# Lack of Privacy Regulations in the Fitness and Health Mobile App Industry: Assessing the Health Insurance Portability and Accountability Act (HIPAA) for Meeting the Needs of User Data Collection

JACQUELINE BUI*

## INTRODUCTION

Imagine a visit to your favorite breakfast restaurant, and just as you catch sight of your beloved bacon, eggs, and toast special at another table, there is a notification from your phone and an application chastising you to eat healthy for the week and avoid empty carbohydrates.[1] That degree of guidance and coaching (or micromanagement and meddling, depending on the user's mood), is a present-day reality, all made possible through the miniaturized personal computers most of us carry around in the form of a smartphone. Lark is a health and fitness mobile application or app, designed to motivate users by tracking their diet, exercise, and sleep schedule.[2] Although users find Lark to be helpful in improving their well-being, these apps also collect more than your information.[3]

Specifically, Lark's end-user licensing agreement and privacy policy state, "We may anonymize your personal information so that you cannot be individually identified, and provide that information to our partners."[4] The conditional language of the previous statement is broad and suggests the possibility of identifying the user to their data in de-anonymized form only to have this personal information revealed to third parties.[5] Lark is not the only app that shares consumer's data, but it is one of several in the mobile app industry that collects your private information with only the vague promise of anonymity.[6] The

*Jacqueline Bui is a graduate of the University of California Davis, where she received her B.A. in Psychology and Asian American Studies. She is a third-year law student at the University of San Francisco School of Law and is currently a visiting student at Boston College Law School. Jacqueline would like to thank adjunct professor, Brian Budds, for his guidance and assistance in developing the article. Jacqueline would also like to give special thanks to her family, friends, and colleagues for their support.

1. LARK, http://www.web.lark.com/ (last visited Mar. 6, 2017).
2. *Id.*
3. *Privacy Policy*, LARK, http://lark.com/lark-privacy-policy/ (last visited Mar. 6, 2017).
4. *Id.*
5. *Id.*
6. *See generally* Kenneth Olmstead, *Mobile apps collect information about users, with wide range of permissions*, PEW RESEARCH CENTER (Apr. 29, 2014), http:// www.pewresearch.org/fact-

invasion does not halt there, but health mobile apps may also legally collect information directly from your device, such as your friends and family's contact information, the use and status of other apps stored on your device, as well as the willful transfer of this data to third parties in an effort to monetize your information.[7]

This paper will explore the dangers created when health mobile apps have access to users' sensitive information with a lack of established consumer privacy protection. Although mobile apps collect data for the primary purposes of improving consumer's lives,[8] there is still potential to exploit end users by repurposing the data and selling to third parties.[9] Additionally, this may lead to violations of assumed privacy without proper consent, the propensity to make false predictions based on someone's health habits, which can result in higher health insurance premiums, companies delivering targeted and sensitive advertisements, and users being denied access to employment, life insurance, and housing.[10]

Similar abuses from health and medical professionals have occurred in the past, but with the enactment of the federal Health Insurance Portability and Accountability Act of 1996 (HIPAA), patients, in a healthcare setting, have more control over who can access their protected health information (PHI). Prior to the passing of HIPAA, individuals seeking treatment for their illness or disease could have been taken advantage of because physicians could take samples of their patient's cells, possibly revealing genetic information, without proper permission.[11] HIPAA expanded individual's privacy protection, outlawing the use of patient-level data without patients' consent or authorization.[12]

If there are no regulations on the collection, sharing, and selling of user information for this new mobile and Big Data frontier, then it may be possible to see similar levels of privacy exploitations in the mobile health app industry. This paper will first review the history of HIPAA, the HITECH Act, and Omnibus Rule and how it affects the current landscape of PHI. Section II compares cases prior to the enactment of HIPAA to a case after HIPAA's enactment. Section III investigates

---

tank/2014/04/29/mobile-apps-collect-information-about-users-with-wide-range-of-permissions/ (discussing the information and data collected by mobile apps and how users may be notified).

7. Andrew W. Bagley & Justin S. Brown, *Limited Consumer Privacy Protections Against the Layers of Big Data*, 31 SANTA CLARA HIGH TECH. L.J. 483, 489 (2015).

8. *Apple Announces ResearchKit Available Today to Medical Researchers*, APPLE PRESS INFO (Apr. 14, 2015), https://www.apple.com/pr/library/2015/04/14Apple-Announces-ResearchKit-Available-Today-to-Medical-Researchers.html.

9. *ToS and Privacy Policy*, AZUMIO (Sep. 1, 2014), http://azumio.com/page/privacypolicy.

10. Richard Warner & Robert H. Sloan, *Self, Privacy, and Power: Is It All over?*, 17 TUL. J. TECH. & INTELL. PROP. 61, 77 (2014).

11. REBECCA SKLOOT, THE IMMORTAL LIFE OF HENRIETTA LACKS 198 (Crown Publishing Group, 2010).

12. Deborah F. Buckman, *Validity, Construction, and Application of Health Insurance Portability and Accountability Act of 1996 (HIPAA) and Regulations Promulgated Thereunder*, 194 A.L.R. FED. 133 (2004).

how unprotected anonymized data may fall under HIPAA's "covered entities" criteria and how this may influence the transfer and sale of user information to third parties. Section IV examines the current state of data ownership once it has been collected and recorded, and what PHI belongs to health mobile app users versus mobile app developers. Section V analyzes the types of discrimination based on Big Data trends collected from mobile app users. Finally, Section VI provides some policy and legislative recommendations that will help ensure user privacy protections in this new era of fitness and health mobile apps.

## I. BACKGROUND ON HIPAA, HITECH, AND OMNIBUS RULE

Today, HIPAA Privacy Rule remains the first comprehensive federal health privacy law.[13] Prior to HIPAA, there was no national health security privacy standard in the health care field that would protect an individual's past, present, and future health information.[14] Essentially, healthcare providers, employers, and health insurers were legally allowed to collect and share patient health information throughout the health care system and to third parties.[15] Patients' sensitive health information could be accessed and distributed without the patient's consent, except in instances where state or local law had explicitly prohibited such practices.[16]

### A. THE ENACTMENT OF HIPAA

In 1996, Congress enacted HIPAA requiring the HHS to create regulations that would provide security and privacy protections for sensitive patient medical information, such as patients' PHI.[17] PHI is defined as, "individually identifiable health information, held or maintained by a covered entity or its business associates acting for the covered entity that is transmitted or maintained in any form or medium."[18] HIPAA pertains to a "covered entity," which is defined as "a health plan, healthcare clearinghouse, or healthcare provider who transmits health information in electronic form in connection with certain specified transactions."[19] This definition changed the way employers' group health plans, service providers and insurers, handled

13. Ronald L. Scott, *Cybermedicine and Virtual Pharmacies*, 103 W. VA. L. REV. 407, 442 (2001).

14. Kimberly L. Rhodes & Brian Kunis, *Walking the Wire in the Wireless World: Legal and Policy Implications of Mobile Computing*, 16 J. TECH. L. & POL'Y 25, 38 (2011).

15. BARRY R. FURROW ET AL., HEALTH LAW: CASES, MATERIALS AND PROBLEMS 267–268 (West Academic Publishing, 7th ed. 2013).

16. *Id.* at 268.

17. *See* Rhodes & Kunis, *supra* note 14, at 38.

18. *What Health Information Is Protected by the Privacy Rule?*, U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES NATIONAL INSTITUTES OF HEALTH, https://privacyruleandresearch.nih.gov/pr_07.asp (last updated Feb. 2, 2007).

19. Rhodes & Kunis, *supra* note 14, at 38.

and transmitted sensitive health information about their patients.[20] HIPAA provides protections for patients' confidential health information, and covered entities must seek authorization for any use or disclosure of PHI that is not for treatment, payment, or healthcare operations, or otherwise permitted or required by the HIPAA Privacy Rule. This Act severely limits the type and usage of patient level data to only what is necessary to provide and bill for healthcare services rendered.[21]

B. HIPAA AMENDED TO INCLUDE THE HITECH ACT

In 2009, when the medical industry shifted from a paper to an electronic healthcare system, progress influenced by subsidies and financial incentives provided by the Affordable Care Act (ACA), HIPAA was amended to include a new provision, entitled the Health Information Technology for Economic and Clinical Health (HITECH) Act to prevent electronic medical record breaches.[22] Originally, HIPAA only applied to certain "covered entities," and it did not require patients to authorize consent for treatment and payment purposes.[23] Under the HITECH Act, the protection was broadened so that group health plans included self-funded and insured group health plans of private and government employers.[24] This Act expanded the scope of how patient data would be protected from those with ulterior motives, including employers who wished to know the general health of their employees, and as a corollary, the relative stability of their personnel to health catastrophes.[25] Additionally, the group health plans subject to HIPAA privacy are defined more broadly to include dental, vision, medical flexible spending accounts, health reimbursement accounts, and employee assistance programs.[26] However, many of the insured group health plans handling only limited information are exempted from many of the HIPAA requirements.[27]

Most importantly, the HITECH Act includes "business associates," who must be HIPAA compliant.[28] Business associates are defined as, "persons or organizations that have access to a considerable amount of PHI in relations to the work and services they provide

20. Rhodes & Kunis, *supra* note 14, at 38.

21. Rhodes & Kunis, *supra* note 14, at 39.

22. Rhodes & Kunis, *supra* note 14, at 40.

23. Rhodes & Kunis, *supra* note 14, at 40.

24. 45 C.F.R. § 164.504(f)(1) (2015).

25. *See id.* § 164.504.

26. *Group Health Plan Compliance with HIPAA and ERISA: Navigating the Legal and Administrative Maze*, BROWN RUDNICK BERLACK ISRAELS LLP 5 (2003), https://benefitslink.com/articles/brownrudnick_hipaa.pdf.

27. *See id.* at 6.

28. Megan Bradshaw & Benjamin K. Hoover, *Not So Hip?: The Expanded Burdens on and Consequences to Law Firms As Business Associates Under Hitech Modifications to HIPAA*, 13 RICH. J.L. & PUB. INT. 313, 321 (2010).

directly to covered entities such as, 'consultants, accountants, claims processors, and law firms.'"[29] Business associates were described as such since the HITECH Act provided more agency oversight for U.S. Health and Human Service Department (HHS) investigations and for the Office of Civil Rights to enforce and levy fines for HIPAA civil and criminal violations.[30]

C. HIPAA AMENDED TO INCLUDE THE OMNIBUS RULE

In 2013, the amendments to HIPAA included the Omnibus Rule, further clarifying that liability extended down the chain from covered entities to business associates, including certain subcontractors because of the breaches from processing PHI.[31] HIPAA expanded "covered entities" to include "business associate(s)" and third parties such as "contractors or subcontractors."[32] Subcontractors are defined as, "any downstream subcontractor that creates, receives, maintains, or transmits PHI on behalf of the business associate, even if they have an indirect relationship with a covered entity."[33] Without the authorization of the individual, the Omnibus Rule created stricter limits on disclosing PHI for marketing and fundraising and prohibited the sale of PHI.[34] This applies to vicarious liability, for example, if a business associate is a covered entity's agent, the covered entity is liable for the business associate's HIPAA violations.[35] Additionally, a business associate is liable for a subcontractor's HIPAA violation,[36] and the civil and criminal penalties have increased. For civil violations, each violation will be fifty thousand dollars ($50,000) up to a maximum of one and a half million dollars ($1.5M) per calendar year.[37] While criminal violations will be two hundred fifty thousand dollars ($250,000) and imprisonment for up to ten years.[38]

---

29. *Id.* at 322.

30. *Id.* at 334.

31. Alicia Gilleskie & Mary Pat Sullivan, *Newly Effective HIPAA Omnibus Rule Makes Sweeping Changes to HIPAA*, SMITH ANDERSON (Apr. 5, 2013), http://www.smithlaw.com/updates-alerts-242.html.

32. *Id.*

33. *Id.*

34. *Final HITECH Omnibus Rules Tighten Breach Notice Sept. 23 Compliance Deadline for Most of Long-Delayed HIPAA Privacy, Security Changes,* 12 NO. 1 EMPLOYER'S GUIDE HIPAA PRIVACY REQUIREMENTS NEWSL. 2. (2013).

35. 45 C.F.R. § 160.402 (2016).

36. *Id.*

37. *HIPAA Final Rule Expands Liability for Violations, Clarifies Penalty Assessment Methodology*, CROWELL MORING (Feb. 22, 2013), https://www.crowell.com/NewsEvents/AlertsNewsletters/all/HIPAA-Final-Rule-Expands-Liability-for-Violations-Clarifies-Penalty-Assessment-Methodology.

38. *HIPAA Violations and Enforcement*, CALVET, https://www.calvet.ca.gov/Pages/HIPAA-Violations-and-Enforcement.aspx (last visited Mar. 6, 2017).

## II. CASE COMPARISON BEFORE AND AFTER THE ENACTMENT OF HIPAA

### A. PRIOR TO HIPAA

In 1951, Henrietta Lacks was a patient treated for cervical cancer at Johns Hopkins Hospital in Baltimore, Maryland.[39] Her oncologist, fascinated by the aggressiveness of her cancer, obtained a sample of her tumor to grow them in his laboratory for further investigation, all without Ms. Lacks expressed permission.[40] Ms. Lacks' cells were the first human cells to be "immortal," meaning that her cells, sampled from a dedifferentiated or immature, aggressive cancer, would not fail to replicate after several generations of cell division.[41] Ms. Lack's cell line later became known as HeLa cells and were the basis of several crucial medical breakthroughs relying on the study of these immortal cells.[42] Her cells allowed for the study and discovery of remarkable scientific advances including the invention of the polio vaccine and human stem cell cloning.[43]

Today, HeLa cells continue to be used for experiments in cancer,[44] HIV treatment,[45] and radiation, as research for anti-aging products,[46] as well as many other applications. These experiments resulted in almost eleven thousand (11,000) patents involving HeLa cells.[47] Despite the medical breakthroughs, there are major issues that arise on whether it was fair for her physicians and researchers to obtain these patents since they benefitted from using Ms. Lacks' cells without her or her family's knowledge and permission.[48] Over the years, individuals

---

39. Malcolm Ritter, *NIH, family of Henrietta Lacks reach deal on access to DNA code*, WASH. POST (Aug. 7, 2013), https://www.washingtonpost.com/national/health-science/nih-family-of-henrietta-lacks-reach-deal-on-access-to-dna-code/2013/08/07/68f3da04-ff8b-11e2-96a8-d3b921c0924a_story.html; *see also* REBECCA SKLOOT, *supra* note 11.

40. *See* REBECCA SKLOOT, *supra* note 11 at 57; *see also* Malcolm Ritter, *NIH, family of Henrietta Lacks reach deal on access to DNA code*, WASH. POST (Aug. 7, 2013), https://www.washingtonpost.com/national/health-science/nih-family-of-henrietta-lacks-reach-deal-on-access-to-dna-code/2013/08/07/68f3da04-ff8b-11e2-96a8-d3b921c0924a_story.html.

41. *See generally* REBECCA SKLOOT, *supra* note 11 at 138.

42. *See* REBECCA SKLOOT, *supra* note 11 at 2–4; *see also* Malcolm Ritter, *NIH, family of Henrietta Lacks reach deal on access to DNA code*, WASH. POST (Aug. 7, 2013), https://www.washingtonpost.com/national/health-science/nih-family-of-henrietta-lacks-reach-deal-on-access-to-dna-code/2013/08/07/68f3da04-ff8b-11e2-96a8-d3b921c0924a_story.html.

43. *See* REBECCA SKLOOT, *supra* note 11 at 93.

44. REBECCA SKLOOT, *supra* note 11 at 127–128.

45. REBECCA SKLOOT, *supra* note 11 at 214.

46. REBECCA SKLOOT, *supra* note 11 at 102.

47. *In 1951 a poor woman's cells were taken without permission, and they revolutionised medicine*, SCIENCE ALERT (Apr. 22, 2014), http://www.sciencealert.com/in-1951-a-poor-womans-cells-were-taken-without-permission-and-they-revolutionised-medicine.

48. Wynne Parry, *HeLa Cells Use Restricted Under New Agreement With Family Of Henrietta Lacks*, HUFFINGTON POST (Aug. 8, 2013, 2:55 PM), http://www.huffingtonpost.com/2013/08/07/hela-cells-restricted-under-agreement-henrietta-

and pharmaceutical companies have made considerable fortunes using HeLa-based experiments, yet Ms. Lacks' family remained destitute and largely unaware of the decades-long use of Ms. Lacks' tumor cell line. Her family was never financially compensated or acknowledged until the release of a best-selling novel describing Ms. Lacks' role in modern medicine and science.[49]

In *Moore v. Regents of Univ. of California*, a doctor was treating John Moore at the University of California Los Angeles (UCLA) Medical Center for hairy-cell leukemia.[50] Similar to Ms. Lacks, the physician in Mr. Moore's case would obtain samples of his bone marrow, blood, and tissues for the purposes of medical research without Mr. Moore's knowledge and authorization.[51] Mr. Moore sued the doctor and the medical center for extracting his cells for the use of commercially valuable research without his permission.[52] In 1990, the California Supreme Court held that once tissues have been removed from an individual's body, the donor no longer had any legal rights to his or her cell lines.[53] Thus, Mr. Moore had no rights to the profits and proceeds from the discoveries. Today, it is estimated that his cell line, Mo, is worth at least three billion dollars ($3B).[54]

### B. CASES AFTER HIPAA

In *Greenberg v. Miami Children's Hosp. Research Inst., Inc.*, a group of parents with children afflicted with Canavan disease, went to see a physician and three non-profits in hopes of identifying the gene responsible for Canavan disease.[55] The doctor and non-profit collected donated blood and body tissue samples from other Canavan families for the purposes of medical research.[56] Using these samples and the clinical and medical information database, the doctor and his research team successfully isolated and patented the sequence of the Canavan gene.[57] The parents sued the physician and the institutions on the basis that they had a property interest in the body tissues and genetic information.[58] In 2003, the United States District Court for the Southern District of Florida held that the plaintiffs suffered from

---

lacks_n_3720691.html.

49. Kimberly L. Rhodes & Brian Kunis, *Walking the Wire in the Wireless World: Legal and Policy Implications of Mobile Computing*, 16 J. TECH. L. & POL'Y 25 (2011).

50. 51 Cal. 3d 120 (1990).

51. *Id.* at 138.

52. *Id.* at 124.

53. *Id.* at 136–137.

54. Rebecca Skloot, *Taking the Least of You*, N.Y. TIMES MAG. (Apr. 16, 2006), http://www.nytimes.com/2006/04/16/magazine/taking-the-least-of-you.html.

55. 264 F. Supp. 2d 1064, 1066 (S.D. Fla. 2003).

56. *Id.*

57. *Id.*

58. *Id.* at 1074.

"unjust enrichment"[59] and that the physician and his team had benefited from the licensing fees negotiated under the commercial patent.[60]

The *Greenberg* case is similar to the situation that occurred with Ms. Lacks and Mr. Moore. In all these cases, physicians and researchers took samples of patient's cells and body tissue for the purposes of medical research. Similar to *Moore*, the *Greenberg* plaintiffs argued that their cells and body tissues were resulting in monetary gain. In *Moore*, the court held that Mr. Moore did not have property rights to his cells and body tissues and dismissed the claim of conversion. Although *Greenberg* made similar unsuccessful arguments, plaintiff's distinguishing claim of "unjust enrichment" was successful in court because the *Greenberg* patients made donations of their body tissues and cells; whereas, Moore did not.[61] The *Greenberg* case provides precedent for future cases concerning patents in biotechnology.

As of 2013, Ms. Lacks' family was able to finalize an agreement with the National Institute of Health (NIH) on a case-by-case basis to approve certain research using HeLa cells for the purpose of experiments and research.[62] Applicants will have to agree to restrictions, such as not sharing the DNA information with others, but they must report back on their results and acknowledge the Lacks in their publications.[63] This agreement shows an improvement among the modern medical research community to find more ethical and considerate approaches in handling patients' confidential health information.

## III. INFORMATION COLLECTED BY FITNESS AND HEALTH MOBILE APPS

Mobile app users voluntarily give away their data through everyday online interactions. Many of these interactions are handled with one-click agreements in which consumers agree to the software terms of use and privacy policy agreements.[64] Through seamless and sometimes subtle online interactions, consumers transmit data that is duplicated on multiple servers, shared to third parties, and repurposed in the Big Data marketplace.[65] Big Data refers to methods

---

59. *Id.* at 1072.

60. *See id.* at 1072 ("Under Florida law, the elements of a claim for unjust enrichment are (1) the plaintiff conferred a benefit on the defendant, who had knowledge of the benefit; (2) the defendant voluntarily accepted and retained the benefit; and (3) under the circumstances it would be inequitable for the defendant to retain the benefit without paying for it.")

61. *See id.* at 1074.

62. Parry *supra* note 48.

63. *Id.*; *see also* Malcolm Ritter, *NIH, family of Henrietta Lacks reach deal on access to DNA code*, WASH. POST (Aug. 7, 2013), https://www.washingtonpost.com/national/health-science/nih-family-of-henrietta-lacks-reach-deal-on-access-to-dna-code/2013/08/07/68f3da04-ff8b-11e2-96a8-d3b921c0924a_story.html.

64. *See generally* Roger E. Schechter, *The Unfairness of Click-on Software Licenses*, 46 WAYNE L. REV. 1735, 1736–37 (2000).

65. *See* Ira S. Rubinstein, *Big Data: The End of Privacy or a New Beginning?* 4 (N.Y.U.

organizations, including government and businesses use to "combine diverse digital datasets and then use statistics and other data mining techniques to extract from them both hidden information and surprising correlations."[66] In a current study, the U.S. Federal Trade Commission (FTC) held that developers of twelve mobile health and fitness apps were sharing user information, such as sensitive information about user's bodies and habits, with seventy-six different parties including advertisers.[67] Generally, most mobile apps will collect basic information such as usernames, email addresses, gender, and location.[68] However, fitness and health mobile apps will collect more than users' basic information, such as height, weight, nutrition data, workouts, sleep habits, and other health-related information, data previously only available to privileged individuals, including healthcare providers.[69] The other troubling concern is that mobile apps can extend their access to collect information in a phone's address book and contacts, which means that unintended parties would have access to the entire social network of an individual, even though only that particular person, the mobile app user, has consented to providing their information to the mobile health app developer.[70]

Another important aspect to consider is that user information is considered an asset to these mobile app companies, having rightful ownership of the user's data.[71] Along with that, they may choose to buy or sell their users' information, and if their company goes bankrupt or is acquired, then said data from users will be transferred or acquired by the third party.[72]

This is similar to the court rulings in *Moore* and *Greenberg*, where once tissues or cells have left a person's body, they no longer have any legal rights to them. Here, instead of tissues and cells, business and mobile app companies might argue that once the data has been collected, the user will lose control and ownership of their data. Further, the mobile app companies and third parties will argue, like in *Moore*, that they are no longer legally accountable to the users and do not need to share any realized monetary profits. However, consumers might argue that their case is more similar to *Greenberg* where users are essentially donating their data, and the business and mobile app companies are earning money from their donation, thus creating

---

Pub. Law & Legal Theory Research Paper Series, Working Paper No.12-56, 2012).

66. *Id.* at 1.

67. Jah-Juin Ho, Keynote Address at the Federal Trade Commission Spring Privacy Series: Consumer Generated Controlled Health Data (May 7, 2014) (transcript available on the Federal Trade Commission website).

68. Daniel Parisi, *Mobile App Privacy: Developing Standard and Effective Privacy Tools for Consumers*, 15 N.C.J.L. & TECH. ON. 240, 244 (2014).

69. *Privacy Policy*, *supra* note 3.

70. *See Privacy and Terms*, MYFITNESSPAL, https://account.underarmour.com/privacy?locale=en_US (last visited Mar.6, 2017).

71. *See id.*

72. *See id.*

"unjust enrichment."[73] The growing and valuable data collected today makes it difficult to predict how it will be used in the future.

## IV. ANONYMIZED DATA UNDER HIPAA AND HEALTH MOBILE APPS

HIPAA provides strict guidelines on the sharing and transmission of PHI and by law this information must be encrypted and transmitted only through secured means. Any disclosure of PHI from covered entities or business associates will likely result in heavy penalties in civil and criminal court. However, for the purpose of research for publication in health and medicine, PHI can be anonymized or de-identified so that the data is no longer considered protected under HIPAA. The data can be released without any harm if the data removes all sixteen HIPAA identifiers including:

> (i) Names; (ii) Postal address information, other than town or city, State, and zip code; (iii) Telephone numbers; (iv) Fax numbers; (v) Electronic mail addresses; (vi) Social security numbers; (vii) Medical record numbers; (viii) Health plan beneficiary numbers; (ix) Account numbers; (x) Certificate/license numbers; (xi) Vehicle identifiers and serial numbers, including license plate numbers; (xii) Device identifiers and serial numbers; (xiii) Web Universal Resource Locators (URLs); (xiv) Internet Protocol (IP) address numbers; (xv) Biometric identifiers, including finger and voice prints; and (xvi) Full face photographic images and any comparable images.[74]

HIPAA rarely extends to individuals who use fitness and health mobile apps because consumers of mobile apps are deemed to be outside of the healthcare setting and are not considered covered entities.[75] Although many health and fitness apps fall outside of a healthcare setting, the app could potentially be required to be HIPAA compliant if covered entities or business associates like healthcare providers become involved. However, it can be argued that to the extent to which users are tracked and connected to their devices, the information entered or collected through their smartphones could be easily linked to their identification, thus qualifying as PHI. Therefore, any breaches of PHI to other parties from fitness and health mobile apps may hold them accountable and possibly subject them to civil and criminal penalties. However, because many fitness and health apps fall outside HIPAA, the use of these apps remains risky to consumers because of the lack of security and privacy protection for their personal information.[76]

If fitness and health mobile apps fell under HIPAA, then mobile app companies might argue that the data being collected from users is

---

73. *Greenberg*, 264 F. Supp. 2d at 1072.

74. 45 C.F.R. § 164.514(e)(2) (2013).

75. Jamie Lynn Flaherty, *Digital Diagnosis: Privacy and the Regulation of Mobile Phone Health Applications*, 40 AM. J.L. & MED. 416, 426 (2014).

76. *Id.*

anonymized or de-identified. They may further claim that many apps generally anonymize data collected, by removing all of the required HIPAA identifiers, and that the data will no longer be subject to HIPAA restrictions and subsequently can be released and shared without harm.

Conversely, users might argue that anonymized data can easily be re-identified and reversed engineered to reconnect an individual to his or her data.[77] Massachusetts Institute of Technology scientist Yves-Alexandre de Montjoye argues that anonymity doesn't ensure privacy, which could render toothless many of the world's laws and regulations around consumer privacy.[78] Many mobile apps depend on anonymity in exchange to freely collect data, but the danger happens if the anonymity can be hacked.[79]

For example, on September 17, 2014, Uber, a popular mobile app that allows users with smartphones to request rides from drivers who use their own car, was hacked by a third party.[80] It was determined that initially the names and driver's license numbers of approximately fifty thousand (50,000) drivers across multiple states were accessed, but not includes an additional sixty thousand (60,000) drivers.[81] Names of workers, driver's license numbers, and types of vehicles are not public information, but if hackers are able to obtain this information, then it is possible to gain access to fitness and mobile app data as well. The risks include exposing individuals' personal information and using it against them because the transfer of data will compromise what should be confidential.[82]

## V. INSUFFICIENT ENCRYPTION OR SECURED NETWORK CONNECTIONS

Smartphones are designed with tools that easily allow hackers to spy on users, such as, internal microphones, cameras, and geolocation maps.[83] Hackers can use a compromised phone as a hidden camera to secretly record video, turn on the microphone to eavesdrop or make audio recordings, and track movements via geo-location.[84] A report by the Information Technology Laboratory at the National Institute of

77. Scott Berinato, *There's No Such Thing as Anonymous Data*, HARVARD BUSINESS REVIEW (Feb. 9, 2015), https://hbr.org/2015/02/theres-no-such-thing-as-anonymous-data.

78. *Id.*

79. *Id.*

80. Katherine Tassi, *Uber Statement Update*, UBER NEWSROOM (Jun. 7, 2016), https://newsroom.uber.com/statement-update/.

81. *Id.*

82. Peter Segrist, *How the Rise of Big Data and Predictive Analytics Are Changing the Attorney's Duty of Competence*, 16 N.C. J. L. & TECH. 527, 574 (2015).

83. Darlene Storm, *Mobile RAT Attack Makes Android the Ultimate Spy Tool*, COMPUTERWORLD (Mar. 1, 2012, 11:50 PM), http://www.computerworld.com/article/2472441/cybercrime-hacking/mobile-rat-attack-makes-android-the-ultimate-spy-tool.html.

84. *Id.*

Standards and Technology found that "[b]uilt-in security mechanisms often go unused or can be overcome or circumvented without difficulty by a knowledgeable party to gain control over the device."[85] Moreover, as devices become more functional, they often become less secure and easier to access by hackers.[86] Georgia Weidman, Chief Executive Office of Bulb Security, an information security consulting firm states, "[e]very app you install on your mobile device could lead to compromise, every text message you receive, [e]very website you browse using your own device's mobile browser is possibly suspect."[87] These vulnerabilities increase the risk of compromised health and fitness data, which is thought by many to be safely housed on devices, falling into the hands of unintended parties.

Furthermore, smartphones and mobile apps pose a tremendous cybersecurity challenge. Although many mobile app companies claim to uphold their privacy policies and terms of use, to protect the privacy and confidentiality of its users' information, more often than not, they transmit data unencrypted over unsecure network connections—HTTP, rather than HTTPS.[88] This reality is troubling because fitness and health mobile apps may also transmit information that includes an individual's disease or user's search history records.[89] For example, if a user searches for sexually transmitted diseases or anti-psychotic drugs, this information might be viewable to a hacker and can be used to expose any user's identity along with his or her online browsing history.[90]

It is important to note, that the mobile app industry is largely unregulated. This is of particular concern with health and fitness apps, which often collect user's basic information such as name, height, geolocation, dietary, fitness, sleep patterns, etc.[91] None of this data is covered by current regulations that protect the privacy and security of personal health information; it only has the protection under the developer's privacy policy, if there is a privacy policy at all.[92]

Additionally, many health and fitness apps encourage users to share sensitive information via social media, often using the social

85. WAYNE JANSEN & TIMOTHY GRANCE, NAT'L INST. OF STANDARDS AND TECH. SPECIAL PUBLICATION 800-144: GUIDELINES ON SECURITY AND PRIVACY IN PUBLIC CLOUD COMPUTING viii (2011), http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-144.pdf.

86. *Id.*

87. David Goldman, *BlackBerry's wipeout creates major mobile security gaps*, CNN (Sep. 26, 2012, 7:25 AM), http://money.cnn.com/2012/09/26/technology/mobile-security-byod/.

88. *Webinar: Mobile Health and Fitness Apps: What Are the Privacy Risks?*, PRIVACY RIGHTS CLEARINGHOUSE (June 19, 2013), https://www.privacyrights.org/mobile-health-and-fitness-apps-what-are-privacy-risks.

89. *Id.*

90. *Id.*

91. *See* Jamie Lynn Flaherty, *Digital Diagnosis: Privacy and the Regulation of Mobile Phone Health Applications*, 40 AM. J.L. & MED. 416, 429 (2014).

92. *See id.*

aspect as a selling point for collaboration and positive feedback.[93] Once information is in the public domain, the user has little to no control over it, practically and legally.[94] Thus, the argument that the developer, who created an application to provide a service for the user to publicize his or her health data, should not be allowed to capitalize on data now in the public space, appears to be misguided at best and hypocritical at worst.

## VI. DANGERS INVOLVED WITH USER DATA TRANSFERS TO THIRD PARTIES

### A. USING PRIMARY DATA SETS AND REPURPOSING USERS' DATA FOR SECONDARY MARKETS

Fitness and mobile apps are not only created for direct wellness or medical purposes, but are also repurposed for new markets. In 2013, medical and fitness mobile apps accounted for at least forty thousand (40,000) apps, with the health app market worth an estimated seven hundred eighteen million dollars ($718M).[95] By 2018, the market for health apps and solutions is anticipated to reach over an astonishing twenty billion dollars ($20.7B).[96] Fitness and health mobile apps' behavioral data is highly valuable for primary and secondary data markets. For instance, Datalogix, a data collection company, can correlate users' interests in certain health conditions based on their search history and items purchased online, classifying users as "allergy sufferers" or "dieters."[97] Another data collection company, Acxiom, sells user data on whether an individual has a "propensity" for a certain "ailment or prescription."[98] Data analysts use correlations to predict which users are likely to contract certain diseases, so that they can counsel individuals on how to avoid these illnesses.[99] These companies "use Big Data to discern which medical treatments are likely to work for which types of people to provide better medical care."[100] An

93. *See The Developing Role of Social Media in the Modern Business World*, FORBES (Aug. 8, 2012), http://www.forbes.com/sites/moneywisewomen/2012/08/08/the-developing-role-of-social-media-in-the-modern-business-world/#1a0aca834189.

94. Storm, *supra* note 83.

95. Jenny Gold, *FDA Face Daunting Task as Health Apps Multiply*, EARL'S VIEW (Jun. 8, 2012), https://earlsview.com/2012/07/08/fda-faces-daunting-task-as-health-apps-multiply-sci-tech-today/.

96. *Mobile Health Apps and Solutions Market Worth $20.7 Billion by 2018*, ELECTRONIC HEALTH REPORTER (Dec. 11, 2013), http://electronichealthreporter.com/hit-news/mobile-health-apps-and-solutions-market-worth-20-7-billion-by-2018/.

97. Lois Beckett, *Everything We Know About What Data Brokers Know About You*, PROPUBLICA (June 13, 2014, 12:59 PM), https://www.propublica.org/article/everything-we-know-about-what-data-brokers-know-about-you.

98. *Audience Propensities*, ACXIOM, http://www.acxiom.com/audience-propensities/ (last visited Mar. 6, 2017).

99. Dennis D. Hirsch, *That's Unfair! Or Is It? Big Data, Discrimination and the FTC's Unfairness Authority*, 103 KY. L.J. 345, 349–53 (2015).

100. *Id.*

advantage of Big Data is that it can help prevent certain diseases before they actually occur, but more germane to this discussion, is that it targets potential patients on the basis of their digital fingerprints, making their identification invaluable to potential marketers.

B. TURNING REPURPOSED DATA INTO "TARGETED ADVERTISEMENTS"

Although Big Data can be helpful in improving the quality of patient care, the risks come when classifying individuals in order to make predictions about their future behavior. Target Brands Inc.'s controversial use of Big Data illustrate this point.[101] Target, the well-known big-box retailer has practiced advanced statistical prediction models using prior purchasing habits to identify those who have recently had a child to mail "targeted advertisements" and coupons to them.[102] Targeted advertisements can be defined as proposed ads that "highlight the increasingly sophisticated ways that Internet companies track users' online and offline activities for marketing purposes," and then send consumers sales and promotions by email or mailing addresses.[103] Several years later, Target shifted focus to potential new mothers by marketing baby goods to them by using such Big Data to determine when a particular woman was pregnant.[104]

Over the years, Target had accumulated a massive amount of data detailing customer purchases.[105] By correlating customers' prior purchases with in-store baby shower registries, the company was able to identify items that pregnant customers regularly purchased, like unscented body lotion, calcium supplements, and hand sanitizers.[106] Target would then apply this profile to their current customer database and compare it to women who made similar purchases.[107] If a woman purchased several of these items from this list of predictive products then those customers were assigned a high "pregnancy prediction score" and received baby-related advertisements and coupons, thereby maximizing the targeting power of the advertisements to those most likely to find them appealing.[108]

After several months of direct marketing to potentially pregnant women, a father entered a Target store and demanded answers to why the company was sending his high school daughter baby-related

101. *See* Charles Duhigg, *How Companies Learn Your Secrets*, N.Y. TIMES MAG. (Feb. 16, 2012), http://nyti.ms/18LN5uz.

102. *Id.*

103. Rolfe Winkler and Jack, *Google May Offer New Way to Target Ads*, WALL ST J: TECH. (Apr. 14, 2015, 5:01 PM), http://www.wsj.com/articles/google-may-offer-new-way-to-target-ads-1429044389.

104. *See* Charles Duhigg, *How Companies Learn Your Secrets*, N.Y. TIMES MAG. (Feb. 16, 2012), http://nyti.ms/18LN5uz.

105. *Id.*

106. *Id.*

107. *Id.*

108. *Id.*

coupons.[109] A store manager later called the father to apologize for the advertisements, but later it was revealed that the daughter was actually pregnant.[110] Target, by using Big Data and population-based trends, was able to identify a pregnant teenager before her own father.[111]

This example helps to demonstrate two harms created by Big Data predictive analysis. First, Target's mailings potentially revealed the daughter's pregnancy to her father without her consent. She was not prepared at the time to disclose this information, an obvious injury to her privacy. The second issue can be explained through a hypothetical. Assume that instead of using the data to figure out who was pregnant that Target elected to use that information to deny job interviews to pregnant females, who attained a high "pregnancy prediction score," for fear of having an unstable workforce prone to maternity leave and disrupted productivity. Many would argue that such actions from a company are harmful and illegal. This kind of practice would constitute a form of discrimination of a protected class, preferring men or certain women in the workforce. Similarly, what if a company refused to give someone a loan, based on health information gathered on those most likely to have a heart attack and highly correlated with a particular racial group? This loan refusal might cause disparate impact and racial discrimination against a protected class of people.

### C. DENYING INDIVIDUALS LIFE OPPORTUNITIES BASED ON BIG DATA TRENDS

Big Data predictive analysis poses not so hypothetical scenarios in which an insurance company may be able to deny coverage to people identified as most likely to suffer a heart attack, something already done through actuary and risk-assessment analysis. But what if insurance companies were supplied with patient-level data collected and transmitted without expressed consent? "Several large insurance firms have been testing whether they can use data from a wide variety of online and offline sources to predict which insurance applicants are most likely to suffer from high blood pressure, depression, or diabetes to identify high-risk i.e. costly applicants."[112] Viktor Mayer-Schönberger, a professor of Internet governance and regulation at the Oxford Internet Institute at Oxford University, and Kenneth Cukier, data editor for *The Economist*, explain that with the increase of predictive ability, "the danger to us as individuals shifts from privacy to probability: algorithms will predict the likelihood that one will get a heart attack (and pay more for health insurance), default on a mortgage (and be denied a loan), or commit a crime (or perhaps get

109. *Id.*
110. *Id.*
111. *Id.*
112. Hirsch *supra* note 99, at 351.

arrested in advance)."[113]

Clearly, withholding jobs, loans, insurance, housing, or other life opportunities could impose a significant cost on those deprived, but it might not be considered illegal because those individuals, who were denied, are not members of a protected class.[114] Additionally, it seems unreasonable to refuse access to individuals, who may never experience a heart attack or even take steps to prevent such a health condition. A business could argue that this type of practice is efficient and produces benefits.[115] Assuming that data analysts can help businesses identify those individuals who are more likely to suffer a heart attack, and that these individuals have a greater risk of performing poorly as "employees, borrowers, tenants, and life insurance customers," then companies can avoid certain individuals, who may be considered risky.[116]

### D. USING BIG DATA TRENDS TO PRICE DISCRIMINATE

Additionally, many companies are using differential pricing models to target specific individuals because they fit into a particular trend in their buying and spending habits.[117] Price discrimination, defined in the broadest sense, is "to denote the various methods of offering essentially the same product for different prices to different people."[118] For example, if health and medical data has been collected by a user indicating that he or she suffers from a chronic disease, then third parties collecting that data may charge more for particular items that individual needs to treat his or her illness.[119] If this individual decides to purchase an item on Amazon, a popular online retailer, to treat his or her illness, such as an over-the-counter medication, then there could be a price increase.[120] In another example, if the individual, who is interested in learning more about his or her own illness and wants to purchase a book, then Amazon might increase the price for that specific item.[121] This type of price discrimination is the type of abuse individuals might suffer if fitness and health mobile apps

---

113. VIKTOR MAYER-SCHÖNBERGER & KENNETH CUKIER, BIG DATA: A REVOLUTION THAT WILL TRANSFORM HOW WE LIVE, WORK, AND THINK 17 (John Murray Publishers, 2013).

114. Dennis D. Hirsch, *That's Unfair! Or Is It? Big Data, Discrimination and the FTC's Unfairness Authority*, 103 KY. L.J. 345, 352 (2015).

115. *Id.*

116. *Id.*

117. Akiva A. Miller, *What Do We Worry About When We Worry About Price Discrimination? The Law and Ethics of Using Personal Information for Pricing*, 19 J. TECH. L. & POL'Y 41, 49 (2014).

118. *Id.* at 43.

119. Peter Segrist, *How the Rise of Big Data and Predictive Analytics Are Changing the Attorney's Duty of Competence*, 16 N.C. J. L. & TECH. 527, 535 (2015).

120. *See* Jeremy Singer-Vine, Ashkan Soltani, & Jennifer Valentino-Devries, *Websites Vary Prices, Deals Based on Users' Information*, WALL ST. J (Dec. 24, 2012), http://www.wsj.com/articles/SB10001424127887323777204578189391813881534.

121. *See* Miller, *supra* note 117, at 48.

continue to share and sell user data to third parties.[122]

The danger lies in the disclosure of individuals' health data that is then used for discriminatory purposes, different pricing models or insurance rates, or targeted advertisements. HIPAA was designed to limit the secondary uses of health data with different types of prohibitions, authorizations, and consent requirements from patients. Big Data, especially in the mobile app industry, includes clinical and other related data that is currently not being regulated. Further, Viktor Mayer-Schönberger and Kenneth Cukier stated that "the [privacy] problem has been transformed. With Big Data, the value of information no longer resides solely in its primary purpose, it is now in secondary uses."[123] Thus, many users may be legally discriminated against, targeted for advertisements, and even denied life insurance based on statistical analyses of Big Data trends.

## VII. RECOMMENDATIONS

Rapid technology advancements could lead to similar levels of abuse of users' private information like the kind that Henrietta Lacks and John Moore experienced. We should learn from the cases that lead to the enactment of HIPAA and apply them to current circumstances. For the purposes of this paper, there will be three suggestions on improving privacy protections for users: (1) broaden HIPAA, (2) restrict the sale of user data by requiring a notice requirement for users, or (3) change the ownership of data and provide upfront transactions so that users can be compensated for sharing their data. With these recommendations, fitness and health mobile app companies would have a greater responsibility and duty to protect user data. With clearly-defined responsibilities, mobile app companies can better understand the legal obligations owed to its users. Likewise, potential mobile app users will be able to rely on the consistent expectation and enforcement of those regulations.

### A. BROADEN HIPAA PRIVACY PROTECTION

The federal government should consider broadening HIPAA to include fitness and health apps to their privacy protections. App developers might argue that forcing fitness and mobile apps to be HIPAA compliant is too strict because of the possible civil and criminal penalties for data breaches. App development is often carried out by small and innovative startup companies incapable of meeting more strict legal liabilities, perhaps bankrupting an up-and-coming company as a result of compromised data.[124] They may further argue that being

122. *See* Miller *supra* note 117, at 48.

123. MAYER-SCHÖNBERGER & CUKIER *supra* note 113, at 153.

124. *See* Mark Sullivan, *Health apps could be heading into a HIPAA showdown*, VENTUREBEAT (June 13, 2014, 9:56 AM), http://venturebeat.com/2014/06/13/health-apps-could-

restricted by HIPAA might limit medical and technology advances by preventing companies from collecting, sharing, and selling data to other third parties.

By expanding HIPAA to include fitness and mobile app companies, it will protect users' privacy to the same extent that patients' PHI is handled at healthcare facilities. Fitness and health mobile app companies will be held accountable for breaches of confidential personal information to unintended third parties.[125] It will ensure that any violation of users' information will have legal consequences in civil and criminal proceedings. Furthermore, this redressability will give users a chance to live a life with less fear of discrimination, modified pricing models, targeted advertisements, employment, housing options, and life insurance and loan denial. Therefore, the protection of HIPAA will outweigh the benefits of advancing medicine because it will prevent data analysts, businesses, and companies from discriminating against users based on Big Data trends.

B. RESTRICT THE SALE OF USER DATA INFORMATION BY GIVING USERS NOTICE

If extending HIPAA to include fitness and health apps is too strict because of the perceived harms from potential violations and penalties, then there should be a policy that provides users with more control over their data that is collected and stored on mobile apps.[126] Fitness and health mobile app companies can change the terms of use and privacy policies, giving users notice of when data is being shared or sold and to whom. Users should be alerted if their data is being sold to a particular type of third party vendor, such as a pharmaceutical company, advertising company, or insurance company. Fitness and health mobile apps should allow users to select the kind of information the user is willing to share or sell, such as name, geographic location, sleeping patterns, exercise, and diet. Additionally, users should be notified if the app sells or shares information that extends to their friends and family members based on their mobile contact lists.

Researchers and mobile app developers should provide notice to users and require explicit consent to collect, store, or use their data.[127] Users must be made aware that data, being collected from mobile apps, is a contribution of the user's own freewill to mobile app companies. Users relinquish all rights and will no longer have future control, even

---

be-heading-into-a-hipaa-showdown/.

125. *Id.*

126. *See generally* Amadou Diallo, *Do Smart Devices Need Regulation? FTC Examines Internet Of Things*, FORBES: TECH (Nov. 23, 2013, 9:01 AM), http://www.forbes.com/sites/amadoudiallo/2013/11/23/ftc-regulation-internet-of-things/#ec6f29e14e5f.

127. *See generally* Adam D. Thierer, *The Internet of Things and Wearable Technology: Addressing Privacy and Security Concerns Without Derailing Innovation*, 21 RICH. J.L. & TECH. 1, 67 (2015).

if they decide to stop participating. A fitness and mobile app company must be explicit in its explanation to consumers about its legal rights to collect, share, and not anonymize user data. Mobile app users should be made aware of the possibilities of commercialization and restrictive patents that may ultimately result in monetary profits. The importance of consent should not be underestimated. A careful review of the terms of use and privacy policy with the mobile app user might prevent legal issues and negative press for researchers and fitness and health mobile app companies.

### C. CHANGE DATA OWNERSHIP TO THE USER AND PROVIDE UPFRONT TRANSACTIONS

Currently, fitness and health mobile apps have the right to share, transmit, and sell user data. By having this arrangement, it takes away the legal right of ownership from the user and gives it to mobile app companies.[128] However, this can quickly devolve into a repeat of the Henrietta Lacks and John Moore situations, where physicians and researchers in the past essentially use the protected health information without permission. To avoid this possible scenario from occurring, mobile app companies can implement an upfront transaction for the sale of their data and information to third parties.

Additionally, there have been several companies that have been direct with their intention to collect, share, and sell user data information. For instance, Nielsen, a mobile app company, collects data from users' smartphones and pays users up to fifty dollars ($50) in rewards for keeping the app.[129] Another mobile app, Smart Panel, pays users if they download their app and keep it on their smartphone every month.[130] Users can potentially earn up to seventy-five dollars ($75) in the first year.[131] Individuals who sign-up will receive some form of monetary reward for their contribution. These mobile apps have made it acceptable to sell user data because they are upfront about their intentions of repurposing users' information to share, trade, and sell to third parties.

## CONCLUSION

With the enactment of HIPAA, cases such as Henrietta Lacks and John Moore, are more heavily scrutinized for their insufficient health privacy protections to individuals and the harm in sharing confidential health information. HIPAA decreased the amount of abuse from the medical and health research community conducting medical

128. Barbara J. Evans, *Much Ado About Data Ownership*, 25 HARV. J. L. & TECH. 69, 89 (2011).

129. *Smartphone Study: FAQs & Contacts*, NIELSEN, https://mobilepanel.nielsen.com/enroll/help.do?l=en_us&pid=1 (last visited Mar. 6, 2017).

130. SMART PANEL, https://smartpanel.io (last visited Mar. 6, 2017).

131. *Id.*

experiments. In addition, those who violate HIPAA and breach PHI regulations are heavily penalized in civil and criminal courts.

Similarly, health and fitness apps that work with covered entities or handling PHI must be HIPAA compliant. Although most health and fitness mobile apps are able to bypass this compliance, these companies remain a huge risk to users because of the ability to access personal information through users' devices. This ability results in a large amount of data collection without the protection of privacy health laws, such as HIPAA. It is important to protect users' confidential information from third parties, who may exploit users' behavioral data, so that only mobile app companies can profit from Big Data trends. Fitness and health mobile apps should be restricted in the data they share by expanding HIPAA, be obligated to provide notice of data distribution or any change in the ownership status of consumers' data, be direct about users' legal rights and receive explicit consent to use the data collected.

Unwanted discrimination and the propensity to make false population-based predictions on an individual's health habits may become prevalent without a change in privacy policies and terms of use. As a result of repurposed data, certain individuals might be denied access to employment, housing, loans, and life insurance. Without the appropriate regulations to protect users' privacy and confidential information, it may be possible to see similar levels of privacy exploitations in the fitness and health mobile app industry as in the past.