether a party must waive privacy of their mental health records, whereas the *Jaffee* court placed the burden of proving necessity of the records on the requesting party.[23] The garden-variety exception, however, aligns with the *Jaffee* court's intention. It adds another layer of protection for a mental health patient: the protection of a judge's discretion from an opposing party who can make a good-enough point as to why mental health records could help make their case. If this occurs when a plaintiff or defendant's mental health is not truly at issue, it would violate that patient's privacy.[24] *Fagen*'s application of the exception also aligns with the Supreme Court's *Jaffee* decision and, in some cases, could be the best way to protect mental health record confidentiality in the course of pre-trial discovery.

This article will first look at the law and logic that created the absolute psychotherapist-patient privilege in *Jaffee* and the subsequent narrowing of that privilege with the garden-variety exception as applied in *Fagen*. This article will then describe why these cases are not at odds, and how they work together to protect the privacy rights of mental health patients. Finally, this article will address opposition to the garden-variety exception. It will explain why, when applied together, *Jaffee* and *Fagen* are the best opportunity for a mental health patient to receive both fairness and privacy when a court determines if their confidential mental health records will be involuntarily disclosed.

---

experienced because of the assault alleged by Fagen.").

22. Jaffee v. Redmond, 518 U.S. 1, 12 (1996).

23. Fagen, 861 N.W.2d. at 833.

24. Daniel W. Shuman et al., *Privilege Study: An Empirical Examination of the Psychotherapist—Patient Privilege*, 60 N.C. L. REV. 893, 899 (1981).

II. THE GARDEN-VARIETY EXCEPTION: GUIDING CASE LAW

When the Supreme Court laid down the 1996 decision in *Jaffee v. Redmond*, federal courts were split on the existence of an absolute privilege between a psychotherapist and patient.[25] In evidentiary proceedings, this was a privilege akin to that between an attorney and client, and was already recognized in all fifty states.[26] In *Jaffee*, the defendant, a police officer, shot and killed a man whose family then brought suit for excessive force.[27] After the shooting, the defendant sought psychotherapy from a social worker concerning the trauma she personally experienced during the shooting.[28] The plaintiffs attempted to compel the defendant to disclose the records from the counseling sessions for cross-examination, despite the assertion by the defendant that these were protected from involuntary disclosure.[29] Seven of the nine Justices agreed with the states on the matter, stating that a balancing test allowing judicial discretion to weigh the value of the privilege against the probative value of the evidence would "eviscerate the effectiveness of the privilege."[30] This was the first time federal courts recognized the absolute confidentiality of communications between a psychotherapist and patient.[31]

Since *Jaffee*, courts continue to grapple with the balance between patient privacy rights and the rights of the other party to either prove their case or mount their defense.[32] The notion of mounting a defense is the crux of the patient-litigant exception, that a litigant may be required to provide a waiver

25. Nelken, *supra* note 16, at 4.
26. *Id.* at 2.
27. Jaffee, 518 U.S. at 4.
28. *Id.* at 5.
29. *Id.*
30. *Id.* at 18.
31. Nelken, *supra* note 16, at 5 ("Although a psychotherapist-patient privilege was among the privileges recommended to Congress in 1972 by the Judicial Conference Advisory Committee, 6 Congress ultimately created no specific privileges and instead adopted Federal Rule of Evidence 501, which provides that privileges in federal court 'shall be governed by the principles of the common law, as they may be interpreted by the courts of the United States in the light of reason and experience.'").
32. Nelken, *supra* note 16, at 16–17.

to the opposing side to view their medical records if the litigant puts their mental health or emotional condition at issue.[33] However, this can be construed broadly, whereby a court may deem all of a litigant's mental health records relevant to a cause of action and, therefore, compel the patient-litigant to make all mental health records discoverable.[34] The litigant must then argue the irrelevance of whatever records they want kept confidential in order to protect their privacy.[35]

In 2015, the Iowa Supreme Court in *Fagan* looked at an issue similar in some respects to *Jaffee*, though the court considered a different argument from the plaintiff: the "garden-variety exception."[36] With this exception, the court could deny a waiver for mental health records even when a plaintiff sought damages for mental pain and anguish, if that pain was merely what an average person would experience due to the trauma of the cause of action, or what would be considered "garden variety."[37] In *Fagen*, the plaintiff, a college student, suffered mental pain and anguish after he was assaulted by six other students who wrapped him in a carpet and proceeded to kick and punch him.[38] The plaintiff brought charges of assault and battery against one of his assailants.[39] The plaintiff sought monetary damages for his "painful and permanent injuries" and for mental disability.[40] While the plaintiff did not seek mental health treatment as a result of the incident, he previously received anger management counseling in middle school, and the defendants asked for a waiver of privilege to obtain those records.[41] The Supreme Court of Iowa reversed the lower court's requirement that the plaintiff sign a

33. *Id.* at 20.
34. *Id.* at 21.
35. *Id.* at 22 (citing Vanderbilt v. Town of Chilmark, 174 F.R.D. 225, 225 (D. Mass. 1997)).
36. Fagen v. Grand View Univ., 861 N.W.2d 825, 837 (Iowa 2015).
37. *Id.*
38. *Id.* at 828.
39. *Id.*
40. *Id.*
41. *Id.* at 829.

privilege waiver and remanded the case.[42] The court felt that the plaintiff's privacy rights would be violated by the disclosure of these records because the records at issue had nothing to do with the cause of action, and, therefore, the violation of privacy did not outweigh the probative value of the evidence.[43] The plaintiff referred to his mental pain and anguish as "garden variety," or something that an ordinary person would experience after the trauma he had experienced.[44] Through this exception, the court deemed the plaintiff's mental health records irrelevant to the garden-variety emotional damages he was claiming, and his medical records were kept confidential.[45]

The manner in which the *Fagen* court protected the plaintiff's privacy may not have been exactly as the *Jaffee* court intended, but in its narrow way, *Fagen* remained consistent with the Supreme Court's view on the subject. Despite *Fagan*'s austere application of the garden-variety exception, this was the court's best option in order to protect the plaintiff's privacy rights as allowed by law.[46]

III. REFUTING OPPOSITION TO THE GARDEN-VARIETY EXCEPTION

It is not difficult to see how the application of the garden-variety exception could be considered counter to the holding in *Jaffee*. For example, in 1998, the court in *McKenna v. Cruz* rejected the garden-variety exception for that

42. *Id.* at 836.

43. *Id.* ("[The defendant] contends he needs plaintiff's Fagen's mental health records to establish a baseline of Fagen's mental condition prior to the assault. He fails, however, to show a good faith factual basis demonstrating how the records are reasonably calculated to lead to admissible evidence germane to Fagen's claim. Iddings presents no facts that Fagen's mental health immediately prior to the assault was anything but normal. (The defendant) presents no facts as to how counseling sessions from grade school are reasonably calculated to lead to admissible evidence regarding a baseline.").

44. *Id.* at 829.

45. *Id.* at 835 ("Before the court can require Fagen to sign a waiver for the anger-management counseling records Iddings seeks, Iddings must advance some good faith factual basis demonstrating how the records are reasonably calculated to lead to admissible evidence germane to mental pain and suffering that any normal person would have experienced because of the assault alleged by Fagen.").

46. *Id.*

very reason.[47] However, the *Jaffee* court was considering patient-psychotherapist privilege in the broadest possible context.[48] The United States Supreme Court took an all-or-nothing stance in an effort to protect patient privacy as much as is allowed according to the "reason and experience" mentioned in Rule 501.[49] The dreaded balancing test that the *Jaffee* court sought to prevent was based on the discretion of a judge, which in turn would be based on all the information the litigants threw at him or her.[50] Specifically, Justice Stevens wrote:

> Making the promise of confidentiality contingent upon a trial judge's later evaluation of the relative importance of the patient's interest in privacy and the evidentiary need for disclosure would eviscerate the effectiveness of the privilege. . . Because this is the first case in which we have recognized a psychotherapist privilege, it is neither necessary nor feasible to delineate its full contours in a way that would "govern all conceivable future questions in this area."[51]

The Garden-Variety exception functions on a much smaller scale, narrow enough in scope that it falls within the "contours" mentioned in *Jaffee*.[52]

The arguments against the usage of the garden-variety exception are based primarily on balancing the plaintiff's privacy rights with the defendant's right to mount an adequate defense, just as the *Jaffee* court analyzed.[53] The garden-variety exception appears to add a level of unpredictability to the Supreme Court's cut and dry stance on waivers of psychotherapist-patient privilege;

---

47. Nelken, *supra* note 16, at 25–26 ("The court worried that attempting to distinguish between Garden-Variety and non-Garden-Variety emotional distress claims during a lawsuit would 're-introduce the very uncertainty the Supreme Court eliminated when it endorsed the psychotherapist-patient privilege as an unconditional privilege.'" (citing McKenna v. Cruz, 1998 WL 809533 at ¶ 2)).

48. Jaffee v. Redmond, 518 U.S. 1, 17 (1996).

49. *Id.* at 8.

50. *Id.* at 17.

51. *Id.*

52. *Id.* at 5.

53. *Id.*

however, the *Jaffee* court recognized that its decision would be further refined,[54] which is exactly what the *Fagen* court did.

One such argument asks whether the mental suffering experienced by a plaintiff is truly garden variety.[55] If it is a close call, litigants may not know what to expect from the court.[56] Post-*Jaffee* decisions – but prior to the *Fagen* decision – could rely somewhat on the expectation that in both state and federal courts, the psychotherapist-patient privilege could halt mandatory disclosure of records without a showing of good faith cause; litigants would not necessarily need to rely on a judge's view of what is "ordinary" mental suffering.[57] While the garden-variety exception does, on its face, place more weight on a judge's discretion and, therefore, affords less credence to a litigant's power of persuasion, whether mental suffering is garden-variety is a decision that must be weighed in every case due to the existence of medical record waivers.[58] Who better to decide a close call than a judge who is familiar with Federal Rule of Evidence 501 and can perform a balancing test to ensure that the private records of a patient are waived by the smallest amount that Rule 501 allows? This balancing test does not go against *Jaffee* because the plaintiff in *Jaffee* sought therapy as a direct result of the cause of action.[59] In a situation like *Fagen*, where the treatment records pertained to unrelated issues from a decade before the cause of action, an entirely different balancing test is necessary to protect privacy rights.

The garden-variety exception also raises the issue that "garden-variety" mental suffering is a legal and not a psychiatric term, therefore having less bearing on its applicability to decide whether a plaintiff's mental suffering

54. *Id.* at 18 ("A rule that authorizes the recognition of new privileges on a case-by-case basis makes it appropriate to define the details of new privileges in a like manner.").

55. Helen A. Anderson, *The Psychotherapist Privilege: Privacy and "Garden Variety" Emotional Distress*, 21 GEO. MASON L. REV. 117, 140 (2013).

56. *Id.* at 137.

57. *Id.*

58. *Id.*

59. Fagen v. Grand View Univ., 861 N.W.2d 825, 829 (Iowa 2015).

reaches a threshold beyond "ordinary."[60] However, courts routinely decide mental health issues in a courtroom setting through the application of legal principles.[61] For example, this occurs during a trial when a court must consider whether a defendant is not guilty by mental disease or defect,[62] whether a party is competent to stand trial,[63] whether a defendant has the requisite mens rea to have committed a crime,[64] or to determine the mental status of a potential witness.[65] The garden-variety exception asks the court to do no different than it is routinely relied on to do: look at the cause of action and what the plaintiff claims as emotional or mental distress and decide if it is "normal."[66]

One may ask whether plaintiffs would then lie or minimize their mental injury in order to keep mental health records confidential and protect their privacy if their real level of mental pain would lead a judge to require a waiver of that confidentiality.[67] A better question is, to what end? Is it reasonable to relinquish valuable privacy protections on the assumption that a plaintiff might sue and then put themselves at risk of receiving lesser damages in an attempt to hide their records? This is unlikely. Additionally, the plaintiff is still in a court proceeding and will testify under oath about their condition.[68] Whether a plaintiff lies to minimize his or her condition to protect records or chooses to waive protection, release records, and then exaggerate his or her condition to maximize damages, cannot be the reason

60. Anderson, *supra* note 55, at 140.
61. Michael L. Perlin & Heather Ellis Cucolo, *Mental Disability Law: Civil and Criminal*, 2007 CUMULATIVE SUPPLEMENT (2007).
62. Clark v. Arizona, 548 U.S. 735, 749 (2006).
63. Dusky v. United States, 362 U.S. 402, 403 (1960).
64. Staples v. United States, 511 U.S. 600, 611 (1994).
65. Fed. R. Evid. 601.
66. Fagen v. Grand View Univ., 861 N.W.2d 825, 835 (Iowa 2015).
67. Anderson, *supra* note 55, at 142.
68. Nicolas Jacquemet et al., *Preference Elicitation under Oath,* HAL ARCHIVES-OUVERTES 1, 4 (2010) ("What the social psychology theory of commitment tells us is that the risk of lying is greatly diminished in an oath-taking context.").

the records of truthful people are at risk for unnecessary disclosure.

IV. CONCLUSION

Confidentiality in medical records is vital in order for the patient to receive full benefits from the treatment,[69] and this is reflected in Rule 504's psychotherapist-patient privilege.[70] However, when mental health is at issue in a lawsuit, Rule 501 allows a judge to require that a party waive confidentiality, making mental health records discoverable before the trial.[71] When the Court in *Jaffee* recognized an absolute privilege between a psychotherapist and patient,[72] it was thought to be necessary to protect patient privacy. However, if a party could show good faith cause, it could still acquire the mental health records of the opposing side.[73] Nineteen years later in *Fagen*, the Iowa Supreme Court applied the "garden-variety exception" to a situation similar to Jaffee.[74] The garden variety exception allowed the *Fagen* court to look beyond the broad holding in *Jaffee* and protect the confidential records of a plaintiff whose mental health was not truly at issue in the case. For that plaintiff, the absolute privilege created in *Jaffee* would have become no privilege at all.

The garden-variety exception allows courts to look at the mental health condition about which one party would like to view privileged medical records, and instead of looking at it in terms of waiver-or-no-waiver, the court could ask, "Is this mental suffering what a normal person would suffer? Is it garden-variety?" If the answer is yes, the patient's privacy can be protected, and he or she can still claim damages for mental and emotional suffering that might, pre-*Fagen*, subject him or her to the violation of an examination of

69. Jaffee v. Redmond, 518 U.S. 1, 23 (1996).
70. Rejected Fed. R. Evid. 504.
71. Fed. R. Evid. 501.
72. Jaffee, 518 U.S. at 12.
73. Fagen v. Grand View Univ., 861 N.W.2d 825, 836 (Iowa 2015).
74. *See generally* Fagen, 861 N.W.2d.

private records.[75]

At first blush, it seems like a court, when applying the garden-variety exception, will take on a new role of improperly examining mental and emotional health through the cold lens of the law, thrusting the judge into the role of an arbiter of mental and emotional health. However, this is already a role that the court plays in examining legal issues involving competencies to participate in the legal system.[76] The only difference is that when employing the garden-variety exception, a court is using this power to protect patient privacy in a nuanced way that the *Jaffee* court could not.

With widespread application of the garden-variety exception, it is hard to say what negative outcomes there could be. Would a litigant lie or minimize mental suffering in order to manipulate the system of protection that the garden-variety exception puts in place? Time will tell if truly adverse outcomes would result. However, *Fagen* displays an extra layer of protection for a patient's confidential medical records during pre-trial discovery, a confidentiality on which successful treatment outcomes may depend.

75. *Id.*
76. Perlin & Cucolo, *supra* note 61, at 77–78.

Undocumented Immigrants and Incomplete Health Information: A Costly Blind Spot for Health Care Providers and Their Patients

Victoire Iradukunda

Immigration reform continues to be a topic of heated debate in the United States.[1] One of the more controversial issues is whether undocumented immigrants should have access to benefits typically provided by the state, particularly subsidized health care.[2] The unsettled nature of this debate affects healthcare providers, leaving them to struggle with the divergent interests of medical ethics, immigration policy, and healthcare regulation. Medical ethics urges physicians to consider the duty of their profession, and prioritize patient care over social or political goals like reserving resources for naturalized citizens, or reporting individuals to Immigration and Customs Enforcement (ICE).[3] Immigration policy itself has a different set of

1. *See* ROBERTO SURO, MIGRATION POLICY INSTITUTE, AMERICA'S VIEWS OF IMMIGRATION: THE EVIDENCE FROM PUBLIC OPINION SURVEYS 2 (2009), http://www.migrationpolicy.org/research/americas-views-immigration-evidence-public-opinion-surveys (analyzing the varied public opinions toward immigration); Sara Kehaulani Goo, *What Americans Want to Do About Illegal Immigration*, PEW RESEARCH CTR. (Aug. 24, 2015), http://www.pewresearch.org/fact-tank/2015/08/24/what-americans-want-to-do-about-illegal-immigration/ (discussing the conflicted political opinions of both republicans and democrats toward immigration policy).

2. *See* Dayna Bowen Matthew, *The Social Psychology of Limiting Healthcare Benefits For Undocumented Immigrants – Moving Beyond Race, Class, and Nativism*, 10 HOUS. J. HEALTH L. & POL'Y 201, 202-207 (2010) (highlighting that the government is still grappling with how to effectively regulate undocumented immigrants' access to the American healthcare system).

3. *See* Fred Arnold, *Providing Medical Services to Undocumented Immigrants: Costs and Public Policy*, 13 THE INT'L MIGRATION R. 706, 711 (1979) (discussing the moral and legal obligations doctors face when treating undocumented aliens); *see also* Atheendar S. Venkataramani & Alexander C. Tsai, *Dreams Deferred – The Public Health Consequences of Rescinding DACA*, NEW ENG. J. OF MED. (Sept. 13, 2017), http://www.nejm.org/doi/full/10.1056/NEJMp1711416 (stressing the humanitarian imperative that the medical community has to counteract a threat to public mental health).

priorities—the deportation of undocumented immigrants and their families has increased under the last two presidential administrations.[4] In addition, public opinion surveys reveal an increasing anxiety toward undocumented immigrants.[5] Yet there exists a body of the law which encourages providers to treat undocumented patients, including the U.S. Constitution which prohibits discrimination on the basis of "national origin" and patient privacy laws which allow providers to care for undocumented immigrants without requiring them to report the immigrant's status.[6] This tangle of contradictory directives is problematic for the provider and for the patient for a number of reasons. Out of fear of deportation, patients are more likely to lie, or underreport symptoms.[7] The healthcare physician who then treats a patient while referencing incomplete or inaccurate medical information places

4. Michael D. Shear & Julie Hirschfield Davis, *Trump Moves to End DACA and Calls on Congress to Act*, N.Y. TIMES (Sept. 5, 2017), https://www.nytimes.com/2017/09/05/us/politics/trump-daca-dreamers-immigration.html?mcubz=1 (reporting that after 200 days in office, President Donald Trump announced his decision to repeal the Deferred Action for Children Arrivals (DACA) program, which protects nearly 800,000 young undocumented immigrants who were brought to the U.S. as children); Scott Horsley, *5 Things to Know About Obama's Enforcement of Immigration Laws*, NAT'L PUBLIC RADIO (Aug. 31, 2016, 5:00 AM ET), http://www.npr.org/2016/08/31/491965912/5-things-to-know-about-obamas-enforcement-of-immigration-laws (reporting that deportation steadily increased during former President Barack Obama's first four years in office, reaching an estimated 400,000 deportees in fiscal year 2012).

5. Suro, *supra* note 1, at 1.

6. 42 U.S.C. §300gg (protecting patient identifiable health information from being disclosed but for very specific situations); 29 U.S.C. §1181; 42 U.S.C. 1320d et seq.; 42 U.S.C. § 2000e (1964) (prohibiting physicians and hospitals receiving federal funding, including Medicare and Medicaid, from discriminating against patients on the basis of race, color, religion, or national origin); *See also* Jeff Sconyers & Tyler Tate, *How Should Clinicians Treat Patients Who Might Be Undocumented?,* AMA J. OF ETHICS (2016), http://journalofethics.ama-assn.org/2016/03/ecas4-1603.html (noting that physicians are not obligated to form the initial patient-doctor relationship if there is legitimate reason for doing so).

7. *See* Jennifer Adaeze Okwerekwu, *Why I've Learned To Leave Blank Spots In Some Patient's Medical Records*, STAT (Mar. 6, 2017), https://www.statnews.com/2017/03/06/immigrants-undocumented-doctors/ (reporting that given the current immigration climate, undocummented immigrants are not giving certain information because it is better to be safe than sorry); *see also* Randy Cohen, *Patients with an Alias*, N.Y. TIMES (June 17, 2009), http://www.nytimes.com/2009/06/21/magazine/21FOB-ethicist-t.html?mcubz=1(providing evidence that undocumented immigrants are seeking care while giving conflicting personally identifiable information to their health care providers).

herself at an increased risk of rendering an unsatisfactory standard of care and inviting adverse reports and action against her medical license.[8] Additionally, treating a patient while referencing incomplete or inaccurate medical information increases the risk of violating regulations such as the False Claims Act (FCA) which requires providers to submit claims free of inaccurate or misleading information.[9]

This Article urges physicians to consider the implications of treating undocumented immigrants who present incomplete or inaccurate medical information because as this becomes more prevalent, physicians are exposed to an increased level of legal, ethical, and professional liabilities. Part I of this Article will introduce foundational information about undocumented immigrants' use of the U.S. healthcare system and will explore laws governing health care delivery to undocumented immigrants. Part II will also explore the ethical drivers urging providers to care for undocumented immigrants. Part III will highlight the potential legal and ethical implications of providing health care to undocumented immigrants while referencing inadequate medical information. Part III will also present the strategies that have been proposed to minimize risk while simultaneously maximizing the standard of care of undocumented immigrants.

I. LEGAL FACTORS AND ETHICAL DRIVERS AFFECTING HEALTH CARE

8. M.A. Shoever et al., *Patient-Held Records for Undocumented Immigrants: A Blind Spot. A Systematic Review of Patient –Held Records,* ETHNICITY & HEALTH (Oct. 2009), https://www.ncbi.nlm.nih.gov/pubmed/19462264 (noting that as a result of inadequate medical information, the care of undocumented immigrants is often time consuming and unsatisfactory); ILL. DEPT. OF PUBLIC HEALTH, http://www.dph.illinois.gov/topics-services/health-care-regulation/complaints (last visited Nov 18, 2017) (providing a vehicle for patients and other citizens to report a healthcare provider for issues related to quality of care and medical errors).

9. 31 U.S.C. § 3729 (2016) (imposing a penalty under federal law of up to $10,000 plus 3 times actual damages for every false claim for services under the Medicare program and similar laws apply at the state level).

DELIVERY TO UNDOCUMENTED IMMIGRANTS

There are approximately 11.3 million undocumented people living in the United States.[10] Of the 11.3 million undocumented immigrants, over 80% of them are Latino.[11] Studies show that Latino immigrants, including both undocumented and documented immigrants, have better health status and lower levels of risky behavior compared to the U.S. citizens.[12] However, barriers that undocumented immigrants face, such as limited access to quality health care, low income and occupational status, and fear of deportation significantly decrease the health advantage of undocumented immigrants, considerably faster than that of the U.S. citizens.[13]

Even with barriers that dissuade undocumented immigrants from utilizing the U.S. healthcare system, such as fear of deportation, a California study revealed that 34.7% of undocumented immigrants were using the emergency room (ER) as their primary source of care and 17.9% were estimated to receive regular ambulatory care.[14] Strong evidence supports the conclusion that providers are treating undocumented patients, whether or not they are aware of their patients' undocumented status.[15]

---

10. Alan Gomez, *Undocumented Immigrant Population in U.S. Stays Flat for Eight Straight Year*, USA TODAY, (Apr. 26, 2017, 10:44 AM), https://www.usatoday.com/story/news/world/2017/04/25/undocumented-immigrant-population-united-states/100877164/.

11. Steven P. Wallace et al., UCLA CENTER FOR HEALTH POLICY RESEARCH, UNDOCUMENTED IMMIGRANTS AND HEALTHCARE REFORM 12 (Aug. 31, 2012), http://healthpolicy.ucla.edu/publications/Documents/PDF/undocumentedreport-aug2013.pdf.

12. *Id.*; *See* THE FREE MEDICAL DICTIONARY, https://medical-dictionary.thefreedictionary.com/health+status (defining health status to mean "a generic term referring to the health (good or poor) of a person, group or population in a pa rticular area, especially when compared to other areas or with national data") (last visited Jan. 1, 2018); *see also* TEREZA KILLIANOVA, SPRINER, https://link.springer.com/referenceworkentry/10.1007%2F978-1-4419-1005-9_1551 (defining risky behavior to mean "any consciously, or non-consciously controlled behavior with a perceived uncertainty about its outcome, and/or about its possible benefits, or costs for the physical, economic or psycho-social well-being of oneself or others") (last visited Jan. 1, 2018).

13. Wallace et al., *supra* note 11, at 12.

14. *Id*. at 19.

15. *Id.*; *see also* Okwereku, *supra* note 7; *see also* Cohen, *supra* note 7.

There are two additional factors that affect physician's decision to provide care to undocumented immigrants, and how. First and foremost, several laws have been enacted that grant undocumented immigrants access to health care, protect undocumented immigrants from unlawful discrimination, and protect undocumented patients' privacy. Additionally, many physicians feel an acute ethical obligation to treat the patient they see, regardless of citizenship status.

A. Legal Factors Governing Health Care Delivery to Undocumented Immigrants Under The U.S. Healthcare System

Several statutory requirements such as the Medicaid Act and the Emergency Medical Treatment and Active Labor Act (EMTALA) are currently in place allowing undocumented immigrants to receive access to health care in the U.S.[16] Courts have established that children of undocumented immigrants have a constitutional right to access health care.[17] The patchwork of legislation and inconsistent legal precedent that regulate the availability of these health benefits results in a series of line-drawing exercises. This has pitted the qualified from the unqualified immigrants, distinguishing emergency care from chronic public health care, and separating children from their parents once they have exited the womb of an undocumented immigrant.[18] This approach reflects the struggle faced by state and federal authorities to send a clear message about immigration policy. As a result, healthcare providers are left with broad discretion and little guidance.

Even where the law permits undocumented immigrants access to some

16. *See* 42 U.S.C. § 1396 (2009) (providing health care for the poor, disabled, or chronically ill and some undocumented immigrants may be eligible to receive health care through Medicaid because of their low income levels); *see* 42 U.S.C. § 1395dd (2010) (granting access to emergency health care to all in an emergency medical condition); *see also* Cohen, *supra* note 7.

17. Lewis v. Thompson, 252 F.3d 567, 569 (2nd Cir. 2001).

18. Bowen, *supra* note 2.

health care, providers may exercise their own discretion because there is generally no legal duty to provide care to an individual absent a pre-existing patient-physician relationship or a life-threatening emergency.[19] Physicians must be careful, however, because they are only free to refuse to accept a prospective patient if their reason for doing so is not prohibited by law.[20] For example, physicians cannot refuse care to a patient based on the discrimination of a protected category—i.e., race, religion, national origin, color, sex/gender/gender identity/sexual orientation, veteran status, or disability.[21] Additionally, section 1557 of the Patient Protection and Affordable Care Act (PPACA) restricts providers from refusing to treat a patient due to discrimination of a protected category including national origin.[22] Furthermore, EMTALA requires any person who presents to an emergency room to be stabilized and treated regardless of their insurance status or ability to pay.[23]

Once the patient-physician relationship is established and the physician agrees to see the patient, the Health Information Portability and Accountability Act (HIPAA) thereafter affords the patient some protection.[24] HIPAA states that a provider may not disclose the personally identifiable information of an immigrant except (1) for purposes of providing her with health care services, obtaining payment, and conducting clinic operations (2) as and to the extent she authorizes disclosure in advance, or (3) in certain very limited circumstances without her prior authorization.[25]

---

19. Sconyers & Tate, *supra* note 6.
20. 42 U.S.C. § 2000e (1964).
21. *Id.*
22. 42 U.S.C. §18001 (2010) (building on the civil rights act, this section of the PPACA provides that all programs administered by HHS and those health care providers receiving federal funding may not refuse treatment to any person based on the discrimination of a protected category such as national origin).
23. 42 U.S.C. § 1395dd (2010).
24. *Supra* note 6.
25. *Id*.

B. Ethical Drivers Affecting Health Care Delivery to Undocumented Immigrants Under The U.S. Healthcare System

Arguably the stronger force driving physicians to care for undocumented immigrants is not legal but ethical, and based in the culture of the medical profession.[26] Recent studies show that the current general attitude of the medical community is to protect the health of all humans, regardless of legal status.[27] A number of providers even report that undocumented immigrants have changed "the way [they] practice medicine" because they look the other way or accept incomplete information when treating the undocumented immigrant population.[28] In one example, a physician reported that she protects her undocumented patients by omitting certain information in their record because "if you don't document it, it's not recoverable."[29] The physician reported that her commitment is to "practice social justice. . .protect our undocumented patients, advocate for their rights, and continue to serve them as healers.[30] For this physician and many like her, helping a government without any benefit to the patient is not something she is willing to take part in out of duty to her profession and to her patient.[31] Physicians are called by the ethics of their profession to see health care as a human right and to refrain from equating "not American" with "not human."[32] Even if it means "changing the way [they] practice medicine," physicians are willing to place the needs of their patients before the demands of their government.[33]

---

26. Sconyers & Tate, *supra* note 6.
27. Am. Medical Ass'n, *AMA Adopts Policies to Protect the Health of Immigrants, Refugees* (June 13, 2017), https://www.ama-assn.org/ama-adopts-new-policies-improve-health-immigrants-and-refugees.
28. Okwerekwu, *supra* note 7.
29. *Id*.
30. *Id*.
31. *Id.*
32. *Id.*
33. *Id.*

Moreover, a policy of the American Medical Association (AMA) was reinforced and it demonstrates that this view goes beyond the view of a select few physicians; it is deeply rooted in the medical profession.[34] In response to President Donald Trump's repeal of the Deferred Action for Childhood Arrivals (DACA) policy which protected over 800,000 children of undocumented immigrants currently residing in the U.S., the AMA published the policy to reinforce its stance on immigration policy.[35] The Association announced that it has had a "long-established opposition to any federal legislation requiring physicians to establish the immigration status of their patients or collect and report data regarding an individual patient's legal resident status."[36] These ethical drivers rooted in the medical profession provide a reasonable explanation why some providers choose to ask fewer questions or take creative measures to relieve the fear undocumented immigrants might have if asked to share certain information.

II. POTENTIAL LEGAL, ETHICAL, AND PROFESSIONAL IMPLICATIONS

To treat a patient effectively, sufficient patient information is critical and this is no different in the context of undocumented immigrants.[37] Without accurate or complete patient information, the physician risks malpractice as a result of rendering unsatisfactory care and claim billing liability.[38]

A. Unsatisfactory Standard of Care Delivered by the Provider to the Patient Due To Inadequate Medical Information

When a provider delivers quality of care that is questionable, she opens

34. Am. Medical Ass'n, *supra* note 27.
35. Shear & Davis, *supra* note 4; *Id*.
36. Am. Medical Ass'n, *supra* note 27.
37. Shoever et al., *supra* note 8.
38. *Id*.; 31 U.S.C. § 3729 (2016) (imposing a penalty under federal law of up to $10,000 plus 3 times actual damages for every false claim for services under the Medicare program and similar laws apply at the state level).

herself up to investigation and potential actions against her medical license.[39] Trust is a significant part of a healthy patient-doctor relationship, and that trust is challenged when an undocumented immigrant presents to a provider who she fears may report her.[40] Without trust, there is an unstable foundation for open communication, necessary for the doctor to make important, informed decisions, such as choosing the best course of treatment.[41] This shaky patient-doctor relationship is further strained when the undocumented immigrant provides incomplete and/or inaccurate information because it results in unsatisfactory care for the undocumented immigrant.[42] For example, knowledge of legal status often helps doctors connect their patients with valuable resources and care.[43] Continuation of care also becomes a struggle when a provider does not have a patient's contact information for when they miss an appointment or need to be referred to a specialist.[44] In addition to the risk it brings on the provider's medical license, providing unsatisfactory care to a patient contradicts the Hippocratic Oath to do no harm.[45]

Rhetoric that surrounds immigration and, more specifically, undocumented immigrants, often lands on the intersection between healthcare policy and immigration policy. Conservatives, for example, blame undocumented immigrants for the high costs of the U.S. healthcare system.[46] Some might argue that the unsatisfactory care of undocumented immigrants

39. ILL. DEPT. OF PUBLIC HEALTH, http://www.dph.illinois.gov/topics-services/health-care-regulation/complaints (last visited Nov, 18, 2017) (providing a vehicle for patients and other citizens to report a healthcare provider for issues related to quality of care and medical errors)

40. W.A. Rogers, *Is There a Moral Duty for Doctors to Trust Patients*?, 8 AMA J. OF ETHICS (2002), http://jme.bmj.com/content/28/2/77.

41. *Id*.

42. Shoever et al., *supra* note 8.

43. Okwerekwu, *supra* note 7.

44. *Id.*

45. Sconyers & Tate, *supra* note 6.

46. Fred Arnold, *Providing Medical Services to Undocumented Immigrants: Costs and Public Policy*, 13 THE INT'L MIGRATION R. 706, 711 (1979).

is not enough to warrant a heightened awareness for this issue. It is for that reason this Article also sheds light on how incomplete and/or inaccurate patient information not only harms the undocumented immigrant, it also increases risks for the provider.[47]

B. Claim Billing Liability

Providers have an obligation under the FCA to ensure all bills submitted for reimbursement are free from any inaccurate, false, or misleading information.[48] Even where a provider meets the FCA's duty to ensure the information on a patient claim is accurate, providers might still face liability under the FCA's implied false certification theory.[49] Under this theory, a provider might be liable if they submit a claim for payment to the government but knowingly omits to disclose the provider's noncompliance with a material statutory, regulatory, or contractual requirement.[50] Penalties of submitting a claim for reimbursement that contains false or inaccurate information could cost a physician up to $10,000, plus three times actual damages for every false claim for services under the Medicare program.[51] Industry guidance also urges physicians to verify and audit their medical records, ensuring they are of the upmost integrity.[52]

---

47. Sconyers & Tate, *supra* note 6 (discussing the legal and moral implications of choosing to turn away an undocumented immigrant).

48. 31 U.S.C. § 3729 (2016); Sconyers & Tate, *supra* note 6.

49. Universal Health Servs., Inc. v. United States ex rel. Escobar, 136 S.Ct. 1989, 200-02 (2016) (affirming the viability of the implied false certification theory).

50. *Id. (*providing that the FCA defines materiality as "having a natural tendency to influence, or be capable of influencing the payment or receipt of money or property).

51. 31 U.S.C. § 3729 (2016); *see* Press Release, Off. of Pub. Affairs, U.S. Dep't of Justice (July 13, 2016), https://www.justice.gov/opa/pr/minnesota-based-hospice-provider-pay-18-million-alleged-false-claims-medicare-patients-who (reporting that a Minnesota-Based hospice provider to pay $18 million for alleged false claims to Medicare for patients who were not terminally ill and for failure to ensure accurate and complete documentation of patient's conditions in medical records).

52. AMERICAN HEALTH INFORMATION MANAGEMENT ASSOCIATION, INTEGRITY OF THE HEALTHCARE RECORD: BEST PRACTICES FOR EHR DOCUMENTATION (2013 UPDATE), (2013), http://library.ahima.org/doc?oid=300257#.WbWMmdPyuCQ (defining medical record integrity to include accurate patient identification and proper auditing the documentation for validity before submitting for claim reimbursement).

III. TAKEAWAYS FOR TREATING UNDOCUMENTED PATIENTS

It is not only undocumented immigrants who suffer from their unauthorized status as they attempt to care for their health; the physician providing treatment must also make challenging decisions that carry heavy costs.[53] On one end of the spectrum, the provider may choose to turn a blind eye, acknowledge the barriers that undocumented immigrants face in seeking care, and choose to advocate for health care as a "human right" rather than an "American right." This choice, however, presents increased risks for both the patient and the provider. On the other end of the spectrum, the provider may choose to take precautionary measures such as enforcing increased screening policies. This choice, too, comes with its own risks such as the increased potential to violate equal protection laws. While this Article does not seek to provide legal advice or to analyze the viability of either approach, it intends to, at minimum, start this conversation.

In efforts to be as well informed as possible about this subject, it is imperative that providers know what is and isn't required of them. While there is no legal duty to report or treat undocumented immigrants,[54] providers are led by professional ethics to treat patients regardless of U.S. citizenship status and to respect the patient's confidentiality.[55] The provider should know that she does not have to treat any patient if she believes the patient is providing incomplete or inaccurate information that will hinder the provider's ability to accurately treat the patient.[56] If the provider chooses to treat the patient, the provider should ensure that appropriate billing practices are in place such that no fraudulent claims are submitted as per direction from the appropriate payer.[57] Whether an undocumented patient is who they say

53. Sconyers & Tate, *supra* note 6.
54. *Id.*
55. *Id*.
56. *Id*.
57. *Id*.

they are, it is the provider's duty to ensure that no claims are submitted until that information is verified.[58]

One solution proposed to combat the issues that arise from the lack of medical information of undocumented immigrants is patient-held records (PHR).[59] A PHR can take many forms but, ultimately, it is a record of the patient's health information that the patient keeps and carries from provider to provider.[60] PHRs can be extremely beneficial for the treatment of undocumented immigrants because they allow the patient to control the privacy, security, and confidentiality of their records.[61] In addition, a PHR improves continuity of care and encourages patients to take an active role in their health care.[62] In addition to concerns about ownership, critics of PHRs highlight the privacy concerns that might arise from patients possessing more control of their protected health information.[63] However, research has shown that there are no substantial practical drawbacks and there are considerable benefits.[64] Several models of patient held record-keeping have been developed and some countries such as Australia have attempted to implement a national model in past years.[65] Health systems developers have also designed several portals that allow patients to access, manage, and share their

58. *Id*.

59. Shoever, *supra* note 8.

60. Marjolein Gysels, *Does the Patient-Held Record Improve Continuity and Related Outcomes in Cancer Care: A Systematic Review*, 10 HEALTH EXPECTATIONS 75, 77 (2006), http://onlinelibrary.wiley.com/doi/10.1111/j.1369-7625.2006.00415.x/full; Lassere et al., BIOMED CENTRAL, THE COMMUNICATE TRIAL 3 (2015), https://trialsjournal.biomedcentral.com/articles/10.1186/s13063-015-0760-8 (providing examples of PHRs that include smart cards, CD ROMs, USB flash drives, and secure web-based portals).

61. LASSERE ET AL., BIOMED CENTRAL, THE COMMUNICATE TRIAL 2 (2015), https://trialsjournal.biomedcentral.com/articles/10.1186/s13063-015-0760-8.

62. *Id*.

63. *Id*. at 2.

64. *Id.*

65. *Id.* at 4 (reporting that between 1999 to 2004, Australia implemented one approach to PHRs called the Health Connect Project and the National E-Health Transition Authority (NEHTA), which included a network of unique patient and provider identifiers. In 2009, Australia again revisited the concept of PHRs through the implementation of the opt-in Personally Controlled Electronic Health Record System (PCEHR) system).

health information.[66] Because this proposed solution is not necessarily within the controls of the physician, providers may consider speaking to their attorneys for guidance in this area.[67]

IV. CONCLUSION

It is not only the undocumented immigrant whose relationship with the healthcare system is complicated by their undocumented status; the physician's role in treating the undocumented patient is also complicated when she renders healthcare services while referencing inadequate medical information. While looking the other way or asking fewer questions might seem to be furthering the medical profession's interest to protect equitable access to healthcare, it also exposes the provider to legal, ethical, and professional liabilities. Additionally, while this approach might seem to be in the best interest of the patient, it increases the risk that the provider will render an unsatisfactory quality of care. It is imperative that physicians consider and understand the implications that arise from treating undocumented immigrants while referencing incomplete or inaccurate medical information an implement appropriate procedures that will minimize the legal and ethical risks highlighted in this Article.

66. *Id.* at 3 (citing several examples of PHRs such as Microsoft HealthVault and Dossia which are both web-based personal health records that are operating today).

67. *See* Sconyers & Tate, *supra* note 6.

Privacy in Public Health Crisis: A Question of Culture

Natalie Novak

I. INTRODUCTION

Americans think of privacy as an unlimited personal right, believing that it is sacrosanct and inalienable since the founding of the United States.[1] Despite this belief, current statutory, regulatory, and case law dictate the right to privacy is limited and may be infringed upon by both the federal and state government.[2] These perspectives demonstrate diametric differences between American citizens' desires for their personal privacy and the government's desire to control its citizens' privacy to protect the general welfare through public health efforts.[3] American law is grounded in principles and ideals focused on the greater good of society.[4] In light of the foundation of American law, at what point does an American's right to personal privacy subside to the greater good of society?

The privacy expectations of Americans must be shifted in perspective to focus on benefitting the general public, rather than emphasizing individual sacrifices of privacy when the federal or state government takes action to

1. *See* Kaci Hickox, *Caught Between Civil Liberties and Public Safety Fears: Personal Reflections from a Healthcare Provider Treating Ebola*, 11 J. HEALTH & BIOMED. L. 9, 9 (2015) (discussing Hickox's Ebola experience); Hickox v. Christie, 205 F. Supp. 3d 579, 584 (D.N.J. 2016).

2. *See* Griswold v. Connecticut, 381 U.S. 479, 1678 (1965).

3. Jim Harper, *Reforming Fourth Amendment Privacy Doctrine*, 57 AM. U. L. REV. 1381, 1386-1404 (2007-2008).

4. *See* Patrick M. McFadden, *Fundamental Principals of American Law,* 85 CAL. L. REV. 6 (1997).

protect society's health.[5] Resolving this conflict requires educating Americans about their misconception that privacy rights are unlimited but rather may be limited in situations where the government must protect the society at large. For example, the federal or state government is free to institute quarantine measures, as long as the quarantine procedure abides by Constitutional limitations, in order to protect the public from a potential disease threat.[6]

The 2014 Ebola Virus outbreak is a recent example of a public health crisis where the government prevented further adverse effects to the general public by limiting individuals' privacy rights.[7] The spread of the Ebola Virus, as a result of increasing globalization, moved quickly and affected many different parts of the world, including the United States.[8] Examining the limitations of privacy rights through the lens of the Ebola Virus crisis demonstrates a needed change in the American cultural understanding of privacy protections and limitations. Part I of this article will discuss the American right to privacy and its history, followed by Part II which describes the translation of the American right to privacy into a health care right to privacy. Next, Part III will discuss privacy in the context of quarantine. Finally, Part IIII will discuss the recent Ebola Virus outbreak and the application of the federal and state government's power to limit privacy.

---

5. Lee Rainie & Shiva Maniam, *Americans Feel Tensions Between Privacy and Security Concerns*, PEW RES. CTR. (Feb. 2016); Janlori Goldman, *Balancing in A Crisis? Bioterrorism, Public Health and Privacy*, 38 J. HEALTH L. 481, 499-503 (2005).

6. *Disclosures for Public Health Activities*, U.S. DEP'T HEALTH & HUM. SERVS., https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/disclosures-public-health-activities/index.html (last visited Sept. 30, 2017).

7. Jennifer Kates et al., *The U.S. Response to Ebola" Status of the FY2015 Emergency Ebola Appropriation*, HENRY J. KAISER FAMILY FOUND., https://www.kff.org/global-health-policy/issue-brief/the-u-s-response-to-ebola-status-of-the-fy2015-emergency-ebola-appropriation/ (last updated Dec. 11, 2015).

8. *CDC Outbreaks Chronology: Ebola Virus Disease,* CDC https://www.cdc.gov/vhf/ebola/outbreaks/history/chronology.html (last visited Sept. 30, 2017) [hereinafter *CDC Outbreaks Chronology*].

II. THE AMERICAN EXPECTATION OF PRIVACY

The right to privacy is one of the most sacrosanct individual rights of modern American citizens.[9] Privacy provides Americans the opportunity to live their lives free from government interference as well as affords an increase in the depth of other American fundamental rights.[10] However, questions arise as to if and when the right to privacy becomes limited or strained.[11] Many Americans advocate for unlimited privacy rights.[12] However, current statutory and regulatory laws do not grant such an unlimited right to privacy.[13] While privacy is a venerated right among the American public, it may be limited for the protection of public health.[14] Many Americans view this limitation as an unnecessary invasion of the individual right to privacy or as an overextension of the federal and state government's power.[15] While this public sentiment should be acknowledged, it illustrates a need to increase the public's understanding of the government's full authority to limit the right of privacy in the face of threats to public welfare through methods such as quarantine for the prevention of disease.[16]

---

9. Mary Madden & Lee Rainie, *Americans' Attitudes About Privacy, Security and Surveillance*, PEW RES. CTR. (May 2015) ("The majority of Americans believe it is important – often "very important" – that they be able to maintain privacy and confidentiality in commonplace activities of their lives. Most strikingly, these views are especially pronounced when it comes to knowing what information about them is being collected and who is doing the collecting.").

10. Griswold v. Connecticut, 381 U.S. 479, 479 (1965); Rainie & Maniam*, supra* note 5; Madden & Rainie, *supra* note 9; Lee Rainie, *The State of Privacy in Post-Snowden America,* PEW RES. CTR. (September 2016); *see also* Lawrence v. Texas, 539 U.S. 558 (2003) (providing for right to intimate association); *see also* Loving v. Virginia 388 U.S. 1 (1967) (providing for a right to marry).

11. Rainie, *supra* note 10.

12. Rainie & Maniam, *supra* note 5.

13. Goldman, *supra* note 5, at 481.

14. *Id.* (stating that privacy rights may be limited for public health as well as national security).

15. *Id.*

16. *Id.*

III. HEALTHCARE PRIVACY LAW

The individual right to privacy is not an inherent right granted by the United States Constitution.[17] In *Griswold v. Connecticut*, the United States Supreme Court recognized privacy as a protected right existing within the "penumbras" or shadows of Constitutional rights.[18] *Griswold* examined whether women possessed a right to use birth control and the degree of privacy afforded to marriage.[19] The Court ultimately held that the Constitution, through the Bill of Rights, recognized the right to privacy as a fundamental right.[20] The Court further held that the breadth and substance of enumerated rights require the acknowledgment of the right to privacy to recognize full protections of other expressly given rights.[21]

While *Griswold* serves as the seminal case on privacy rights,[22] subsequent privacy precedents further extended *Griswold*'s privacy protections to other aspects of an individual's personal life such as private relationships, civil rights, and criminal protections.[23] The evolving canon of privacy cases demonstrates the American public's demands for individual privacy

17. *See* Griswold v. Connecticut, 381 U.S. 479 (1965).

18. *Id.* at 1680-82 (stating "existing within the shadows" refers to rights that exist though not expressly given).

19. *Id.* at 1679-81; David Helscher, *Griswold v. Connecticut and the Unenumerated Right of Privacy*, 15 N. ILL. U. L. REV. 33, 38-43 (1994).

20. *See* Griswold, 381 U.S. 479; *see also* Helscher, *supra* note 19.

21. *See* Griswold, 381 U.S. 479; *see also* Helscher, *supra* note 19, at 33 ("United States Supreme Court first recognized that there are behavioral matters into which the government may not intrude, specifically adult consensual marital sexual relations.").

22. Griswold, 381 U.S. 479; *see also* Helscher, *supra* note 19.

23. *See* Sorell v. IMS Health Inc., 564 U.S. 552, 556 (2011) ("[P]rivacy is a concept too integral to the person and a right too essential to freedom to allow its manipulation to support just those ideas the government prefers."); *see also* Katz v. U.S., 389 U.S. 347 (1967) ("[P]erson's general right to privacy—his right to be let alone by other people—is, like the protection of his property and of his very life, left largely to the law of the individual States."); *see also* Eisenstadt v. Baird, 405 U.S. 438 (1972) (discussing privacy rights of birth control in unmarried relationships); *see also* Lawrence v. Texas, 539 U.S. 558 (2003) (discussing privacy rights within sexual acts); *see also* Mapp v. Ohio, 367 U.S. 643, 1685 (1961) (concerning privacy rights in relation to unreasonable searches and seizures); Roe v. Wade, 410 U.S. 113, 164 (1973) (providing right to privacy within fourteenth amendment); NAACP v. Alabama, 357 U.S. 449, 1166 (1958) (discussing privacy rights in relation to the Fourteenth Amendment).

contrasted by the federal and state government's ability to limit the scope of privacy rights.[24] Through these various cases, courts have been able to not only define the right to privacy but also set a reasonable scope of privacy for the American public.[25]

A. Health Insurance Portability and Accountability Act of 1996

The Health Insurance Portability and Accountability Act of 1996 ("HIPAA") serves as evidence of the ongoing expansion of American privacy rights.[26] Congress passed HIPAA with the intent of making healthcare delivery more efficient and to increase the amount of health insurance coverage.[27] As Congress continued to draft HIPAA, it became apparent that there was a significant risk of exposing digital health records as a result of possible data breaches and misuse.[28] To combat these concerns, Congress added provisions under the HIPAA Privacy Rule that required healthcare entities to develop adequate security measures to protect the new electronic health information from data breaches.[29] Through their debates, Congress realized that digitizing health information would be the most effective method to accomplish these goals.[30]

The HIPAA Privacy Rule's required security measures protect individually identifiable health information or protected health information ("PHI") by mandating that healthcare providers and other users of PHI

24. *See* Rainie, *supra* note 10.

25. Griswold, 381 U.S. 479; Helscher, *supra* note 19.

26. 45 C.F.R. § 164.512; Stephen B. Thacker, *HIPAA Privacy Rule and Public Health: Guidance from the CDC and the U.S. Department of Health and Human Services*, https://www.cdc.gov/mmwr/preview/mmwrhtml/m2e411a1.htm (last visited Sept. 30, 2017).

27. *Beyond the HIPAA Privacy Rule: Enhancing Privacy, Improving Health Through Research*, NAT'L ACADS. PRESS (2009), https://www.ncbi.nlm.nih.gov/books/NBK9576/ [hereinafter *Beyond the HIPAA Privacy Rule*].

28. *Id.*

29. *Id.*; *Summary of the HIPAA Privacy Rule*, U.S. DEP'T HEALTH & HUM. SERVS., https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html (last updated July 26, 2013) (providing that HIPAA is the authorizing statute for the HIPAA Privacy Rule).

30. *Beyond the HIPAA Privacy Rule, supra* note 27.

provide adequate security measures, such as limiting access of files and using physical barriers to protect information.[31] However, HIPAA acknowledges that privacy rights given to PHI are subject to limitations and states that public health authorities may collect PHI for use in aiding the prevention of disease, public health surveillance, and public health interventions.[32] HIPAA requires authorized public health officials to use or disclose PHI only when they are acting in good faith and with the belief that the use or disclosure is necessary to protect the public at large.[33] The situations and activities during which PHI use and disclosure are permitted are limited in scope and must be justified before the commencement of said use or disclosure.[34]

Thus, HIPAA provides a primary example of the conflicting understanding of what the right to privacy looks like: although there is some protection afforded to PHI, the government can override these protections for public health concerns, such as disease prevention.[35]

B. State Privacy Law

In addition to federal law, states also have their own privacy laws and statutes.[36] State laws may add or expand individual privacy rights and are only constrained by federal laws which grant federal rights.[37] The full authority states possess over their citizens' privacy rights results in differing state ideologies pertaining to personal privacy.[38] For example, only ten states

31. 45 C.F.R. § 164.500; *HIPAA Security Series*, U.S. DEP'T HEALTH & HUM. SERVS., https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/security101.pdf?language=es (last updated Mar. 2007).

32. 45 CFR 160.103; 45 CFR 164.501; 42 U.S.C. § 1320d–6 (stating that the list of occurrences in which the government may use PHI is not exclusive and therefore other appropriate times of use may exist).

33. 87 AM. JUR. 3D *Proof of Facts* § 259 (2006); *see also Disclosures for Public Health Activities*, *supra* note 6.

34. 87 AM. JUR. 3D *Proof of Facts* § 259 (2006); *see also Disclosures for Public Health Activities*, *supra* note 6; Goldman, *supra* note 5, at 510.

35. *See Disclosures for Public Health Activities*, *supra* note 6.

36. U.S. CONST. amend. X; ILL. CONST. art. I, § 6; Harper, *supra* note 3, at 512.

37. U.S. CONST. amend. X; ILL. CONST. art. I, § 6; Harper, *supra* note 3, at 512.

38. *See States*, HEALTH INFO. & L., http://www.healthinfolaw.org/state (last visited Oct.

have laws that explicitly recognize the right to privacy.[39] For instance, Illinois recognizes the right to privacy, but acknowledges that this right is not absolute.[40]

On the other hand, some states adopt privacy laws through various acts including medical privacy acts and patient rights acts.[41] The various acts are forms of privacy protection that address specific issues and provide further privacy protection than what is afforded by HIPAA.[42] For example, the Illinois Medical Patient Rights Act provides protection for patients' medical records and other information, unless there is an exception provided by law.[43] In addition, Illinois specifically requires patients' privacy protection in mental health treatment and substance abuse treatment.[44] Comparatively, Tennessee has an exhaustive list of medical privacy legislation.[45] Not only does Tennessee legislation provide privacy rights in substance abuse and mental health, but Tennessee legislation also includes privacy rights in cancer, sexually transmitted diseases, abortion, and congenital disabilities, among many other topics.[46] The variance in privacy laws between states is

---

23, 2017); *see also* Lara Cartwright-Smith et al., *Health Information Ownership: Legal Theories and Policy Implications*, VAND. J. ENT. & TECH. L. (2016), http://www.jetlaw.org/journal-archives/volume-19/volume-19-issue-2/health-information-ownership-legal-theories-and-policy-implications/.

39. *Privacy Protections In State Constitutions*, NAT'L CONF. ST. LEGISLATURES, http://www.ncsl.org/research/telecommunications-and-information-technology/privacy-protections-in-state-constitutions.aspx (last visited Sept. 30, 2017).

40. U.S. CONST. amend. X; ILL. CONST. art. I, § 6; People v. Cornelius, 821 N.E.2d 288, 298 (2004).

41. 45 C.F.R. §160.203; *see also* Goldman, *supra* note 5; *What Are My Health Care Rights and Responsibilities?*, U.S. DEP'T HEALTH & HUM. SERVS., https://www.hhs.gov/answers/health-care/what-are-my-health-care-rights/index.html (last visited Nov. 29 2017).

42. Jessica Luna, *Texas Medical Privacy Act Adopts and Expands the HIPAA Privacy Regulations,* U. HOUSTON'S HEALTH L. & POL'Y INST. (2001), https://www.law.uh.edu/healthlaw/perspectives/Privacy/010830Texas.html; *see also State HIV Laws*, CDC, http://www.cdc.gov/hiv/policies/law/states (https://perma.cc/DWU5-KRG4) (last updated Mar. 14, 2017) [hereinafter *State HIV Laws*].

43. 410 ILL. COMP. STAT. ANN. 50/3.

44. *Privacy and Confidentiality in Illinois*, HEALTH INFO. & L., http://www.healthinfolaw.org/state-topics/14,63/f_states (last visited Oct. 23, 2017).

45. *Id.*

46. *Id.*

further evidence of the errored American perspective of a right to unlimited privacy; not only is privacy limited, but it is also unequal among fellow Americans.[47]

IV. PRIVACY IN ACTION: QUARANTINE

Individual privacy rights are often implicated in the context of public health crises, especially in relation to quarantines.[48] Federal law recognizes quarantine powers are within the province of the states' police power.[49] Under the states' police power, state surgeon generals are authorized to make protective decisions, including the decision to quarantine, through their respective departments of health and human services.[50] For example, Illinois law provides that the State Department of Public Health oversees the interest of the state and may use isolation and quarantine methods to preserve public health.[51] Illinois law further provides that individuals who are subject to isolation or quarantine are entitled to legal counsel.[52] Thus, Illinois possesses the power to legally and significantly limit the privacy rights of its individual residents for the greater good of society.[53]

However, federal law limits the exercise of state police power to implement quarantine laws by requiring the state legislatures limit the scope of quarantine laws.[54] Specifically, federal law requires quarantine must be

47. *See States*, *supra* note 38; *see also* Eyragon Eidam & Jessica Mulholland, *10 State Take Privacy Matters Into Their Own Hands*, GOV. TECH (Apr. 10 2017), http://www.govtech.com/policy/10-States-Take-Internet-Privacy-Matters-Into-Their-Own-Hands.html.

48. 20 ILL. COMP. STAT. ANN. 2305/2.

49. *See State HIV Laws*, *supra* note 42.

50. *Id.* at 68.

51. 20 ILL. COMP. STAT. ANN. 2305/2.

52. Jacobson v. Commonwealth of Massachusetts, 197 U.S. 11, 25 (1905); 42 U.S.C.S. § 264.

53. *See* Jacobson, 197 U.S.

54. Nazita Gamini, *The Need for Stronger Implementation of Quarantine Laws: How Adopting China's Strategy to Fight SARS Can Help the United States Effectively Utilize Quarantine Powers in the Fight Against Ebola,* 11 J. HEALTH & BIOMED. L. 57, 86 (2015).

completed in "the least restrictive[55] means necessary so as to not infringe upon the federal government's powers under the Commerce Clause.[56] In addition, federal law also provides that the Surgeon General has authority to make protective decisions, such as quarantine, through the Department of Health and Human Services akin to the state-level surgeons general.[57]

One approved method of quarantine is the Centers for Disease Control and Prevention's ("CDC") quarantine stations which are "located at ports of entry and land border crossings."[58] At the quarantine stations, potentially infectious individuals are separated from the general population and their ability to move is restricted until it is determined whether the individual will in fact become infected with a disease.[59] The CDC describes the scope of authority of the quarantine stations as having the ability to detain any person that may be infected with a disease specified in an Executive Order.[60] Thus, quarantine is a legal and extreme method of public health protection that significantly infringes upon American citizens' personal right to privacy.[61] While quarantine has rarely been used, it reflects the length of the government's ability to remove individual privacy rights for the greater good

55. *See* Shelton v. Tucker, 364 U.S. 479, 488 (1960) ("[P]urpose cannot be pursued by means that broadly stifle fundamental personal liberties when the end can be more narrowly achieved."); Alan O. Sykes, *The Least Restrictive Means,* 70 U. CHI. L. REV. 403, (2003) (stating least restrictive means refers to using the minimal amount of force or limitation to accomplish a governmental goal).

56. *See* Emanuel Francone, *Commerce Clause*, CORNELL L. SCH., https://www.law.cornell.edu/wex/commerce_clause (last updated June 2016) (discussing that Commerce Clause allows Congress to regulate all things that relate to the buying and selling of items); Gamini, *supra* note 54.

57. Gamini, *supra* note, 54 at 68.

58. *Quarantine and Isolation*, CDC, https://www.cdc.gov/quarantine/index.html (last visited Nov. 28, 2017) [hereinafter *Quarantine and Isolation*].

59. *See id.*; *US Quarantine Stations*, CDC, https://www.cdc.gov/quarantine/quarantine-stations-us.html (last visited Nov. 28, 2017) [hereinafter *US Quarantine Stations*] (providing there are currently 20 quarantine stations).

60. *See US Quarantine Stations*, *supra* note 59; *FAQ's About Executive Orders*, NAT'L ARCHIVES, https://www.archives.gov/federal-register/executive-orders/about.html (last visited Nov. 28, 2017) ("Executive Orders are official documents, numbered consecutively, through which the president of the united states manages the operations of the federal government.").

61. Gamini, *supra* note, 54 at 68.

of the American public.[62]

V. EBOLA

A. Globalization

The American public typically carries little concern regarding privacy in a public health crisis, most likely because the majority of Americans have not been affected by a public health crisis personally.[63] But with the rise of globalization, the changing landscape of travel and foreign goods, and the increasing spread of disease, the likelihood of being impacted by a public health crises increases.[64] Globalization has many definitions but generally refers to the changing landscape of travel, foreign business and trade, and the increasing spread of disease as a result of the increased movement of people and goods.[65] The World Health Organization has stated that globalization has led to "a result of increased amount, frequency and speed of population

62. *Id.*

63. *See Public Health as a Problem-Solving Activity: Barriers to Effective Action*, NAT'L ACADS. PRESS (1988), https://www.ncbi.nlm.nih.gov/books/NBK218227/.

64. Lance Saker et al., *Globalization and infectious diseases: A review of the linkages*, WORLD HEALTH ORG. (2004), http://www.who.int/tdr/publications/documents/seb_topic3.pdf \; U.S. Dep't Transportation, *Overseas Travel Trends*, https://www.rita.dot.gov/bts/sites/rita.dot.gov.bts/files/publications/us_international_travel_and_transportation_trends/2002/overtrends.html (last visited Sept. 30, 2017); *see also Globalization*, NAT'L ACADS. SCI., ENGINEERING, MED., http://needtoknow.nas.edu/id/challenges/globalization/ (last visited Nov. 14, 2017) ("The 2009 "swine flu" pandemic starkly illustrated the impact of globalization and air travel on the movement of infectious diseases—with the infection spreading to 30 countries within 6 weeks and to more than 190 countries and territories within months."); *Disease Go Global*, GLOBALIZATION 101, http://www.globalization101.org/diseases-go-global/ (last visited Nov. 15, 2017) ("Several new infectious diseases, including severe acute respiratory syndrome-associated coronavirus (SARS-CoV), henipaviruses (Hendra and Nipah), avian influenza virus, and the H1N1 virus (Swine influenza) are some of the newest diseases that have received much attention, due to their rapid spread around the world. Other historic, infectious diseases, such as West Nile fever, human monkeypox, dengue, tuberculosis, and malaria are reemerging as well. Other well-known, historic infectious diseases, such as tuberculosis, are also unfortunately making a comeback; in the United Kingdom, which had almost completely eradicated tuberculosis from the British Isles by 1953, about 9,000 new cases of the disease are reported annually (Public Health England, n.d).").

65. *See* Saker et al., *supra* note 64.

mobility" which in turn leads to quickly spread infectious diseases.[66] As diseases are able to spread quickly, the United States is more likely to utilize the instituted quarantine stations to stop the spread of disease.

B. 2014–16 Ebola Outbreak

The effect of globalization has led to various public health crises which impacted the United States,[67] with one of the most memorable crises being the Ebola Virus (Ebola) outbreak in 2014.[68] Ebola is a highly contagious disease which is spread through close contact with an infected person.[69] Once infected, a person has roughly a 50 percent chance of survival.[70] Ebola presents symptoms similar to other diseases, which can result in patients not receiving an accurate diagnosis for an extended period of time which can result in the disease continuing to spread at a rapid rate.[71] Once a patient is diagnosed, caregivers must take extra precautions to ensure that the disease does not spread through the use of protective measures.[72]

---

66. *Id.* at 5.

67. *CDC Timeline*, CDC, https://www.cdc.gov/museum/timeline/ (last visited Sept. 30, 2017) [hereinafter *CDC Timeline*].

68. *Id.*; *Situation Report Ebola Virus Disease*, WORLD HEALTH ORG., http://apps.who.int/ebola/ebola-situation-reports (last visited Nov. 28, 2017) [hereinafter *Situation Report Ebola Virus Disease*].

69. *CDC Case Definition for Ebola Virus Disease (EVD)*, CDC, https://www.cdc.gov/vhf/ebola/healthcare-us/evaluating-patients/case-definition.html (last visited Sept. 30, 2017) [hereinafter *CDC Case Definition for Ebola Virus Disease (EVD)*]; *Ebola Virus Disease Fact Sheet*, WORLD HEALTH ORG., http://www.who.int/mediacentre/factsheets/fs103/en/ (last visited Sept. 30, 2017) [hereinafter *Ebola Virus Disease Fact Sheet*].

70. *CDC Case Definition for Ebola Virus Disease (EVD)*, CDC, https://www.cdc.gov/vhf/ebola/healthcare-us/evaluating-patients/case-definition.html (last visited Sept. 30, 2017); *Ebola Virus Disease Fact Sheet*, WORLD HEALTH ORG., http://www.who.int/mediacentre/factsheets/fs103/en/ (last visited Sept. 30, 2017).

71. *CDC Case Definition for Ebola Virus Disease (EVD)*, CDC, https://www.cdc.gov/vhf/ebola/healthcare-us/evaluating-patients/case-definition.html (last visited Sept. 30, 2017); *Ebola Virus Disease Fact Sheet*, WORLD HEALTH ORG., http://www.who.int/mediacentre/factsheets/fs103/en/ (last visited Sept. 30, 2017).

72. *CDC Case Definition for Ebola Virus Disease (EVD)*, CDC, https://www.cdc.gov/vhf/ebola/healthcare-us/evaluating-patients/case-definition.html (last visited Sept. 30, 2017); *Ebola Virus Disease Fact Sheet*, WORLD HEALTH ORG., http://www.who.int/mediacentre/factsheets/fs103/en/ (last visited Sept. 30, 2017).

The 2014 Ebola outbreak predominantly took place in Guinea, Liberia, and Sierra Leone.[73] A total of thirty-six confirmed cases occurred in other countries, including the United States.[74] The outbreak lasted approximately two years and resulted in an estimated 28,616 documented infections and 11,310 deaths.[75] These numbers are staggering and may be difficult to contextualize. In order to truly appreciate the impact of Ebola, if the United States had a comparable outbreak, approximately 392,000 people would be infected resulting in 131,000 deaths.[76]

When analyzing these statistics and their ultimate effect on the general population, it shows how imperative it is to prepare for a public health crisis as grievous as Ebola. Granted, the countries affected by the Ebola outbreak have different resources and spend different amounts of their gross domestic products (GDP) on health care services.[77] However, the United States is inefficient in its healthcare delivery and healthcare system and ranks as one of the worst performing developed countries within the health industry.[78] It appears that although the United States spends a high percentage of its GDP

73. *CDC Outbreaks Chronology*, *supra* note 8.

74. *Id.* (discussing other countries effected by the Ebola outbreak including Italy, Mali, Nigeria, Senegal, Spain and the United Kingdom).

75. *Id.* (stating roughly 40% of confirmed cases resulted in death).

76. *Id.*; *The World Factbook*, CIA, https://www.cia.gov/library/publications/the-world-factbook/ (last visited Sept. 30, 2017) (Listing Guinea to have a population of 12,413,867, Liberia a population of 4,689,021, and Sierra Leone a population of 6,163,195 for a combined total of 23,266,083. These countries, Guinea, Liberia, and Sierra Leone have a combined population of 23,266,083 people. Therefore, .001(28,616/23,266,083=0.0012) percent of the population of these countries was affected by this outbreak; this percentage should not be taken lightly. The United States has a population of 326,625,791 (326,625,791x.001=326,625.791) people. If .001 percent of the United States' population were affected by a similar outbreak, roughly 392,000 people would have contracted Ebola. Out of the estimated number of United States citizens infected, roughly 131,000 (326,625.791x.4=130,650.3164) people would likely die from the disease).

77. *CDC Outbreaks Chronology*, *supra* note 8.

78. Maggie Fox, *United States Comes in Last Again on Health, Compared to Other Countries*, NBC NEWS (Nov. 16 2016), https://www.nbcnews.com/health/health-care/united-states-comes-last-again-health-compared-other-countries-n684851; *2016 Commonwealth Fund International Health Policy Survey - In New Survey of 11 Countries, U.S. Adults Still Struggle with Access to and Affordability of Health Care*, COMMON WEALTH FUND (2016), http://www.commonwealthfund.org/publications/in-the-literature/2016/nov/2016-international-health-policy-survey-of-adults.

on healthcare, Americans are not happy with the current healthcare system and its short comings.[79] One method used in tracking a country's level of health is the infant mortality rate which compares the number of infant deaths per 1,000 death for a given year.[80] The United States ranks as having one of the worst infant mortality rates, while Sierra Leone has a significantly better ranking.[81]

C. Ebola in the United States

The United States felt the Ebola outbreak's effects with four documented infections and one death.[82] One suspected case was Kaci Hickox,[83] a nurse who was suspected to have contracted Ebola while caring for patients in Sierra Leone.[84] Upon her return to the United States, Hickox was quarantined in New Jersey, despite testing negative for Ebola.[85] Hickox filed lawsuits against the State of New Jersey and New Jersey's governor Chris Christie, claiming that her quarantine violated her privacy rights under the Fourth and Fourteenth Amendments, in addition to filing state law claims of false

79. *See* Alan M. Garber & Jonathan Skinner, *Is American Health Care Uniquely Inefficient?*, J. ECON. PERSPECT., (Sept. 2008); *see also* David Squires & Chloe Anderson, *U.S. Health Care from a Global Perspective*, COMMON WEALTH FUND (Oct. 2017), http://www.commonwealthfund.org/publications/issue-briefs/2015/oct/us-health-care-from-a-global-perspective; *The World Factbook Country Comparison: Health Expenditures*, CIA, https://www.cia.gov/library/publications/the-world-factbook/rankorder/2225rank.html#us (last visited Nov. 18, 2017) (stating the U.S. ranks 1 while Sierra Leone ranks 13 out of 225 countries in Health Expenditures).

80. *The World Factbook Country Comparison: Infant Mortality Rate*, CIA, https://www.cia.gov/library/publications/the-world-factbook/rankorder/2091rank.html#us (last visited Nov. 18, 2017).

81. *Id.* (stating the U.S. ranks 170 while Sierra Leone ranks 10 out of 225 countries in infant mortality).

82. *2014 Ebola Outbreak in West Africa - Case Counts*, CDC, https://www.cdc.gov/vhf/ebola/outbreaks/2014-west-africa/case-counts.html (last visited Sept. 30, 2017) [hereinafter *2014 Ebola Outbreak in West Africa*].

83. Hickox, *supra* note 1 (discussing Hickox's Ebola experience); Hickox v. Christie, 205 F. Supp. 3d 579 (D.N.J. 2016).

84. Hickox, *supra* note 1 (discussing Hickox's Ebola experience); Hickox, 205 F. Supp. 3d.

85. Hickox, 205 F. Supp. 3d at 585-88.

imprisonment and false light.[86]

In response to Hickox's filed federal claims, the district court dismissed the federal claims.[87] The court reasoned that the government did not violate quarantine law as it met the federal test provided by *Jacobson v. Massachusetts*.[88] *Jacobson* provides that the government is able to use various methods to protect public health so long as the method is necessary for public health and safety, is reasonable and has a real, substantial relationship between the means and the ends, and finally, is proportional to the public health concern and not arbitrary, oppressive, or unjust.[89] The court determined that, given the severity of the threat imposed by Ebola and the government's desire to protect the American public, the quarantine procedure was legal under the *Jacobson* test.[90] Furthermore, the court held the government possessed qualified immunity[91] for the claims of violating the Fourth Amendment and its attached privacy rights.[92] Regarding the false light and false imprisonment claims, the court allowed the claims to continue and held the qualified immunity did not extend to these claims and further inquiry was warranted.[93]

Although the court expressed sympathy for Hickox's position, it acknowledged that her quarantine was not only reasonable but also necessary

86. *Id.* at 603-05 ("[T]he tort of false imprisonment requires (1) 'an arrest or detention of the person against his or her will' and (2) 'lack of proper legal authority or legal justification.'").

87. *Id.* at 584.

88. Jacobson v. Commonwealth of Massachusetts, 197 U.S. 11 (1905); Hickox, 205 F. Supp. 3d at 592; *see also* Wendy K Mariner et al., *Jacobson v. Massachusetts: It's Not Your Great-Great-Grandfather's Public Health Law*, 95 AM. J. PUB. HEALTH 581 (2005), https://www.ncbi.nlm.nih.gov/pmc/articles/PMC1449224/pdf/0950581.pdf.

89. Jacobson, 197 U.S.; Hickox, 205 F. Supp. 3d at 592.

90. Hickox, 205 F. Supp. 3d.

91. *Id.* at 589 ("[Q]ualified immunity shields government officials from civil liability as long 'as their conduct does not violate established statutory or constitutional rights of which a reasonable person would have known.").

92. *Id.* at 596-97.

93. *Id.* at 603-05.

because at the time Ebola quickly spread and lacked effective treatment.[94] Additionally, the court discussed the CDC's Ebola guidelines,[95] which discussed classifying healthcare workers who cared for Ebola patients within a risk of infection category.[96] The guidelines stated that healthcare workers who previously cared for Ebola patients were classified in a risk category of infection.[97] Hickox was able to have Maine's quarantine requirement overturned and returned to her home.[98]

VI. A CHANGE IN PERSPECTIVE

Hickox v. Christie presents an image of the American general public's nightmare—the loss of control over an individual's personal privacy within their own healthcare diagnosis.[99] As stated, HIPAA allows for the disclosure of PHI in times of public health crisis.[100] As Hickox posed as a potential risk to society, HIPAA allowed for the disclosure of her private information in order to protect public health.[101] Although Hickox lost a degree of her privacy, her quarantine and loss of privacy protected the general public from a significant and life-threatening risk.[102] While Hickox focuses on the individual perspective, if the perspective is changed to focus on the collective

94. *Id.* at 592-94.

95. *Id.* at 590.

96. Hickox, 205 F. Supp. 3d at 590; *Epidemiological Risk Factors To Consider When Evaluating A Person for Exposure to Ebola Virus*, CDC, https://www.cdc.gov/vhf/ebola/exposure/risk-factors-when-evaluating-person-for-exposure.html (last updated May 28, 2015) [hereinafter *Epidemiological Risk Factors*].

97. Hickox, 205 F. Supp. 3d.

98. Hickox, *supra* note 1, at 10.

99. *Id.* (discussing Hickox's Ebola experience); Hickox, 205 F. Supp. 3d; Lynn Sessions & Cory J. Fox, *United States: Ebola Information Quarantine: Balancing Patient Privacy with Public Health*, MONDAQ, http://www.mondaq.com/unitedstates/x/352396/Healthcare/Ebola+Information+Quarantine+Balancing+Patient+Privacy+With+Public+Health (last updated Nov. 6, 2014); *see also Disclosures for Public Health Activities*, *supra* note 6.

100. *See Disclosures for Public Health Activities*, *supra* note 6.

101. *Id.*

102. Hickox, *supra* note 1 (discussing Hickox's Ebola experience); Hickox, 205 F. Supp. 3d.

American public, Hickox's small sacrifice of privacy seems insignificant.[103]

American law is built upon principles and ideals for the greater good of society.[104] Indeed, Americans possess many individual rights, but these individual rights may be overshadowed by both the federal and state government's concern for the general public.[105] The argument of privacy infringement arises within the individual concern; however, Americans should focus upon the collective concern and support small sacrifices of privacy when necessary.[106]

VII. CONCLUSION

The American government is authorized to exercise reasonable limitations on privacy rights in many areas of an individual's life, including individual health and public health initiatives. Americans need to shift their perspectives regarding their individual rights to better understand the benefits that arise from a limited individual right to privacy for the benefit and protection of the collective good. By limiting privacy in some areas of an individual's life, the American public can be protected from global risks of public health crises. As new threats of public health crises are presented on a regular basis[107], understanding an individual's right to privacy will aid the United States in moving towards a focus on the collective good of public health.

---

103. Hickox, *supra* note 1 (discussing Hickox's Ebola experience); Hickox, 205 F. Supp. 3d; *see also* Madden & Rainie, *supra* note 9.

104. *See* McFadden, *supra* note 4.

105. Goldman, *supra* note 5, at 509.

106. *See* Madden & Rainie, *supra* note 9; *see also* Suyawen Hao, *An Analysis Of American Individualism Culture*, HAOSUYAWEN, https://haosuyawen.wordpress.com/2015/02/19/an-analysis-of-american-individualism-culture/ (discussing a comparison of American Individualism and Japanese collective culture).

107. *See CDC Current Outbreak List*, CDC, https://www.cdc.gov/outbreaks/index.html (last visited Nov. 28, 2017) (stating a new Ebola Virus Outbreak has been listed as an international threat as of May 2017, additionally as Mumps in New Zealand and Measles in Italy have been placed on the watch list as of November 2017).