NOTE

Profiting on Your Pulse: Modernizing HIPAA to Regulate Companies' Use of Patient-Consumer Health Information

*Anna Mizzi**

ABSTRACT

Technology knows the most intimate details of our lives: our exercise and eating habits, our ability to conceive children, even how often we dream or have sex. Companies like the fitness wearable giant FitBit, the meditation and anxiety support app Headspace, and the widely used period and ovulation predictive company Flo Health, Inc., have built their businesses on the interaction between the consumer's raw health data and the company's data analysis.[1] The increasing prevalence of consumer health interactive analysis companies ("CHIACs") and the consumerization of health care have, however, far outpaced existing patient-consumer protection laws.[2] This lack of regulation creates an environment where individuals have little control over their own health data. CHIACs frequently buy and sell sensitive health data with virtually no patient-consumer consent or notification.[3] Intensely private

* J.D. 2020, The George Washington University Law School. Deepest thanks to Professor Jessica Arco and Dean Emily Hammond for their continued support and insight.

1 *See, e.g.*, FITBIT, https://www.fitbit.com/ [https://perma.cc/F587-GY9C]; FLO HEALTH, https://flo.health [https://perma.cc/9333-PSRZ]; *Meditation for Anxiety*, HEADSPACE, https://www.headspace.com/how-it-works [https://perma.cc/UR9R-AWZ3].

2 *See* AM BAR ASS'N HEALTH LAW SECTION, WHAT IS . . . MHEALTH? 1, 2 (Covington & Burling LLP ed., 2017).

3 *See, e.g.*, FTC, SELF-REGULATORY PRINCIPLES FOR ONLINE BEHAVIORAL ADVERTISING i, ii (2009), https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commis-

information is now easily discoverable by anyone with access to the internet—including employers,[4] *credit score or insurance companies,*[5] *and even criminals.*[6] *This Note argues that the best way to fill this regulatory gap is to bring CHIACs into the existing interpretation of "covered entities" under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA").*[7]

TABLE OF CONTENTS

---

sion-staff-report-self-regulatory-principles-online-behavioral-advertising/p085400behavadreport.pdf [https://perma.cc/H2TE-85HA]; JANE SARASOHN-KAHN, CAL. HEALTHCARE FOUND., HERE'S LOOKING AT YOU: HOW PERSONAL HEALTH INFORMATION IS BEING TRACKED AND USED 8–9 (2014), https://www.chcf.org/wp-content/uploads/2017/12/PDF-HeresLookingPersonalHealthInfo.pdf [https://perma.cc/97NT-BZUD].

4 *See, e.g.*, Julie Appleby, *Workplace Wellness Plans Offer Big Incentives, But May Cost Your Privacy*, NPR (Sept. 22, 2018 7:02 AM), https://www.npr.org/sections/health-shots/2018/09/22/649664555/workplace-wellness-plans-offer-big-incentives-but-may-cost-your-privacy [https://perma.cc/LZH5-FXUG].

5 *See, e.g.*, Marshall Allen, *Health Insurers Are Vacuuming up Details About You—and It Could Raise Your Rates*, PROPUBLICA (July 17, 2018, 5:00 AM), https://www.propublica.org/article/health-insurers-are-vacuuming-up-details-about-you-and-it-could-raise-your-rates [https://perma.cc/VKC5-FDYW]; *FICO Medication Adherence Score*, FICO (2017), https://www.fico.com/en/resource-download-file/3317 [https://perma.cc/EN55-WNDC]; *see also* PAM DIXON & ROBERT GELLMAN, WORLD PRIVACY FORUM, THE SCORING OF AMERICA: HOW SECRET CONSUMER SCORES THREATEN YOUR PRIVACY AND YOUR FUTURE (2014), http://www.worldprivacyforum.org/wp-content/uploads/2014/04/WPF_Scoring_of_America_April2014_fs.pdf [https://perma.cc/XMV7-ARN8].

6 *See, e.g.*, Stanley C. Ball, *Ohio's "Aggressive" Attack on Medical Identity Theft*, 24 J.L. & HEALTH 111, 112 (2011); *Domestic Violence and Privacy*, ELECTRONIC PRIVACY INFO. CTR., https://www.epic.org/privacy/dv/ [https://perma.cc/QVS3-SQZH].

7 45 C.F.R. § 160.103 (2017).

INTRODUCTION

Until Spring 2018, every time users engaged with Standard Innovation's newest smart product, the company quietly collected those users' data, transmitted it to company servers, and then analyzed it without users' knowledge or consent.[8] Following recent scandals surrounding Facebook and other big tech companies,[9] Standard Innovation's actions alone may not have surprised most consumers.

But Standard Innovation did not collect data on ad clicks or cat photo "likes." Standard Innovation manufactures a smart vibrator called We-Vibe.[10] The company invited its users to download a corresponding mobile app that controlled the device and allowed users to invite their intimate partners to control the device remotely.[11] By looking at who used the mobile app, when they used it, and what devices were connected to it, Standard Innovation could determine users' locations, how often they used the device, and how many intimate partners they had.[12] When the device was used with the app, the app would transmit up-to-the-minute data on the device's settings—even its temperature.[13] Last year, Standard Innovation faced a lawsuit for collecting and tracking this intimate data without consumer notification or consent.[14] While the lawsuit settled for close to four million

8 Camila Domonoske, *Vibrator Maker to Pay Millions over Claims It Secretly Tracked Use*, NPR (Mar. 14, 2017 1:52 PM), https://www.npr.org/sections/thetwo-way/2017/03/14/520123490/vibrator-maker-to-pay-millions-over-claims-it-secretly-tracked-use [https://perma.cc/R7QC-K8X2].

9 *See, e.g.*, Emily Stewart, *Facebook's Very Bad Year, Explained*, VOX (Dec. 21, 2018, 11:20 AM), https://www.vox.com/technology/2018/12/21/18149099/delete-facebook-scandals-2018-cambridge-analytica [https://perma.cc/LJD2-2XTY].

10 Domonoske, *supra* note 8.

11 *Id.*

12 *See id.*

13 Alex Hern, *Vibrator Maker Ordered to Pay out C$4m for Tracking Users' Sexual Activity*, GUARDIAN (Mar. 14, 2017, 6:08 PM), https://www.theguardian.com/technology/2017/mar/14/we-vibe-vibrator-tracking-users-sexual-habits [https://perma.cc/DAQ6-LULW].

14 Domonoske, *supra* note 8.

dollars and the company agreed to change its data policies, Standard Innovation maintained that they had done nothing wrong.[15]

Standard Innovation faced no consequences from the administrative agencies usually charged with protecting patient-consumers and their personal, health-related information. The device is not regulated by the Food and Drug Administration ("FDA"),[16] and the Federal Trade Commission ("FTC") never opened an investigation.[17] While HIPAA certainly extends to sexual health, Standard Innovation is not considered a "covered entity" under the law, meaning it is not required to protect user data in compliance with HIPAA.[18]

As other countries expand protection for *all* consumer data, regulations for health-related data in the United States remain insufficient.[19] One reason for this is that laws like HIPAA regulate *companies or channels* through which data travels, not data itself.[20] However, as the use of Mobile Health Technologies ("mHealth"),[21] has rapidly expanded, these channels of data have also continued to evolve. Consequently, the U.S. Department of Health and Human Services ("HHS"), which administers HIPAA, has struggled with how to regulate these new players in the health field.[22]

---

15 *Id.*

16 *See* AM. BAR ASS'N HEALTH LAW SECTION, *supra* note 2, at 4–6, 15–16 (discussing the FDA's broad policy of not regulating "general wellness products," as they pose a "low-risk").

17 *See* Federal Trade Commission, Comment Letter on Developing the Administration's Approach to Consumer Privacy (Nov. 9, 2018), at 2, https://www.ftc.gov/system/files/documents/advocacy_documents/ftc-staff-comment-ntia-developing-administrations-approach-consumer-privacy/p195400_ftc_comment_to_ntia_112018.pdf [https://perma.cc/EY36-JU77] [hereinafter FTC Comment Letter].

18 *See* 45 C.F.R § 160.103 (2017) (defining "covered entity" as a "health plan," "health clearinghouse," or covered "health care provider." Though they make a sexual health device, Standard Innovation is not considered a covered "health care provider").

19 *See, e.g.*, Regulation 2016/679 of the European Parliament and of the Council of 27 Apr. 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), art. 4(1), 2016 O.J. (L 119) 1, 33 (EU), http://data.europa.eu/eli/reg/2016/679/oj/eng [https://perma.cc/44G4-6WGU] [hereinafter GDPR] (the European Union's data privacy protections); *PIPEDA in Brief*, OFF. OF THE PRIVACY COMM'R OF CAN., https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda_brief/#_what_is [https://perma.cc/7TM8-9EKW].

20 *Compare* GDPR, art. 4(1), *and PIPEDA in Brief*, *supra* note 19, *with* 45 C.F.R. § 160.103 (HIPAA's definitions of the entities which it regulates), *and* 15 U.S.C. § 45 (2012) (FTC's authority to regulate companies' unfair or deceptive practices).

21 *See* AM. BAR ASS'N HEALTH LAW SECTION, *supra* note 2, at 1.

22 *See* HHS, EXAMINING OVERSIGHT OF THE PRIVACY & SECURITY OF HEALTH DATA COLLECTED BY ENTITIES NOT REGULATED BY HIPAA 8 (2016).

Without regulatory protection, patient-consumers are vulnerable to having their data used or disclosed without authorization, such as through a data breach or unauthorized sale.[23] This Note argues that HHS can and should include CHIACs in HIPAA's definition of "covered entities" to better protect sensitive patient-consumer data from unauthorized use or disclosure.

This Note will proceed in five parts. Part I will explore the expansion of mobile health technologies and the risks associated with failing to protect these data channels on a federal level. Part II will analyze the shortcomings of existing regulatory frameworks for these data channels, including under HIPAA and the FTC. Part III will focus on the particular advantages of regulating CHIACs under HIPAA. Part IV will argue that HIPAA gives HHS the statutory authority to regulate CHIACs. Finally, Part V will address challenges to this proposed reinterpretation of HIPAA and explain why reinterpreting HIPAA is the most effective way of providing crucial data protection to patient-consumers.[24]

I. BACKGROUND

A. Expansion of the mHealth Market & the CHIAC Business Model

mHealth encompasses a broad range of "medical and public health practices supported through mobile communication devices, such as smartphones, personal digital tablets, patient monitoring devices, wearable technology, and other wireless devices."[25] mHealth use over the past several years has expanded dramatically.[26] In 2014,

---

23 *See id.* at 8–9; SARASOHN-KAHN, *supra* note 3, at 5, 8–9.

24 Beyond the scope of this Note are the policy implications of expanding HIPAA to include CHIACs. Expanding HIPAA protections could drive up the cost of certain CHIAC products; these companies often provide "free" products in exchange for the opportunity to sell the data that consumers generate on their products. *See The New Merchants of Data: Creating a More Equitable Exchange of Data Between Digital Businesses and Their Customers*, HARV. BUS. REV. (Nov. 17, 2017), https://hbr.org/sponsored/2017/11/the-new-merchants-of-data-creating-a-more-equitable-exchange-of-data-between-digital-businesses-and-their-customers [https://perma.cc/L4UF-ULJG] (exploring Microsoft, the content's paid sponsor's perspective on this "barter" system). It is possible that in response to market pressures—or the reinterpretation of HIPAA proposed in this Note—companies could provide HIPAA-compliant notices that would allow patient-consumers to choose between two levels of service from the CHIAC: a free (or lower cost) version where the company has the right to sell the individual's data, and a paid (or higher cost) version where the patient-consumer pays for the increased privacy and control over their data. This forces an interesting legal question: Would this pay-for-privacy create class inequities that violate the spirit of HIPAA in an actionable way?

25 *See* AM. BAR ASS'N HEALTH LAW SECTION, *supra* note 2, at 1.

26 *See id.* at 1–2.

one-third of U.S. smartphone owners used fitness and health apps.[27] By 2023, the market for smartwatches and fitness trackers is expected to be worth $30 billion[28]—and fitness wearables are not the only kind of mHealth technology. Companies have tried to develop bras to detect breast cancer,[29] smart sensors to detect falls in elderly people's homes,[30] and even smart devices to improve users' sexual health.[31]

One growing player in mHealth is CHIACs—companies whose focus is the creation of consumer-facing health analysis generated primarily by the interaction of a patient-consumer with a device owned by that consumer, such as a wearable device, smart sensor enabled device, or a mobile or desktop app (*i.e.*, those designed for self-therapy, tracking pregnancy, or recording infant health to see overall trends).[32] The interaction between the patient-consumer and the company is the hallmark of the CHIAC business model; consumers purchase devices, the devices send data to the company, and the company returns increasingly accurate analysis and prediction to the consumer in a continuous cycle.[33]

---

27 *Hacking Health: How Consumers Use Smartphones and Wearable Tech to Track Their Health*, NIELSEN (Apr. 16, 2014), http://www.nielsen.com/us/en/insights/news/2014/hacking-health-how-consumers-use-smartphones-and-wearable-tech-to-track-their-health.html [https://perma.cc/3CH4-Z52K].

28 *See, e.g.*, *Forbes Insights: Can a Fitness Tracker Save Your Life?*, FORBES (Oct. 15, 2019), https://www.forbes.com/sites/insights-teradata/2019/10/01/can-a-fitness-tracker-save-your-life/#4e67ab8047a2 [https://perma.cc/SZV5-L64T].

29 *See* Li Zhou, *Could a Bra Actually Detect Breast Cancer?*, SMITHSONIAN MAG. (Mar. 19, 2015), https://www.smithsonianmag.com/innovation/could-a-bra-actually-detect-breast-cancer-180954612/ [https://perma.cc/S4JD-9JCZ].

30 *See* Guilherme Gerzson Torres et al., *An EnOcean Wearable Device with Fall Detection Algorithm Integrated with a Smart Home System*, 51 IFAC PAPERSONLINE 9 (2018).

31 *Pelvic Exerciser with App Kehel*, JOY ON TOYS, https://us.joyontoys.com/en/pelvic-exerciser-with-app-kehel/ [https://perma.cc/3KCT-2YD3] (marketing product as helpful to people with urinary incontinence or preparing for childbirth and as having healthcare professionals on staff to help patient-consumers).

32 Other mHealth mobile applications that simply log information instead of providing some analysis (either predictions or trends) are also beyond the scope of this Note.

33 This definition excludes other types of mHealth like health social media (posting on forums or participating in groups designed to support achieving health goals or managing chronic conditions) and simple online health research (using a search engine or going to general information pages like the Mayo Clinic's website). CHIACs uniquely focus on the cyclical relationship between the patient-consumer and company. CHIACs create specific, detailed profiles of a person's health, similar to what someone might receive in a doctor's office (heart rate, sleeping patterns, details of pregnancy progression, etc.) rather than the comments, questions, and search terms catalogued by health social media and online health research. Including data generated from online health research and health social media in the definition of CHIACs would be well beyond the enforcement capabilities of HIPAA, a statute regulating the health industry, and essentially turn it into to a data regulating statute like Europe's General Data Protection Regulation ("GDPR").

As mHealth use becomes more widespread, an evolving business model for many CHIACs is to buy and sell the data generated by the consumers using their products.[34] This collection and sale of data most often occurs without the user's knowledge. The user engages with an app or device, and the CHIAC sells their user's information either directly to a consumer-facing company (like Facebook) or to a data aggregator (like Acxiom, LexisNexis, Optum, or IBM Watson Health).[35]

The Wall Street Journal reported recently that apps handing over data to Facebook included health-focused apps like Instant Heart Rate, HR Monitor (the most popular heart rate app on Apple's iOS), and Flo Health Inc.'s Flo Period & Ovulation Tracker, a top health app used by 31 million people monthly.[36] Another study of 24 top health mobile apps found that 19 shared user data with companies like Facebook, Google, and Amazon, even though the apps have no connection to those companies, and the apps themselves claim they did not collect personally identifiable health information. The study also reported that the users could be identified easily, through metadata like their unique Android IDs.[37] While these particular mobile apps may not all have fallen under the definition of CHIACs, this cavalier attitude toward what is, in effect, health-related data highlights the growing problem of underregulation.

But CHIACs do not just sell to consumer facing companies, but also to third-party data aggregators.[38] On their own website, data aggregator Acxiom explains the breadth of this data and the power of

---

34 *See* JOHN DEIGHTON ET AL., INTERACTIVE ADVERTISING BUREAU, ECONOMIC VALUE OF THE ADVERTISING-SUPPORTED INTERNET ECOSYSTEM 7 (2017), https://www.iab.com/wp-content/uploads/2017/03/Economic-Value-Study-2017-FINAL2.pdf [https://perma.cc/5A6Q-ZULP] (finding that the ad-supported internet ecosystem, which is driven by consumer data, generated $1.121 trillion for the U.S. economy in 2016); *The Daily: The Business of Selling Your Location*, N.Y. TIMES (Dec. 10, 2018) https://www.nytimes.com/2018/12/10/podcasts/the-daily/location-tracking-apps-privacy.html [https://perma.cc/6LBH-KV2U] (exploring the rise of data aggregation, surveillance, and location data).

35 Sam Schechner & Mark Secada, *You Give Apps Sensitive Personal Information. Then They Tell Facebook*, WALL STREET J. (Feb. 22, 2019, 11:07 AM), https://www.wsj.com/articles/you-give-apps-sensitive-personal-information-then-they-tell-facebook-11550851636 [https://perma.cc/G8CS-4R2K].

36 *Id.*; FLO HEALTH, *supra* note 1.

37 Quinn Grundy et al., *Data Sharing Practices of Medicines Related Apps and the Mobile Ecosystem: Traffic, Content, and Network Analysis*, BMJ ONLINE (2019), http://dx.doi.org/10.1136/bmj.l920 [https://perma.cc/TQH6-8YWK].

38 *See* Allen, *supra* note 5.

this burgeoning industry: "data is being collected, connected, compiled and sold every minute of every day."[39]

Acxiom sells the data it collects across various industries, including the health care industry, and touts its ability to "connect datasets, across channels and silos, for better insight, decision making and performance management."[40] One "Case Study" on its advertising page explains how Acxiom used the data gathered on behalf of a client to identify and target patients who were most likely to respond to solicitation advertising for a new wellness program—all without the patient-consumer ever interacting with Acxiom or the client directly.[41]

Some data aggregators merely resell raw data, while others do their own analysis or re-identify data to create data profiles (bundles of information from various sources about a particular consumer or set of consumers) that they can resell to companies looking to better target particular demographics.[42] One example of a "data profile" is a "consumer score" like FICO's controversial Medication Adherence Score, which is sold to pharmaceutical companies.[43] FICO created this score to predict which patients will take medication according to their doctor's directions.[44] While this may have some helpful applications, FICO has indicated that it will sell the score information to individual health care practices, insurance providers, and other healthcare groups.[45] It is unclear if the insurance companies chose to do anything with this score beyond sending medication reminders—and that uncertainty alone is concerning.[46] As reported by ProPublica in July 2018, "[c]ompanies like LexisNexis say the data shouldn't be used to

---

39 Leah Quinn, *Not All Data Is Created Equal—When Experience Matters*, ACXIOM (Aug. 13, 2018), https://www.acxiom.com/blog/not-all-data-is-created-equal-experience-matters/ [https://perma.cc/49PU-AZXC].

40 *Acxiom Health Industry Page—Case Studies*, ACXIOM, https://www.acxiom.com/healthcare/ [https://perma.cc/Q73H-ZGLQ].

41 *Leading Health Insurer's Wellness Plan Sees Huge Response, Lower Cost*, ACXIOM, https://www.acxiom.com/healthcare/ [https://perma.cc/Q73H-ZGLQ].

42 Steven Melendez & Alex Pasternack, *Here Are the Data Brokers Quietly Buying and Selling Your Personal Information*, FAST CO. (Mar. 2, 2019), https://www.fastcompany.com/90310803/here-are-the-data-brokers-quietly-buying-and-selling-your-personal-information [https://perma.cc/V7AP-RZMF].

43 *See FICO Medication Adherence Score*, *supra* note 5; *see also* DIXON & GELLMAN, *supra* note 5.

44 Tara Parker-Pope, *Keeping Score on How You Take Your Medicine*, N.Y. TIMES WELL BLOG (June 20, 2011 5:23 PM), https://well.blogs.nytimes.com/2011/06/20/keeping-score-on-how-you-take-your-medicine/ [https://perma.cc/7ET2-LZM3].

45 *See id.*

46 *See id.*

set prices. But as a research scientist from one company told [the reporter]: 'I can't say it hasn't happened.'"[47]

Although aggregation companies like FICO have always had access to general, public demographic data, CHIACs give these companies access to much more specific data that in the past was only obtainable through doctors. As CHIACs grow as a channel for health data, so does the risk of their underregulation. Eric McCulley, Director of Strategic Solutions for data aggregator LexisNexis Risk Solutions, explained its role as a data aggregator unapologetically: "We sit on oceans of data . . . the fact is, our data is in the public domain. We didn't put it out there."[48]

B. The Harm of Unregulated CHIACs

While invasion of privacy and lack of control over personal data is itself harmful, the lack of regulation of CHIACs also creates more quantifiable harms stemming from unauthorized access to that data, such as individual safety risks and employer misuse. The lack of regulatory oversight makes unauthorized data access more likely for two reasons. First, as discussed earlier, CHIACs sell data to third parties who can then either utilize the data for their own purposes or sell it again.[49] Second, as data is held in more places by more parties, it is more likely to be hacked, leaked, or sold on the black market.

These harms illustrate the paradox of failing to regulate CHIACs under HIPAA: not regulating them undercuts the very protections HIPAA provides. As explained in Part III, HIPAA regulates data channels rather than data itself.[50] Consequently, even if a doctor has the same information as a CHIAC, the doctor's use of the data is HIPAA-regulated, but the CHIAC's use is not.[51] Hackers, aggregation companies, or employers looking to purchase health data can circumvent the protections of HIPAA by simply going directly to the CHIAC, instead of having to go through your doctor.

1. Increased Vulnerability to Individual Crimes

The underregulation of CHIACs poses individual crime risks because unprotected health information is easily exploitable. For example, sensitive information needed to commit medical identity theft is

47 Allen, *supra* note 5.

48 *Id.*

49 *See supra* Section I.A.

50 *See* U.S. DEP'T OF HEALTH & HUMAN SERVS., *supra* note 22, at 12–14.

51 *See id.* at 22.

easier to acquire. Medical identity theft occurs when new medical information (*i.e.*, drug results, chronic conditions, hospital visits) becomes associated with the identity of a different person, often to avoid negative consequences like credit history impact, debt, and criminal penalties, such as for positive drug tests.[52] Previously, a criminal had to breach a hospital's computer system to view a patient's health history and steal the patient's medical identity; now that hacker need only search for data leaked from a CHIAC or purchase data from a third or fourth party. Criminals can then use that data to steal the patient-consumer's medical identity. In one startling instance of medical identity theft, a mother nearly lost custody of her own children when someone stole her identity and used it to check into a hospital while in labor; the new baby tested positive for illegal drugs, leaving the identity theft victim with a $10,000 hospital bill and a fight to prove that she was not an unfit mother to her children.[53]

Lack of CHIAC regulation can also create new avenues for abusers to control their victims.[54] Under HIPAA, there are layers of privacy requirements to prevent accidental disclosure to potentially abusive parties; individuals have to affirmatively grant providers permission to leave health details in voicemail, text, or email messages, and the patient must consent to the way that electronic medical records are used.[55]

HIPAA also requires certain levels of encryption to prevent unauthorized access (sometimes called "eavesdropping").[56] Without these protections, victims are vulnerable to having their data accessed impermissibly by abusers through such "eavesdropping."[57] A 2013

---

52 Ball, *supra* note 6, at 112, 118. While identity theft most often results in financial consequences for victims, medical identity theft can also result in health consequences because doctors rely on this information when making medical decisions. For example, if the identity thief checks into a hospital with one blood type and the victim has a different blood type, the victim might receive the wrong transfusion. *Id.* at 118–20.

53 *Id.* at 111, 117–18; *see also* Caitlin Johnson, *Protect Against Medical ID Theft*, CBS NEWS (Oct. 9, 2006, 8:15 AM), https://www.cbsnews.com/news/protect-against-medical-id-theft/ [https://perma.cc/85UX-MDL9].

54 For more information on domestic violence and technology, see generally Nellie Bowles, *Thermostats, Locks and Lights: Digital Tools of Domestic Abuse*, N.Y. TIMES (June 23, 2018), https://www.nytimes.com/2018/06/23/technology/smart-home-devices-domestic-abuse.html [https://perma.cc/9QE6-EF3Y]; Jennifer Valentino-DeVries, *Hundreds of Apps Can Empower Stalkers to Track Their Victims*, N.Y. TIMES (May 19, 2018), https://www.nytimes.com/2018/05/19/technology/phone-apps-stalking.html [https://perma.cc/QFQ4-5ZK5].

55 *See* 45 C.F.R §§ 164.510(b)(3), 522(a)–(b) (2017).

56 *Id.* § 164.312 (HIPAA technical safeguards).

57 *See* Nat'l Network to End Domestic Violence, *Smartphone Encryption: Protecting Victim Privacy While Holding Offenders Accountable*, TECH. SAFETY (Apr. 12, 2016), https://

study found that only six percent of free health apps and 15% of paid health apps consistently used encrypted SSL connections for transferring data to third parties.[58] As health technology further permeates everyday life, its lack of regulation creates startling vulnerabilities to crime.

2. Employer Misuse

Lack of CHIAC regulation also makes it unclear what information employers can access about the health of an employee or prospective employee.[59] Without HIPAA protections, the ways that employers can obtain, utilize, or publicize health data might be regulated only by tangential regimes like the Americans with Disabilities Act, which was not designed to protect against these types of disclosures.[60]

Many employers offer workplace wellness programs that incentivize employees to log their health data or wear CHIAC devices like FitBits.[61] The "goals" set by these programs can range from step counts to weight loss.[62] This level of oversight by a company can start to feel coercive when the "incentives" amount to thousands of dollars[63] or company-wide recognition for participation.[64] The Equal Employment Opportunity Commission ("EEOC") previously provided guidance to workplaces on these large incentives, stating that they may only discount health insurance costs by up to 30%.[65] Following a recent court challenge, however, even the EEOC guidance is in

---

www.techsafety.org/blog/2016/4/12/smartphone-encryption-protecting-victim-privacy-while-holding-offenders-accountable [https://perma.cc/EL42-SRQV]. *See generally* FTC, INTERNET OF THINGS: PRIVACY & SECURITY IN A CONNECTED WORLD 17, 18 (2015); *Domestic Violence and Privacy*, *supra* note 6.

58 *See* U.S. DEP'T OF HEALTH & HUMAN SERVS., *supra* note 22.

59 *See* Ifeoma Ajunwa, *Workplace Wellness Programs Could Be Putting Your Health Data at Risk*, HARV. BUS. REV. (Jan. 19, 2017), https://hbr.org/2017/01/workplace-wellness-programs-could-be-putting-your-health-data-at-risk [https://perma.cc/WS54-ET4E].

60 *See* Appleby, *supra* note 4.

61 *Id.*

62 *See id.*

63 *Id.*

64 *See, e.g.*, *Workplace Health: Continuous Quality Improvement for Employee Health*, AM. HEART ASS'N, https://www.heart.org/en/professional/workplace-health [https://perma.cc/TEA2-7D4G] [hereinafter *Workplace Health*] (The American Heart Association's Workplace Health Plan is designed for employers to implement in their own workplaces and includes public "dashboards" for displaying employees' progress).

65 *EEOC's Final Rule on Employer Wellness Programs and Title I of the Americans with Disabilities Act*, EEOC, https://www.eeoc.gov/laws/regulations/qanda-ada-wellness-final-rule.cfm [https://perma.cc/62C7-C35J].

limbo.[66] Furthermore, this court challenge never addressed the coerciveness of "public shaming"-type tactics like participant lists or leaderboards.[67] Although HIPAA regulations do not protect information that is part of an individual's employment record,[68] it is unclear whether employer-sponsored wellness challenges are part of the employment record. Consequently, clearer regulations for CHIACs would help remedy potential employer misuse of this data.

Looking beyond employer wellness challenges, aggregation companies could easily sell information to employers or prospective employers. The lack of CHIAC regulation means that an individual's exercise, sleep, and health habits are available to that individual's current or prospective employer.[69] CHIAC regulation would make it more difficult for employers to conduct such invasive individual espionage.

II. CHIAC Regulation

The evolution of mHealth has left patient-consumers struggling to find a balance between the promise and the intrusion of technology. Despite the incredibly personal nature of this data, CHIACs' use of this data is relatively unregulated. HIPAA, the main source of protection for health information, has not been interpreted to cover CHIACs.[70] Instead, CHIACs are solely regulated through inadequate consumer-based protections, like the FTC.[71] However, the regulatory

66 AARP v. U.S. EEOC, No. 16-2113 (JDB), 2018 U.S. Dist. LEXIS 27317, at *1 (D.D.C. Jan. 18, 2018). It appears that the district court's 2018 ruling suspending the guidance went into effect in January 2019. *Legal Alert: EEOC's Status Report in* AARP v. EEOC *Creates Uncertainty for Wellness Programs*, JA Counter (Apr. 17, 2018), https://jacounter.com/legal-alert-eeocs-status-report-aarp-v-eeoc-creates-uncertainty-wellness-programs [https://perma.cc/WY6L-K3QU] ("For years, the EEOC had declined to provide specific guidance on the level of incentive that may be provided under the ADA . . . In 2016, after years of uncertainty on the issue, the agency released rules on wellness incentives that resemble, but do not mirror, the 30% limit established under U.S. Department of Labor . . . regulations applicable to health-contingent employer-sponsored wellness programs.").

67 *See, e.g.*, *Workplace Health*, *supra* note 64.

68 45 C.F.R. § 160.103 (2017) (defining "protected health information").

69 *See, e.g.*, *FICO Medication Adherence Score*, *supra* note 5; Fitbit, *supra* note 1, ("At Fitbit, health and fitness come first. Each Fitbit product includes these core features and more to inspire you on your journey: exercise & activity tracking; health & fitness app; and innovative sleep tools."). Beyond the scope of this Note is the question of whether the Americans with Disabilities Act or other laws could prevent employers from using this information in hiring decisions.

70 *See infra* Part III.

71 The FDA does not have the authority to effectively regulate CHIACs or other mHealth data because CHIACs and the resulting patient-consumer data mostly fall outside of the FDA's regulatory jurisdiction. *See* Am. Bar Ass'n Health Law Section, supra note 2, at 4–5, 11–14.

bodies lack the institutional knowledge and necessary authority to protect patient-consumers in this unique, evolving, and interdisciplinary field.

A. HIPAA and CHIACs

Congress passed HIPAA in 1996 to expand health insurance coverage and raise the standard of health care in America.[72] In 2002 and 2003, HHS promulgated the HIPAA Privacy Rule[73] and Security Rule[74] to meet the requirements of Title II of HIPAA, which directed the HHS Secretary to issue standards for transmitting electronic personal health information.[75]

In 2009, following the passage of the Health Information Technology for Economic and Clinical Health ("HITECH") Act, HHS issued rules to "conform the enforcement regulations" of HIPAA to the requirements of the HITECH Act and address the expanding use of digital technology in health care delivery.[76] These rules (collectively referred to as HIPAA) apply to "covered entities": "health plans," "health care clearinghouses," "a health care provider who transmits any health information in electronic form" in connection with certain transactions, and certain business associates that provide services on behalf of other covered entities.[77] As explored more fully in Part III, despite the "modernization" in the HITECH Act amendments, HHS does not view CHIACs as covered entities unless the CHIACs work directly with a "covered entity" as defined under HIPAA, such as if FitBit partnered with a health insurance company to provide the insurer's clients with FitBits.[78] This means that if a health insurance plan

---

The FDA does not regulate most mobile apps because it does not typically consider them "medical devices" within its regulatory purview. *Id.* at 4–5. CHIACs that produce devices are also not regulated by the FDA because the agency classifies these devices as low-risk products for "general wellness." *Id.* at 15.

72 *See* Office of Corp. Compliance, Univ. of Chi. Med. Ctr., *HIPPA Background*, HIPPA PROGRAM OFF. (Oct. 23, 2006), http://hipaa.bsd.uchicago.edu/background.html [https://perma.cc/P4E4-2WS6].

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

74 Health Insurance Reforms: Security Standards, 68 Fed. Reg. 8,334 (Feb. 20, 2003) (to be codified at 45 C.F.R. pts. 160, 162, 164).

75 HHS, *Summary of the HIPAA Security Rule*, HEALTH INFO. PRIVACY, https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html [https://perma.cc/S7SQ-JHJ8].

76 HIPAA Administrative Simplification: Enforcement, 74 Fed. Reg. 56123, 123–26 (Oct. 30, 2009) (to be codified at 45 C.F.R. pt. 160).

77 45 C.F.R. § 160.103 (2017).

78 *See* U.S. DEP'T OF HEALTH & HUMAN SERVS., *supra* note 22, at 4.

covers health-tracking wearables, the data is protected; but, if a patient-consumer purchases the same device out-of-pocket, the data is not protected until the patient-consumer gives the data to a doctor.[79] Even when the data makes it in the doctor's hands, it is only *that copy* of that data that is protected. The CHIAC that sold the product and that has an identical set of data (perhaps with more detail) is not regulated under HIPAA at any point during the transaction.[80] Furthermore, because HIPAA does not provide a private right of action for misuse of data, courts have been unable to respond.[81] Any change must therefore come from Congress or HHS.

B. The FTC and CHIACs

The FTC has authority to regulate companies generally, which theoretically means they have more authority to regulate CHIACs; however, the FTC's current regulation is not sufficient when applied to the unique challenges of health care.[82] Section 45 of the Federal Trade Commission Act grants the FTC authority to regulate "unfair or deceptive acts or practices."[83] If a CHIAC engages in deceptive practices, the FTC can investigate or sanction it.[84] The "unfair or deceptive . . . practices" standard, however, is insufficient in two ways.

First, the definition of "unfair or deceptive" practices is not as inclusive or robust as HIPAA's regulatory protections. HIPAA requires that information about the use and disclosure of a patient's data be presented in a clear, user-friendly way.[85] On the other hand, sufficient notification under the Federal Trade Commission Act is anything that is *not* "unfair or deceptive."[86] For example, wordy "Terms and Conditions" pages might not satisfy HIPAA regulations. Most consumers do not read these extensive and confusing notices,[87] mak-

79 *See id.* at 9.

80 *See id.* at 9 n.40. Furthermore, that copy of the data is only protected in the hands of the health provider if the health provider engages in "covered transactions" as defined in HIPAA, which focus on health insurers. *See* 42 U.S.C. § 1320d-2(a)(2) (2012). This means that if a health provider does not accept insurance, and potentially if a patient does not use insurance, the interaction is not covered, thus exposing potential gaps in HIPAA, particularly as health insurance changes over time. This issue, however, is beyond the scope of this Note.

81 *See* Acara v. Banks, 470 F.3d 569, 571–72 (5th Cir. 2006) ("Every district court that has considered this issue is in agreement that the statute does not support a private right of action.").

82 *See, e.g.*, U.S. DEP'T OF HEALTH & HUMAN SERVS., *supra* note 22, at 17–18.

83 15 U.S.C. § 45 (2012).

84 *See* U.S. DEP'T OF HEALTH & HUMAN SERVS., *supra* note 22, at 17.

85 *See* 45 C.F.R § 164.520 (2014).

86 *See* 15 U.S.C. § 45.

87 *See, e.g.*, Shankar Vedantam, *Do You Read Terms of Service Contracts? Not Many Do, Research Shows*, NPR (Aug. 23, 2016, 5:06 AM), https://www.npr.org/2016/08/23/491024846/do-

ing it difficult for a company to claim they are either clear or user-friendly. "Terms and Conditions" pages might satisfy Federal Trade Commission Act requirements, however, because the pages are not necessarily unfair or deceptive—they are simply unclear.

Second, a CHIAC may simply choose not to include the exact details of how data will be used in the company's terms and conditions page. Except in the most flagrant cases,[88] this omission does not violate the Federal Trade Commission Act. As detailed in the Introduction, smart vibrator company Standard Innovation settled a lawsuit with customers, agreeing to change its Terms and Conditions and to pay individuals who used its product.[89] The lawsuit alleged that the company tracked and analyzed consumers' usage of the product without notification or consent.[90] Despite the intensely personal nature of the data, the FTC has not identified this omission as unfair or deceptive enough to warrant opening a formal investigation.[91]

The FTC *has* used its authority to regulate companies deemed to have inadequate security to protect consumer data by investigating and correcting those practices if consumers report those security practices to the agency.[92] This is insufficient to prevent breaches in a landscape where companies regularly buy and sell data without consumer knowledge. The average consumer cannot track when and where their data is sold, making it difficult to know if a third—or fourth, or fifth—party *has* the data, let alone whether their data is properly protected.

For example, following Facebook's Cambridge Analytica scandal in early 2018, individuals scrambled to find out how they could locate their potentially compromised data.[93] Then, Facebook admitted in a news report—albeit, in extremely fine print—that it "do[es] not know precisely what data the app shared with Cambridge Analytica or ex-

---

you-read-terms-of-service-contracts-not-many-do-research-shows [https://perma.cc/F9EX-KA3X].

88 *See, e.g.*, *In the Matter of PaymentsMD, LLC*, 159 F.T.C. 241, 243–47 (2015) (holding PaymentsMD accountable where PaymentsMD altered its sign-up process to include a hidden permission to collect sensitive health information; Payments MD actively reached out to insurance companies, labs, and pharmacies to collect such information without express consent).

89 Domonoske, *supra* note 8.

90 Hern, *supra* note 13.

91 *See* FTC Comment Letter, *supra* note 17, at 2 n.9 (identifying the We-Vibe lawsuit as an example of "problematic privacy practices" that raise "important questions about the ability of the existing legal landscape to protect consumers' privacy interests").

92 *See* U.S. Dep't of Health & Human Servs., *supra* note 22, at 17–18.

93 *See* Bill Chappell, *How to Check if Your Facebook Data Was Used by Cambridge Analytica*, NPR (Apr. 10, 2018, 1:59 PM), https://www.npr.org/sections/thetwo-way/2018/04/10/601163176/how-to-check-if-your-facebook-data-was-used-by-cambridge-analytica [https://perma.cc/2DKQ-EVRE].

actly how many people were impacted."[94] While the data involved in that case was not specifically health-related, it easily could have been—many tracking applications, including FitBit, connect to Facebook.[95] This illustrates the insufficiency of the FTC regulation for this type of company: individual consumers—and evidently the companies holding their data—just do not understand how their data is being used. Bringing CHIACs under HIPAA would require those companies to give clear, user-friendly information about how an individual's data is being used. This would give patient-consumers better access to the information they need to hold companies accountable.

C. State-Level Regulations

Unlike federal protections, state regulations sometimes address data rather than the channels through which the data moves; however, they also focus on online data generally instead of health-related data particularly.[96] Furthermore, state protections focus mostly on notification requirements after breaches have already occurred,[97] or other similar *post hoc* security measures,[98] rather than regulating the use and disclosure of data in the first place. While many states considered implementing expanded consumer data protections in 2018, those measures mostly failed.[99] Federal protections are ultimately preferable because state protections can create a confusing patchwork of regulations for consumers and companies; while a consumer may be in a state with strong data protection, their data may exist on a server in a state that has very different data protection standards.[100]

---

94 Mike Schroepfer, *An Update on Our Plans to Restrict Data Access on Facebook*, FACEBOOK NEWSROOM (Apr. 4, 2018), https://newsroom.fb.com/news/2018/04/restricting-data-access/ [https://perma.cc/Z35C-GVKW].

95 FitBit touts the ability to connect your FitBit to social media channels like Facebook, where users can share their progress. *See Fitbit App*, https://www.fitbit.com/app [https://perma.cc/EU7K-ZUP3].

96 *Data Security Laws—Private Sector*, NAT'L CONF. OF ST. LEGISLATURES, http://www.ncsl.org/research/telecommunications-and-information-technology/data-security-laws.aspx [https://perma.cc/8UVA-ZS85].

97 *See, e.g.*, *Security Breach Notification Laws*, NAT'L CONF. OF ST. LEGISLATURES, http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx [https://perma.cc/RJ39-4S68].

98 *See, e.g.*, *Data Security Laws—Private Sector*, *supra* note 96.

99 *2018 Privacy Legislation Related to Internet Service Providers*, NAT'L CONF. OF ST. LEGISLATURES, http://www.ncsl.org/research/telecommunications-and-information-technology/privacy-legislation-related-to-internet-service-providers-2018.aspx [https://perma.cc/9FWC-34MS].

100 The added complexity of the Internet makes determining what part of a jurisdiction's standards to apply, adding another layer to the complicated field of Conflict of Laws. *See, e.g.*, Microsoft Corp. v. United States, 829 F.3d 197 (2d Cir. 2016), *vacated and remanded* 138 S. Ct. 1186 (2018) (discussing the difficulties posed by conflict of law questions in the digital age);

III. HIPAA's Existing Structure

A. *Definitions in HIPAA*

HIPAA currently applies to all "covered entities."[101] Covered entities include health plans, health clearinghouses, or any health care provider "who transmits any health information in electronic form in connection with a [covered] transaction."[102] "Covered transactions" are ones for which the HHS Secretary has adopted standards,[103] and "transactions" are defined as "the transmission of information between two parties to carry out financial or administrative activities related to health care."[104] Health care providers include "any other person or organization who furnishes, bills, or is paid for health care in the normal course of business."[105] Health care is broadly defined as "care, services, or supplies *related* to the health of an individual."[106] Health information is similarly broadly defined as information

> created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse and relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual.[107]

HHS's interpretation of "covered entities" does not appear to have changed much—if at all—in the 20 years that HIPAA has been in place. Thus, the interpretation of "covered entities" receives very little attention.

Because HIPAA has a fairly large exception for law enforcement and court orders and it contains no private right of action, most courts' examination of the interpretation of "covered entity" or "health care provider" is ancillary at best.[108]

Barcelona.com, Inc. v. Excelentisimo Ayuntaiento de Barcelona, 330 F.3d 617 (4th Cir. 2003); GlobalSanteFe Corp. v. Globalsantefe.com, 250 F. Supp. 2d 610 (E.D. Va. 2003).

101 45 C.F.R. § 160.103 (2017).

102 *Id.*

103 The standards can be found in the regulations, 45 C.F.R. pt. 162.

104 *Id.* § 160.103.

105 *Id.*

106 *Id.* (emphasis added); *see also* 42 U.S.C. § 1320d(4) (2012).

107 42 U.S.C. § 1320d(4).

108 45 C.F.R. § 164.512(f)(1) (HIPAA's law enforcement exception); *see, e.g.*, United States v. Elliott, 676 F. Supp. 2d 431, 439–40 (D. Md. 2009) (stating that law enforcement exception in HIPAA makes a discussion of whether HIPAA applies unnecessary); United States v. Zamora, 408 F. Supp. 2d 295, 298 (S.D. Tex. 2006) (noting that "HIPAA was passed to ensure an individual's right to privacy over medical records [and] not intended to be a means for evading prosecu-

Within HHS's own guidance documents, interpretations of "covered entity" are self-referencing, repeating statutory definitions rather than providing guidance for determining when an entity is covered.[109] For example, HHS's "Covered Entity Guidance" tool simply recites HIPAA's definitions using the same language in the statute.[110] HHS's "Covered Entities and Business Associates" webpage provides a chart to give examples of health care providers, health plans, and health care clearinghouses, but the list for "health care provider" merely states that "[t]his includes providers such as: doctors, clinics, psychologists, dentists, chiropractors, nursing homes, [and] pharmacies."[111] Other guidance documents focus on gray areas that existed at the time HIPAA was enacted over two decades ago: the role of employers and health care business associates.[112] None of the guidance documents provide an in-depth analysis of what a less traditional or more modern covered entity looks like.

Looking back at early public comment periods provides some insight into just how broad HHS intended "health care provider" to be. Indeed, in one rule proposal, HHS stated: "The statutory definition of a health care provider is broad."[113] HHS has also consistently refused to narrow the definition in response to requests to exclude or list specific providers, referring back to the statutory definition instead:

---

tion in criminal proceedings," and therefore whether HIPAA applied was immaterial); United States v. Grace, 401 F. Supp. 2d 1093, 1097–98 (D. Mont. 2005) ("Although it is not entirely clear that ATSDR or DHHS meet the definition of a 'health care clearinghouse' as defined by HIPAA, [the court assumes] that HIPAA applies to the agency holding the medical records."). When courts examine the definition of "health care provider," the focus appears to be on whether the care provided by the entity relates to the individual's health or for some other purpose. *See, e.g.*, Beard v. City of Chicago, No. 03 C 3527, 2005 WL 66074, at *2 (N.D. Ill. Jan. 10, 2005) (finding employer's return-to-work fitness examination did not make employer a healthcare provider because examination was "for the purpose of determining fitness to return to work").

109 *See* U.S. DEP'T OF HEALTH & HUMAN SERVS., *supra* note 22, at 13–14.

110 CTRS. FOR MEDICARE & MEDICAID SERVS., ADMINISTRATIVE SIMPLIFICATION: COVERED ENTITY GUIDANCE, https://www.cms.gov/Regulations-and-Guidance/Administrative-Simplification/HIPAA-ACA/Downloads/CoveredEntitiesChart20160617.pdf [https://perma.cc/CL55-MQXS].

111 HHS, *Covered Entities and Business Associates*, HEALTH INFO. PRIVACY, https://www.hhs.gov/hipaa/for-professionals/covered-entities/index.html [https://perma.cc/8PQV-RBX5].

112 *See, e.g.*, HHS, *Business Associates*, HEALTH INFO. PRIVACY, https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/business-associates/index.html [https://perma.cc/GHW9-7HJN]; HHS, *Business Associate Contracts*, HEALTH INFO. PRIVACY, https://www.hhs.gov/hipaa/for-professionals/covered-entities/sample-business-associate-agreement-provisions/index.html [https://perma.cc/S9N3-VZRV].

113 National Standard Health Care Provider Identifier, 63 Fed. Reg. 25,320, 25,325 (proposed May 7, 1998) (to be codified at 45 C.F.R. pt. 142).

> To the extent that a "department-operated hospital" *meets the definition of a "health care provider" and conducts any of the standard transactions*, it is a covered entity for the purposes of this rule.
>
> . . . As with other aspects of this rule, we do not define "health care provider" based on the title or label of the professional. The professional activities of these kinds of providers vary; a person is a "health care provider" *if those activities are consistent with the rule's definition of "health care provider."*
>
> . . . The manufacturer must be *providing health care consistent with the final rule's definition* in order to be considered a health care provider.[114]
>
> Instead, we will *use our definition of "health care" found at 160.103* to determine whether a particular service is a "health care" service or not.[115]

Moreover, while the definition of "covered entities" has not changed, HHS has expanded the definitions underlying "covered entities" to reflect changing realities of healthcare. For example, "health information" now includes explicitly genetic information,[116] "business associate" now better reflects the ways insurance companies do business,[117] and "health plan[s]" now include prescription drug card sponsors, a relatively new category of insurance providers.[118] This willingness to change in the face of technological progress was reflected during the notice-and-comment process in 2000. HHS noted that:

> A number of commenters asked that we include disease management activities and other similar health improvement programs, such as preventive medicine, health education services and maintenance, health and case management, and risk assessment, in the definition of "health care." Commenters maintained that the rule should avoid limiting tech-

---

114 Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. 82,462, 82,568–69, 82,573 (Dec. 28, 2000) (to be codified at 45 C.F.R. § 160.103) (emphasis added).

115 Health Insurance Reform: Standards for Electronic Transactions, 65 Fed. Reg. 50,312, 50,316 (Aug. 17, 2000) (to be codified at 45 C.F.R. pts. 160, 162) (emphasis added).

116 45 C.F.R. § 160.103 (2017).

117 45 C.F.R. §§ 153.20, 160.103 (2014).

118 *See* Medicare Prescription Drug, Improvement, and Modernization Act of 2003, 42 U.S.C. § 1395w-141(h)(6)(A) (2012).

> nological advances and new health care trends intended to improve patient "health care."[119]

Instead of disagreeing or taking the opportunity to clarify what technological advances HHS considered valid "health care," HHS actually appeared to agree that the final rule should not limit technological advances and new health care trends:

> . . . rather than create a blanket rule that includes such terms in or excludes such terms from the definition of "health care," we define health care based on the underlying activities that constitute health care . . . Listing activities by label or title would create the risk that important activities would be left out and, given the lack of consensus on what these terms mean, could also create confusion.[120]

While the existing definitions of "covered entity" do not explicitly include CHIACs and HHS has not interpreted the definition to cover them, HHS has repeatedly left the door open to expand their interpretation of HIPAA to keep up with technological and health care innovations.

B. Protective Provisions in HIPAA

HIPAA has three main rules regarding privacy: (1) breach notification,[121] (2) security, and (3) privacy.[122] Interpreting covered entities to include CHIACs would require CHIACs to adhere to these protective rules.

The Breach Notification Rule requires covered entities to notify affected individuals following a breach of protected health information.[123] While this notification is important once an individual's information is released, extending this rule to CHIACs is not as crucial because of the protections of other consumer agencies like the FTC[124] and evolving tort law surrounding breach liability.[125]

---

119 Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. at 82,571.

120 *Id.*

121 45 C.F.R. pt. 164(D) (2018).

122 *See* Standards for Privacy of Individually Identifiable Health Information, 67 Fed. Reg. 53,182 (Aug. 14, 2002) (to be codified at 45 C.F.R. pt. 160, 164); Health Insurance Reform: Security Standards, 68 Fed. Reg. 8,334 (Feb. 20, 2003) (to be codified at 45 C.F.R. pt. 160, 162, 164). The HIPAA Privacy rules were updated in 2009 by the HITECH Act § 13407(g)(1).

123 45 C.F.R. pt. 164(D).

124 Although HIPAA's breach notification requirements may be more stringent than FTC enforcement, which is optional, this Note focuses on affirmative regulations for CHIAC like protecting data prior to its breach. These differences therefore will not be examined.

125 *See generally* Mark A. Geistfeld, *Protecting Confidential Information Entrusted to*

The Security Rule requires a covered entity to "[e]nsure the confidentiality, integrity, and availability of all electronic protected health information . . . [it] creates, receives, maintains, or transmits,"[126] and to identify and protect against anticipated threats or disclosures.[127] Increasing the required encryption standards to which CHIACs are subject would decrease the likelihood of breaches.[128]

The Privacy Rule governs how a healthcare provider may disclose or use data and lays out the requirements for obtaining authorization to do so.[129] Specifically, 45 C.F.R. § 164.501 and § 164.508 limit the use of personally identifiable health information by covered entities for marketing purposes.[130] This would require a company like FitBit to obtain a patient-consumer's permission through a series of highly regulated steps prior to selling data to advertisers or aggregation companies.

IV. HIPAA AS A SOLUTION TO CHIAC REGULATION

Because of HHS's experience regulating health-related companies under HIPAA,[131] and as technology allows individuals to drive their own health care in new ways,[132] it makes the most sense that

Others in Business Transactions: Data Breaches, Identity Theft, and Tort Liability, 66 DEPAUL L. REV. 385, 387–88 (2017); Alicia Solow-Niederman, *Beyond the Privacy Torts: Reinvigorating a Common Law Approach for Data Breaches*, 127 YALE L.J.F. 614 (2018), https://www.yalelawjournal.org/pdf/Solow-Niederman_qthw8784.pdf [https://perma.cc/UX3W-LTRM].

126 45 C.F.R. § 164.306(a).

127 *See* Health Insurance Reform: Security Standards, 68 Fed. Reg. 8,334.

128 It is true that HIPAA itself may be insufficient to keep pace with technological advances and to ensure that data is stored in a way that prevents it from ever being re-identified or de-aggregated. Certain levels of de-identifying data are increasingly easy to reverse engineer, like deletion or use of pseudonym data. *See* Boris Lubarsky, Note, *Re-Identification of "Anonymized Data,"* 1 GEO. L. TECH. REV. 202 (2017); *see also* Vanessa Teague et al., *The Simple Process of Re-Identifying Patients in Public Health Records*, PURSUIT: UNIV. OF MELB. (Dec. 18, 2017), https://pursuit.unimelb.edu.au/articles/the-simple-process-of-re-identifying-patients-in-public-health-records [https://perma.cc/H9MC-5X4G]. These dangers, however, exist for all data—covered by HIPAA or not—and is not a reason not to reinterpret HIPAA protections to apply to CHIACs.

129 45 C.F.R. § 164.508. The Privacy Rule also governs how individuals may access their data. 45 C.F.R. § 164.524; HHS, *Individuals' Right Under HIPAA to Access Their Health Information*, HEALTH INFO. PRIVACY, https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/access/index.html#newlyreleasedfaqs [https://perma.cc/9UC7-ANA9]. Although the right to access data is important, it is potentially less pressing for patient-consumers worried about their data because CHIACs give individuals access to their health data through aggregated reports or online interfaces.

130 45 C.F.R §§ 164.501, 164.508(a).

131 *See* U.S. DEP'T OF HEALTH & HUMAN SERVS., *supra* note 22, at 31.

132 *See* Jonah Comstock, *Connecting the Dots of Health Consumerism, Digital Health, and Health and Social Policy*, MOBILE HEALTH NEWS (Apr. 30, 2019), https://

CHIAC regulation comes through HIPAA. Because CHIACs are now a prominent channel for health-related data, HIPAA is especially well-suited for regulating them.[133]

Because HHS is an executive agency, the President has the ability to direct the HHS Secretary to promulgate regulations and guidance that include CHIACs in HIPAA's definition of covered entities. Congress could achieve a similar outcome by amending HIPAA or passing another bill to require HHS to promulgate new regulations under HIPAA, as Congress did with the HITECH Act.

The most sensible method for including CHIACs in HIPAA's definition of covered entities, however, is through HHS itself.[134] As discussed in Part III, HIPAA applies to "covered entities," which include any "health care provider" that "transmits any health information in electronic form in connection with a [covered] transaction."[135] HHS should consider CHIACs as health providers in order to bring them under the umbrella of "covered entities."

Changing this definition is relatively straightforward. CHIACs transmit health information[136] and are arguably health providers; however, they do not fit neatly into any current covered transactions. This is because covered transactions are "transactions that the Secretary may prescribe by regulation,"[137] and all existing standards apply solely to interactions with health insurers.[138] The lack of applicable standards with respect to covered transactions is not a jurisdictional bar, however, because HHS has the authority to adopt new transactional standards.[139] Therefore, a rule adopting new transactional standards and

---

www.mobihealthnews.com/content/connecting-dots-health-consumerism-digital-health-and-health-and-social-policy [https://perma.cc/D5AQ-6WYB] (discussing how increasing consumerization and technology are driving individuals to drive treatment in a shift away from medical professionals alone driving all treatment decisions); Jess Scherman, *5 Ways Technology in Healthcare Is Transforming the Way We Approach Medical Treatment*, RASMUSSEN C. (May 20, 2019), https://www.rasmussen.edu/degrees/health-sciences/blog/technology-in-healthcare-transformation/ [https://perma.cc/82LA-CTHU].

133 *See supra* Section I.A.

134 HHS could subject CHIACs to only some parts of HIPAA by, for example, applying only HIPAA's privacy rules but not its access rules. HHS may want to limit the expansion of HIPAA; for example, a limited expansion could create smaller pushback and reduce the possibility of unforeseen interactions with existing regulations.

135 45 C.F.R. § 160.103 (2018).

136 CHIACs clearly transmit "health information in electronic form." *Id.* The hallmark of these companies is to electronically receive raw health data from patient-consumers and transmit analysis back.

137 *Id.*

138 *See* 42 U.S.C. § 1320d-2(a)(2) (2012).

139 42 U.S.C. § 1320d-2(a)(3) (2012). Congress gave HHS the authority to adopt new trans-

folding CHIACs into "covered entities" does not impermissibly expand HHS's jurisdiction. This rule would merely interpret HHS's *existing* jurisdictional limits consistent with modern, digital, consumer-driven health care. The Supreme Court has consistently ruled that agencies interpreting their own jurisdiction are entitled to the same deference that agencies receive when interpreting their organic statutes.[140]

Not only is it within HHS's legislative authority to issue this regulation, it is appropriate for HHS to do so. CHIACs already engage in analogous transactions and health care that fit within HHS's existing definition of a covered health provider. Furthermore, refusing to regulate CHIACs arguably abdicates HHS's responsibility to enforce HIPAA.[141]

A. CHIACs Fit Existing Regulatory Definitions

CHIACs fit into HHS's existing regulatory definition of a "health provider," and including CHIACs in a new regulation would not contravene existing regulations or impermissibly expand HHS's reach. CHIACs are arguably health care providers in the modern context because they provide health care and care coordination.[142]

Health care providers include "any other person or organization who furnishes, bills, or is paid for health care in the normal course of business."[143] HHS has repeatedly interpreted the definition of health care broadly; it is the provision of "care, services, or supplies related to the health of an individual,"[144] including care coordination.[145]

---

actional standards under § 1174 of HIPPA. *See* HIPAA, Pub. L. No. 104-191, § 1174, 110 Stat. 1936, 2026 (1996).

140 City of Arlington v. FCC, 569 U.S. 290, 299 (2013) ("The reality, laid bare, is that there is *no difference*, insofar as the validity of agency action is concerned, between an agency's exceeding the scope of its authority (its 'jurisdiction') and its exceeding authorized application of authority that it unquestionably has."). The example used by the majority opinion to illustrate this point is directly parallel to HIPAA's construction, where the first section of the statute states the rule, and the second part states that an agency "may prescribe rules and regulations necessary" to carry out the first section. *Id.* at 298.

141 *See generally* Massachusetts v. EPA, 549 U.S. 497 (2007).

142 Although CHIACs might argue that they are not health care providers under HIPAA because they also develop nonhealth-focused technology, HHS has clarified that an entity does not have to be "primarily" engaged in health care to be considered a health care provider. *See* Standards for Privacy of Individually Identifiable Health Information; Final Rule, 65 Fed. Reg. 82,462, 82,569–70, 82,575 (Dec. 28, 2000) (to be codified at 45 C.F.R. pt. 160, 164). Furthermore, all of a company's services do not have to be HIPAA-protected for some of its work to be subject to HIPAA. *See id.*

143 45 C.F.R. § 160.103 (2017).

144 *Id.*

CHIACs advertise themselves as providing services related to health.[146] Health care wearables are seeing increasing use by traditional healthcare providers, indicating that even these providers think wearables provide a valuable healthcare resource.[147] The National Institutes of Health is using wearables in a nationwide initiative, called *All of Us*, to build "a diverse database that can inform thousands of studies on a variety of health conditions."[148] The project started with participants filling out surveys and providing physical samples, but in January 2019, the program announced that it was enabling participants to "link their Fitbit accounts to the program to share additional data for research."[149] While HIPAA regulates the companies providing the blood collection and urine sample services in this program—and the labs analyzing those samples[150]—HIPAA should also protect the health data coming from the Fitbit. The National Institutes of Health values the information and analysis provided by Fitbit just as it values the data from conventional health care providers; in fact, the director of the program said that "[c]ollecting real-world, real-time data through digital technologies will become a fundamental part of the program."[151]

Similarly, in 2016 the director of the FTC's Bureau of Consumer Protection spoke about the increasing use of mHealth technologies—including Fitbit and mobile health applications—and discussed the gap in regulation for healthcare services provided "outside of hospi-

145 *See* Health Insurance Reform: Standards for Electronic Transactions, 65 Fed. Reg. 50,312, 50,315–16 (published Aug. 17, 2000) (to be codified at 45 C.F.R. pt. 160, 164).

146 *See, e.g.*, FITBIT, *supra* note 1 ("At Fitbit, health and fitness come first."); *Forbes Insights: Can a Fitness Tracker Save Your Life?*, *supra* note 28; *Meditation for Anxiety*, *supra* note 1.

147 *See, e.g.*, Press Release, Fitbit, Fitbit Launches Fitbit Care, A Powerful New Enterprise Health Platform for Wellness and Prevention and Disease Management (Sept. 19, 2018), https://investor.fitbit.com/press/press-releases/press-release-details/2018/Fitbit-Launches-Fitbit-Care-A-Powerful-New-Enterprise-Health-Platform-for-Wellness-and-Prevention-and-Disease-Management/default.aspx [https://perma.cc/XQV2-VSKX]; Amy McDonough, *How Wearable Devices Are Improving Clinical Outcomes*, CERNER (Aug. 22, 2018), https://www.cerner.com/blog/wearable-devices-improving-clinical-outcomes [https://perma.cc/WL5P-BK9G]; Mark Sullivan, *How Fitbit Is Trying to Transform Healthcare, and Itself*, FAST CO. (June 8, 2018), https://www.fastcompany.com/40578138/how-fitbit-is-trying-to-transform-healthcare-and-itself [https://perma.cc/Z2MP-ZFB5].

148 Nat'l Inst. of Health, All of Us *Research Program Overview*, ALL OF US, https://allofus.nih.gov/about/all-us-research-program-overview [https://perma.cc/U6W3-ACV5].

149 Nat'l Inst. of Health, All of Us *Research Program Expands Data Collection Efforts with Fitbit*, ALL OF US (Jan. 16, 2019), https://allofus.nih.gov/news-events-and-media/announcements/all-us-research-program-expands-data-collection-efforts-fitbit [https://perma.cc/4WZT-JRGS].

150 *See* 45 C.F.R. § 160.103 (2017).

151 National Institute of Health, *supra* note 149.

tals and doctors' offices . . . ."[152] Her comment shows that other government agencies see these technologies as health care providers. AthenaHealth, a data management platform for health-services providers and insurers, considers CHIACs like FitBit to be providing a health care resource, saying that "[p]atients use mobile health technology to . . . [t]rack their own health data through mHealth apps and devices like the Fitbit . . . ."[153] Fitbit itself is starting to grow the distinctly "health care" portion of its business, advertising to patient-consumers the health benefits of Fitbit's algorithms.[154]

Even if CHIACs do not fit neatly into "health care providers," CHIACs certainly fall into the category of case management. Case management is a process of coordinating, assessing, and evaluating a patient's health and overall needs.[155] CHIACs often help individuals coordinate, assess, and evaluate their health.[156] HHS has chosen to interpret case management services (a broad category itself) as part of the definition of health care.[157] CHIACs therefore fit within the definition of health care providers in multiple ways and would be appropriately regulated by HIPAA.

B. HHS Has Legislative Authority to Issue New Transaction Regulations

HHS has the legislative authority to issue new transactional standards to regulate health care providers. HIPAA expressly states that the "Secretary shall review the standards adopted under section 1320d-2 of this title, and shall adopt modifications to the standards (including additions to the standards), as determined appropriate."[158] The statute instructs the Secretary to adopt standards related to transactions that fit into nine categories outlined in § 1320d–2, or "other

---

152 Jessica Rich, Dir., Bureau of Consumer Prot., FTC, Speech at National Advertising Division Annual Conference: Trends in Consumer Protection: Issues Facing the FTC Today (Sept. 26, 2016), https://www.ftc.gov/system/files/documents/public_statements/987463/rich_-_nad_annual_conf_2016_remarks_9-26-16.pdf [https://perma.cc/C6WH-PF9B].

153 *What Is Mobile Health Technology?*, ATHENAHEALTH, https://www.athenahealth.com/knowledge-hub/mobile-health-technology/what-is-mobile-health-technology [https://perma.cc/7FNR-XA7V].

154 *See, e.g.*, *Forbes Insights: Can a Fitness Tracker Save Your Life?*, *supra* note 28.

155 *See, e.g.*, *What Is a Case Manager?*, CASE MGMT. SOC'Y OF AM., http://www.cmsa.org/who-we-are/what-is-a-case-manager/ [https://perma.cc/N939-FKBD].

156 *See, e.g.*, *Forbes Insights: Can a Fitness Tracker Save Your Life?*, *supra* note 28.

157 Health Insurance Reform: Standards for Electronic Transactions, 65 Fed. Reg. 50,312, 50,315–16 (Aug. 17, 2000) (to be codified at 45 C.F.R. pt. 160, 164).

158 42 U.S.C. § 1320d-3(b)(1) (2012); HIPAA, Pub. L. No. 104-191, § 1174(b)(1), 110 Stat. 1936, 2026 (1996).

financial and administrative transactions determined appropriate by the Secretary, consistent with the goals of improving the operation of the healthcare system and reducing administrative costs."[159] The definitions of these transactions were set by HHS, and are part of the regulations adopting the standards applicable to that defined transaction.[160] Because HHS defined these transactions to begin with, issuing a new transactional standard would not be beyond HHS's legislative authority. It would not change the three core categories under HIPAA's protection (healthcare clearinghouses, health plans, or health providers who engage in transactions)[161] but would merely expand the final category and therefore is appropriate.

C. CHIACs Engage in Analogous Transactions

Not only would issuing new transactional standards comport with HHS's duty and authority to issue standards related to the goals of "improving the operation of the health care system and reducing administrative costs,"[162] doing so is appropriate because CHIACs engage in transactions analogous to those already covered in HIPAA. One currently covered set of transactions is transactions for referral certification and authorizations. These transactions are defined as: "(a) A request . . . for the review of health care to obtain an authorization for the health care[;] (b) A request . . . to obtain authorization for referring an individual to another health care provider[;] [and] (c) A response . . . to a request described in paragraph (a) or paragraph (b) of this section."[163] This describes the process of a health care provider transmitting health information to a third party to obtain authorization to provide services or a referral for services. This is analogous to how CHIACs transmit data to third-party servers to seek authorization to use that server to display or analyze information. CHIACs often transmit information to third parties, including cloud storage or computing services like AWS.[164] Just like a patient's primary care doc-

159 42 U.S.C. § 1320d-2.

160 *See* 45 C.F.R § 162.1101 (2017) (defining healthcare claims); 45 C.F.R. § 162.1102 (adopting standards for health care claims); 45 C.F.R. § 162.1201 (defining eligibility for a health plan transaction); 45 C.F.R. § 162.1202 (adopting standards for eligibility for a health plan transaction).

161 45 C.F.R. § 160.103.

162 42 U.S.C. § 1320d-2.

163 45 C.F.R. § 162.1301.

164 *See generally AWS Startup Spotlight: ReadyPulse, SmartNews, Fitbit, Sprinklr*, AWS (Apr. 2, 2015), https://aws.amazon.com/blogs/startups/aws-startup-spotlight-readypulse-smartnews-fitbit-sprinklr/ [https://perma.cc/K87Q-QPPA] (providing news about AWS powered platforms, including Fitbit, evidencing that CHIACs like Fitbit use AWS).

tor may transfer a patient's health information to their pain specialist so that the pain specialist and the primary care doctor can coordinate the patient's medications, CHIACs transfer health information to cloud computing or outside storage networks to better coordinate the patient-consumer's experience.

D. Failing to Regulate CHIACs Contravenes HIPAA

Because it is HHS's responsibility to enforce HIPAA, HHS's failure to issue new transaction regulations to cover CHIACs is arguably a failure to properly administer the statute. As discussed above, the lack of regulation of CHIACs undermines the purpose of HIPAA by failing to regulate identical copies of protected information. Furthermore, because HHS is charged by HIPAA with regulating channels of health data and CHIACs represent a large channel for such data, HHS's failure to regulate CHIACs is arguably a failure under HIPAA. In *Massachusetts v. EPA*, the Supreme Court held that EPA's failure to regulate greenhouse gases constituted a failure under the Clean Air Act because science had evolved to make it clear that greenhouse gases were "air pollutants" within EPA's regulatory jurisdiction under the Clean Air Act.[165] Because the science on greenhouse gases that existed in 2007 was more advanced that the science on which Congress relied when initially passing the Clean Air Act, the Court held that Congress's broad language ("any air pollutant") in the Clean Air Act made it clear that Congress would have included greenhouse gases had Congress been able to contemplate them at the time.[166] Similarly, while Congress could not have even considered CHIACs as an important channel of medical data when it passed HIPAA, Congress applied HIPAA to "*any* . . . person furnishing health care services or supplies"[167] who is engaged in covered transactions. This precedent makes it possible that a court would not only uphold a broad new regulation addressing CHIACs but also look negatively on HHS failing to do so.

V. Addressing Opposition to a HIPAA Expansion

CHIACs could make three main arguments against this proposed reinterpretation of HIPAA. First, they could argue that consumers actually want their data to be sold because it allows companies to provide free- or low-cost services.[168] This argument is flawed because it

165 549 U.S. 497, 528–30 (2007).

166 *Id.* at 528–29, 532.

167 45 C.F.R. § 160.103.

168 *See supra* note 24.

assumes consumers are relatively sophisticated in understanding how their data is being bartered to pay for services. The nationwide outrage and surprise following Facebook's Cambridge Analytica scandal indicates that consumers do not and would not consent to the sale of their data if fully informed.[169] While some of the outrage may be rooted in Facebook's lack of transparency about the use of consumer data, the fact that Facebook itself did not know the full extent of the breach[170] sows doubt that a regular consumer could sufficiently grasp how companies use their data to make a rational economic choice. Additionally, the lack of clear guidance about CHIACs is already having an impact on the market: despite the best efforts of HHS, consumers' and developers' lack of understanding of HIPAA's boundaries creates uncertainty in the market, influencing what software and business developers are comfortable producing and what patient-consumers are comfortable sharing.[171]

Second, CHIACs might argue that while the fiduciary duty between doctors and patients is clear, the fiduciary duty between big companies and individual patient-consumers is not, and so those relationships should not be protected in the same way. This argument fails for two reasons: (1) fiduciary duties are considered created when parties have a continuing relationship of trust,[172] and one hallmark of CHIACs is the ongoing, interactive relationship between the company and the patient-consumer; (2) the expansion of liability in tort law for data breaches indicates that companies *do* have a clear fiduciary duty to protect consumer privacy; while protecting the patient-consumer from unauthorized disclosure is not the only duty imposed by HIPAA, it supports extending regulations to CHIACs.[173]

Third, companies might argue that the FTC is the more appropriate regulatory body for achieving patient-consumer data protection because it regularly handles consumer protection cases. This is theoretically possible if the FTC were to take a more aggressive interpretation of "unfair or deceptive acts or practices" standards.[174] Still, the HIPAA approach is preferable, because coverage under HIPAA

---

169 *See, e.g.*, Nicholas Confessore, *Cambridge Analytica and Facebook: The Scandal So Far*, N.Y. TIMES (Apr. 4, 2018), https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html [https://perma.cc/J34A-Q4RS].

170 *See* Schroepfer, *supra* note 94.

171 *See* U.S. DEP'T OF HEALTH & HUMAN SERVS., *supra* note 22, at 5.

172 *See* Solow-Niederman, *supra* note 125, at 625–28.

173 *See supra* note 125.

174 15 U.S.C. § 45(a) (2012); *see* U.S. DEP'T OF HEALTH & HUMAN SERVS., *supra* note 22, at 17–18.

would result in a more uniform enforcement regime (FTC enforcement requires investigation and prosecution, whereas HIPAA would create ongoing obligations for CHIACs).[175] Furthermore, HIPAA has been a cornerstone of protecting patient-consumers over the past two decades; it makes sense to protect this evolving part of patients' lives in the same arena, under the agency with the applicable institutional knowledge.

Policymakers might argue that including CHIACs in the definition of "covered entities" would be unmanageable, that HIPAA did not and should not cover all electronic health data because it is impossible to draw the line in deciding what health data is. It is true that HHS has refused to "generally expand the scope of the rule to cover all entities that receive or maintain individually identifiable health information" and to include all "legal entities that have access to individually identifiable health information."[176] However, this proposed reinterpretation of "covered entities," would still allow HIPAA to focus on regulating the channels through which health data flows rather than on the data itself. Therefore, drawing a line between "health information" and other sensitive information is not necessary under this proposal.[177] This proposal simply reflects a modern understanding of health care and the impact of technology in creating patient-consumer driven health care. While this would result in more work for HHS, the importance of regulating CHIACs and the harms that result from failing to regulate them make it clear that administrative difficulty must be a surmountable obstacle.

Expanding "covered entities" is not the sole potential solution to the lack of regulation for CHIACs, but legislative solutions are inherently less practicable. Passage of a broader data protection bill similar to the GDPR could protect patient-consumers, but given the political climate[178] and the continuing lack of public consensus surrounding how or even if data use and privacy should be regulated,[179] a broad consumer data protection bill seems unlikely. Similarly, Congress

---

175 *See supra* Part II.

176 Standards for Privacy of Individually Identifiable Health Information; Final Rule, 65 Fed. Reg. 82,462, 82,567 (Dec. 28, 2000) (to be codified at 45 C.F.R. pt. 160, 164).

177 Notably, other countries have not shied away from broader data protection for sensitive information simply because this line is difficult to draw, resulting in more expansive protections than the proposal in this Note. *See supra* note 20.

178 *See, e.g.*, John D. McKinnon, *Partisan Rift Threatens Federal Data-Privacy Efforts*, WALL. STREET J. (Feb. 17, 2019, 12:00 PM), https://www.wsj.com/articles/partisan-rift-threatens-federal-data-privacy-law-11550422831 [https://perma.cc/386T-NN3E].

179 *Compare* Marty Swant, *Andrew Yang Proposes Digital Data Should be Treated Like a Property Right*, FORBES (Oct. 1, 2019, 4:27 PM), https://www.forbes.com/sites/martyswant/2019/

could amend HIPAA to include a private right of action, but like passage of a broader data protection bill, this is both unlikely to occur and more likely to balloon CHIACs' responsibilities than by reinterpreting HIPAA.

Conclusion

As patient-consumers take a more active role in their individual health care, sensitive health information is increasingly vulnerable. To better protect patient-consumers, provide increased certainty for companies, and accomplish the patient privacy goals inherent in HIPAA, HHS should adopt the transactional regulations necessary to incorporate CHIACs into HIPAA. HHS has the statutory authority to issue these standards and incorporate CHIACs into HIPAA under the "health provider" category. This broader rule would take advantage of HHS's existing institutional knowledge regarding sensitive health-related data and provide crucial privacy and security regulation.

10/01/andrew-yang-proposes-digital-data-should-be-treated-like-a-property-right/#c8b0f483ab7d [https://perma.cc/5U22-SU4M], *with* Melendez & Pasternack, *supra* note 42.