Hastings Business Law Journal

Volume 15
Number 2 *Summer 2019*

Article 5

Summer 2019

The Future is Femtech: Privacy and Data Security Issues Surrounding Femtech Applications

Celia Rosas

The Future is Femtech: Privacy and Data Security Issues Surrounding Femtech Applications

Celia Rosas[*]

I. INTRODUCTION

The year is 2264 and the bracelet on your wrist flashes a white light. You hardly flinch. In under twenty seconds, a small capsule dispenses from a cylinder above your desk. You grab it without giving it much thought. In it lies a pill and a small note. When you read the note, you are reminded of a distant childhood memory of when your second-grade class sampled a 'Chinese fortune cookie' as part of Interplanet History Day at your virtual school. You vividly remember your excitement upon seeing the fortune paper inside the cookie which was quickly met with confusion as you read, "A good way to keep healthy is to eat more Chinese food."[1] Food no longer exists. You are accustomed to only ingesting synthetic tablets manufactured to specifically maintain your body's vitals and nutrient levels. This time, your note reads "ergocalciferol + ferrous sulfate." You realize your body must be experiencing vitamin D and iron deficiencies in response to the hormonal imbalance caused by your monthly cycle. You ingest the pill and the white light on your bracelet turns off.

While the above futuristic scenario seems all too implausible, emerging technologies addressing women's health are on the rise.[2] Female Technology, colloquially referred to as Femtech[3] in the technology and

---

* Celia Rosas is a law student at the University of California, Hastings College of the Law. She extends tremendous thanks to: Professor Jennifer Dunn for helpful comments; Alexander Bastian and Maxwell Szabo for mentorship with policy drafting and the legislative process; and Anthony Isola for feedback and support during the writing process.

1. *Fortune Cookie Message Archive*, FORTUNE COOKIE MESSAGE, http://www.fortunecookiemessage.com/archive.php [perma.cc/3MFY-2T8B].

2. Berenice Magistretti, *The rise of femtech: women, technology, and Trump*, VENTURE BEAT (Feb. 5, 2017, 10:03 AM), https://venturebeat.com/2017/02/05/the-rise-of-femtech-women-technology-and-trump/ [perma.cc/LVA8-V78L].

3. The term "Femtech" was coined by Ida Tin, co-founder of the fertility-tracker *Clue* who states on her blog, "an enormous range of technology innovations such as temperature patches, insertable devices, wristbands, clip-ons, smart jewelry, DNA testing related to fertility and many other devices and data analytics helping people figure out their female health . . . addressing female health needs through technology: femtech." Ida Tin, *The Rise of a New Category: Femtech*, CLUE (Sept. 15, 2016), https://helloclue.com/articles/culture/rise-new-category-femtech [https://perma.cc/ECC8-JY89].

health industry, is one of the largest growing sectors catching the eyes of venture capitalists[4] and entrepreneurs alike. What was largely an ignored health area, is now a feeding ground for investors who realize the market potential of Femtech[5] because nearly half of the globe is female.[6] In 2015, the digital health industry as a whole raised $5.8 billion from investors, $82 million of which was invested into nine Femtech companies.[7]

Femtech is a term applied to a category of software, diagnostics, products, and services that use technology to focus on women's health.[8] The Femtech industry is comprised of digital or standard health tools focusing on fertility solutions, period-tracking, pregnancy and nursing care, women's sexual wellness, and reproductive system health care.[9] Products currently on the market range from *Elvie's* pelvic-floor strengthening device,[10] to period-tracking apps like *Clue*[11] and *Glow.*[12] The Femtech industry also includes products like *L.*'s organic cotton tampons and chemical-free, bioethical condoms.[13]

Recall the futuristic yet-all-too-plausible scenario described at the beginning of this introduction? A bracelet triggered the release of a pill to assist the woman in regulating her health vitals. Such a technology can only exist to the extent it analyzes the woman's personal health status in real time. While a bracelet that monitors and dispenses personalized health vitamins has yet to launch, similar technologies regulating female health are currently on the market. Many of the technologies available include a

4. *Id.*

5. Jill Richmond, *The New Year Of Optimism For Femtech*, FORBES (Dec. 31, 2016, 5:55 PM), https://www.forbes.com/sites/jillrichmond/2016/12/31/the-new-year-of-optimisim-for-femtech/#1f7d7dcc54c9 [perma.cc/BGF4-YUAP].

6. The World Bank estimates the female population is roughly 49.5 percent of the world's total population, based on age and sex distributions of UN World Population Prospect countries. THE WORLD BANK, https://data.worldbank.org/indicator/SP.POP.TOTL.FE.ZS [perma.cc/4UBW-EFBM].

7. Richmond, *supra* note 5.

8. *See generally* Mona Fromm, *The Femtech Revolution*, HANDELSBLATT GLOBAL (Mar. 4, 2017, 2:00 PM), https://global.handelsblatt.com/companies-markets/the-femtech-revolution-713865 [perma.cc/Z23K-HNLZ]; *see* Heather Mack, *Clue Gets $20M to Enhance Intelligence of Period-Tracking App, Grow Team*, MOBIHEALTH NEWS (Nov. 30, 2016), http://www.mobihealthnews.com/content/clue-gets-20m-enhance-intelligence-period-tracking-app-grow-team [perma.cc/B4LQ-ZA65].

9. *See generally* Heather Mack, *In-Depth: Digital Health Innovation In Fertility and Women's Health- Not So Niche Anymore*, MOBIHEALTH NEWS (Dec.22, 2016), https://www.mobihealthnews.com/content/depth-digital-health-innovation-fertility-and-womens-health-%E2%80%93-not-so-niche-anymore [perma.cc/3XPQ-H8M4].

10. *Elivie Trainer*, https://www.elvie.com/shop/elvie-trainer [perma.cc/4NHJ-XRSZ].

11. CLUE, https://www.helloclue.com/ [perma.cc/R46K-UVTD].

12. GLOW, https://glowing.com/ [perma.cc/4A2N-RG3A].

13. *L.*, https://thisisl.com/ [perma.cc/2V54-NNJW].

device synced to a companion mobile application[14] or involve only the singular use of a mobile application.[15] When a user first begins using the device and companion mobile application, the user is prompted to input personal information into the mobile application which can range from name and age to more personal information like health history. The mobile application is an integral feature of these health technologies because the mobile application stores, analyzes, and provides the user with personalized reports of her health status.

Of the most popular Femtech products currently on the market is the *Elvie Trainer*. *The Elvie Trainer*, an "award-winning Kegel trainer for a stronger pelvic floor" visualizes a woman's pelvic floor movements in real time and provides biofeedback accessible through a companion mobile application[16] to "strengthen [a woman's] pelvic floor muscles for fewer leaks within weeks."[17] Typically, kegal strengthening includes "clench-and-release" exercises of pelvic floor muscles that improve or eliminate bowel and bladder leakage.[18] Women who suffer from incontinence—the inability to control one's bladder resulting in urinary leaks—after giving birth, often engage in pelvic floor strengthening exercises.[19] The *Elvie Trainer* provides women with a more sophisticated and high-tech alternative to targeting these muscles through its Elvie Trainer device and companion mobile application.

To begin, a user simply needs to purchase the Elvie *Trainer* kegal and register as a user on the *Elvie* mobile application. The user then turns the kegal device on and places the small, silicone device inside her vagina. She then connects to the mobile application to begin workouts that target her pelvic floor muscles. Motion and force sensors are part of the device's design that sync with the mobile application to track the user's progress

14. The *Sonata* Smart Breast Pump is a double-electric breast pump that pairs with a companion application, the MyMedela app. Through the MyMedela app, users can directly access International Board Certified Lactation Consultants and view statistical data collected from the breast pump device. SONATA SMART BREAST PUMP, http://www.medelabreastfeedingus.com/products/905/sonata-smart-breast-pump#tabs-horizontal1 [perma.cc/59Y7-PGTT].

15. *Clue* is a fertility tracker application that operates without a companion device. *Clue*, https://www.helloclue.com/ [perma.cc/R46K-UVTD]. The application relies on a user to provide personal information and continually input information about her health and body including any period-related symptoms, descriptions of bodily fluids, or any changes she notices.

16. *Elvie*, https://www.elvie.com/shop/elvie-trainer.

17. Elvie, https://www.elvie.com/ [perma.cc/BJ5Y-BPD9].

18. NATIONAL ASSOCIATION FOR CONTINENCE, https://www.nafc.org/kegel/ [perma.cc/3WU5-G2F4] [hereinafter NAFC].

19. WEBMD, https://www.webmd.com/urinary-incontinence-oab/womens-guide/bladder-control-menopause#1 [perma.cc/5SHN-FN3R].

and provide her with personalized analytics.[20] The application allows the user to freely provide personal data but personal data may also be collected automatically when using the application. Personal data includes the user's name, contact information, geographic position and workout data. The Privacy Policy detailed in the company's Terms and Conditions makes clear that "[f]ailure to provide certain Personal Data may make it impossible for this Application to provide its services."[21]

Kindara, a fertility-tracking application offers to help a woman "[g]et pregnant faster, avoid pregnancy naturally, or better understand [her] body with the world's most powerful and useful fertility charting system."[22] As a fertility solution that can operate on analytics calculated solely through the application, the application requires the user to input personal data at the onset of use. Personal data includes details surrounding the user's cervical fluids, menstruation, sex and health-related history. *Kindara*'s Privacy Policy acknowledges the sensitivity of some of this information and advises the user to "choose carefully regarding whether and if [she] will use the Service."[23]

Glow, Inc., an ovulation and health-tracking application, boasts its "powerful ability to crunch vast amounts of data to investigate the science behind . . . menstruation, sex, fertility, pregnancy, parenthood, and beyond."[24] The application indicates that "the more data [entered], the more accurate [the] predictions."[25] *Glow*'s Privacy Policy states that personal data such as name, gender, and contact information will be collected at the onset of registration with the application. The Privacy Policy also provides that the application will allow the user to input individualized data which "include[s] sensitive personal data about personal health issues and/or information related to . . . past, present, or future physical or mental health condition[s]."[26] Importantly, and distinct from the aforementioned health applications, *Glow* displays a HIPAA Complaint notice on its website.[27]

The significant commonality between the applications described above and many others on the market, is the applications' reliance on users' personal health information. The disclosure and use of personal health

20. *Id.*

21. Terms and Conditions, Privacy Policy, *Elvie* Mobile Application (last updated Jan. 22, 2016) [https://perma.cc/6VEN-2FUC], [perma.cc/488W-JRUG].

22. *Kindara*, https://www.kindara.com/ [perma.cc/6V5E-C7MG].

23. Kindara Terms of Use, KINDARA [perma.cc/VFR2-FPN9].

24. *About Glow*, GLOW, https://glowing.com/about [perma.cc/5SGA-R5UQ].

25. *Glow*, https://glowing.com/glow [perma.cc/GSA6-FBEU].

26. *Glow Privacy Policy*, GLOW, https://glowing.com/privacy [perma.cc/82FN-A98R].

27. *Id.*

information is met with promises to better provide users with more accurate personalized data. In effect, much of the personal health information stored on these applications is collected freely and automatically because users are encouraged to disclose such information.[28]

Under HIPPA, "protected Health Information" ("PHI")[29] defines what types of personal health information covered entities are required to protect. The definition of PHI is a focal point for regulation of related digital health information. A question of law exists as to whether the personal health information collected, stored and used by Femtech applications, should fall under the definition of PHI and consequentially be subject to federal regulation and oversight. For the reasons set forth in this paper, privacy and data security regulations concerning personal health information must be amended to protect users of Femtech mobile applications because current laws do not regulate Femtech mobile applications. Specifically, the Health Insurance Portability and Accountability Act ("HIPAA") must be amended to minimize the potential data and privacy risks associated with Femtech technologies.

II. THE PROBLEM–WHY FEMTECH PRODUCTS AND ITS LACK OF REGULATION ARE OF GROWING CONCERN

Femtech companies who collect and store personal health data often fall outside the purview of HIPAA.[30] While subject to Federal Trade Commission Act ("FTC Act") regulations,[31] Femtech companies are largely left unregulated on a federal level as it pertains to privacy and data security requirements regarding PHI. Of the emerging Femtech companies, most of them do not fall under the Code of Federal Regulation's definition of a covered entity.[32] This exposes Femtech application users to a myriad of privacy and data security issues. Expansion of HIPAA's covered entity definition is of recent rhetoric[33] as a greater number of mobile health ("mHealth") applications continue to emerge.[34] Proposed solutions include

28. *See* NAFC, *supra* note 18.

29. *What is PHI?*, U.S. DEP'T OF HEALTH & HUMAN SERVICES, https://www.hhs.gov/answers/hipaa/what-is-phi/index.html [perma.cc/Q3AQ-E4HJ].

30. 45 C.F.R § 160.103 (2014).

31. 15 U.S.C. § 45 (2006).

32. 45 C.F.R § 160.103 (2014).

33. *See generally* Jamie Lynn Flaherty, *Digital Diagnosis: Privacy and the Regulation of Mobile Phone Health Applications*, 40 AM. J.L & MED. 416 (2014); *see also* Nicholas P. Terry, *Regulatory Disruption and Arbitrage in Health-Care Data Protection*, 17 YALE J. HEALTH POL'Y L. & ETHICS 143 (2017).

34. *See* Peter McLaughlin & Melissa Crespo, *The Proliferation of Mobile Devices and Apps for*

a broad sweeping of mHealth applications under HIPAA's covered entity definition.[35] However, such a broad proposal unnecessarily burdens all Femtech mobile health companies, regardless of the technology invented or the amount of personal health information collected and stored. Covered entities must be redefined to include Femtech applications that are synced to 'biosensing products'[36] and applications that provide similar analytics. A distinction must be made between certain Femtech products and services that analyze highly personal information often measured by body-invasive devices and Femtech applications that offer simple tracking services. In drawing this distinction, the regulations imposed on simple Femtech applications will be lessened and allow such applications to more freely enter the market because of the less stringent regulations that are in place. Therefore, only sophisticated, high-tech devices and their companion applications that collect personal health information will be subject to HIPAA regulations.

However, HIPAA reform should not rely solely on expanding the definition of HIPAA's "covered entities" because such a solution does not adequately address the implications of an ever-changing technological landscape. Rather, reform should also focus on updating industry standards as it relates to physical and technical safeguards mandated under HIPAA. Specifically, encrypted data need not be a solution a company can elect to comply with but, instead, be a required measure that Femtech and similar mHealth applications must implement to ensure encrypted data becomes the "commercially-reasonable standard." This will ensure that technical safeguard requirements under HIPAA more accurately reflect modern technologies to better protect Femtech mobile application users.

A. CURRENT FEMTECH COMPANIES' PRIVACY POLICIES ARE INADEQUATE AND EXPOSE USERS TO POTENTIAL DATA BREACHES

The notion that consumers who voluntarily use products and services are thereby impliedly consenting to the policies in place by such companies is not novel.[37] The FTC Act plays a large role in ensuring that consumers

Healthcare: Promises and Risks, BLOOMBERG BNA (May 21, 2013), http://about.bloomberglaw.com/practitioner-contributions/the-proliferation-of-mobile-devices-and-apps-for-health-care-promises-and-risks/ [perma.cc/E27R-ZY8T].

35. Flaherty, *supra* note 33.

36. The term "biosensor" is short for "biological sensor" which is defined as "chemical sensing device in which a biologically derived recognition is coupled to a transducer, to allow the quantitative development of some complex biochemical parameter." Sally Robertson, *What are Biosensors?* (Feb. 26, 2019) https://www.news-medical.net/health/What-are-Biosensors.aspx [perma.cc/4S3G-ZDX6].

37. This notion does not run afoul from the concept that policy terms must not be inconspicuous

are made aware of company practices and acts, or at the very least, that customers are not misled about deceptive practices.[38] Because current Femtech mobile applications are unregulated, privacy and data security practices are left to the discretion of the company.

Ava, for example, a fertility tracking bracelet and companion application that offers insight about fertility, pregnancy and female health,[39] states the company has "implemented commercially reasonable procedural, physical and technical safeguards to protect [a user's] personal information against loss, theft or alteration as well as unauthorized access and disclosure."[40] The Privacy Policy details its data storing and processing practices which indicates that "information is stored and processed on servers located in the [US], either by [Ava] or by a third party . . . such as Amazon Web Services, or in any other country in which Ava or its service providers may operate."[41]

Flo, a period tracking application that "uses artificial intelligence for the most accurate menstrual cycle predictions,"[42] states it takes "commercially reasonable measures to protect all collected information"[43] but further indicates that it "cannot guarantee the security of the [application]."[44] Unlike *Ava*, *Flo's* Privacy Policy does not disclose the company's data storing and processing practices.

After a comparison of *Ava*, *Flo*, *Elvie*, *Kindara*, and *Glow*'s privacy policies, it is apparent *Glow* is the only company with a privacy policy that prominently identifies the company's satisfactory HIPAA compliance.[45] Unlike the other companies, *Glow* is considered a "business associate" under HIPAA's covered entity definition because *Glow* offers users the ability to elect into the "Glow Fertility Program Patient Services

and must provide the user with reasonable notice. *See* Vernon v. Qwest Communs. Int'l, Inc., 857 F. Supp. 2d 1135, 1149 (D. Colo. 2012).

38. 15 U.S.C. § 45 (2006).

39. AVA, https://www.avawomen.com/ [perma.cc/CRJ3-5EU8].

40. *Ava Privacy Policy*, AVA, https://www.avawomen.com/privacy/ [perma.cc/WN26-BJJT].

41. *Id.*

42. FLO, https://flo.health [perma.cc/P934-WEJY].

43. *Privacy Policy*, FLO, https://flo.health/privacy-policy [perma.cc/44SY-RU29].

44. *Id.*

45. GLOW, https://glowing.com [perma.cc/GSA6-FBEU] ("HIPAA Compliant" emblem on the bottom right of the homepage). HIPAA does not provide a certification indicating that a company or organization is fully compliant. A "HIPAA" certification solely means that a person or persons of the company have "successfully undergone a course designed to train and teach . . . the information . . . [needed] to enable [a] business or organization to become HIPAA compliant." HIPAA certifications are issued by many online courses. *HIPAA Compliance Tools*, https://www.hipaacomp liance.org/hipaa-certified/ [perma.cc/BQ3T-9XPC].

Agreement" ("Fertility Program").[46] *Glow's* Fertility Program enables *Glow* to "act as a conduit between (a) health care providers offering fertility-related services, [and] (b) other persons involved in the arranging, provision or financing of health care services."[47] As "business associate," *Glow* is therefore required to comply with HIPAA. To comply with HIPAA, *Glow* explicitly discloses that it "maintain[s] physical security measures to guard against unauthorized access to systems and use[s] safeguards such as firewalls and data encryption."[48] No other privacy policy makes references to data encryption.[49]

Although these case studies are merely a sample, they provide ample color as to the commercially reasonable safeguards Femtech companies choose to employ. Most often, encryption as a means of data security falls wayside to other technical safeguards such as utilization of secure servers. This is presumably attributed to cost and other extenuating circumstances.[50] The HIPAA Security Rule defines technical safeguards as "the technology and the policy and procedures for its use that protect electronic protected health information and control access to it."[51] Covered entities may essentially "use any security measure that allow [them] to reasonably and appropriately implement the necessary standard for protection."[52] Covered entities are required to encrypt PHI during data transmission but can choose the type of encryption and whether such data will remain encrypted thereinafter.[53] Femtech mobile applications, on the other hand, are free to employ any security measure as the company so chooses—which includes not implementing any sort of security measure.

Such lenient standards result in inadequate privacy and data security protection for Femtech mobile users. A prime example of this problem is *Yahoo! Inc's.* ("*Yahoo*") recent data breaches. As an e-mail and internet service provider, *Yahoo* collects and stores individuals' personal information (much like Femtech mobile applications) ranging from an individual's contact information to credit card and social security

46. *Privacy Policy*, GLOW, https://glowing.com [perma.cc/82FN-A98R].

47. *Id.*

48. *Id.*

49. This determination is made in reference to a blind sample I conducted of seven Femtech Applications currently on the market.

50. Elizabeth Snell, *HIPAA Technical Safeguards: A Basic Review*, HEALTHIT SECURITY (Nov. 11, 2014), https://healthitsecurity.com/news/hipaa-technical-safeguards-basic-review [perma.cc/7D7T-SWGX].

51. Snell, *supra* note 50; *see generally*, *The Security Rule*, HEALTH INFORMATION PRIVACY https://www.hhs.gov/hipaa/for-professionals/security/index.html [perma.cc/QDK2-B63W].

52. Snell, *supra* note 50.

53. *Id.*

identification. An examination of *Yahoo's* recent data breaches highlights the catastrophic consequences to users' privacy because of outdated technical safeguards implemented under inadequate and lenient laws.

B. AN EXAMINATION OF *YAHOO!, INC.'S* UNENCRYPTED DATA BREACHES ILLUSTRATES THAT POTENTIAL DATA BREACHES ARE LIKELY TO OCCUR AMONG FEMTECH MOBILE APPLICATIONS.

In a putative class action against Defendant *Yahoo*, Plaintiffs alleged because of *Yahoo*'s history of data security failure between 2014-2015, *Yahoo* should have been put on notice (prior to the third data breach in 2016 that led to this lawsuit) of the need to enhance their data security.[54] Plaintiffs specifically alleged that *Yahoo* "fail[ed] to cryptographically store the passwords in its database."[55] Plaintiffs proffered evidence to support *Yahoo*'s deliberate decision to not encrypt their user data, as former *Yahoo* security staffers interviewed said requests made by *Yahoo*'s security team for new tools and features, such as strengthened cryptography protections were rejected on the grounds that the requests were too costly, complicated, or were simply too low a priority.[56]

This demonstrates the inherent tensions that arise when companies are too free to decide the ways in which they will implement security measures. While the Northern District Court of California has yet to issue a final judgment on the merits, the parties have entered into a preliminary settlement agreement in which the court relies on Plaintiffs' expert Mary Frantz's 92-page report regarding *Yahoo*'s data security.[57] "The report shows repeated failures to follow industry-standard security practices, extensive knowledge of ongoing security breaches beginning in 2008 with failure to adequately respond, failure to provide adequate staffing and training, and failure to comply with industry standard regulations."[58] but if the allegations are true, issues surrounding the efficacy of companies' privacy and data security policies are of harrowing concern.

54. *In re Yahoo!* Inc. Customer Data Sec. Breach Litig., 313 F. Supp. 3d 1113 (N.D. Cal. 2018) the case has yet to proceed to adjudication on the merits of the case.

55. *In re Yahoo!* Inc. Customer Data Sec. Breach Litig., No. 16-MD-02752-LHK, 2017 WL 3727318, *2 (N.D. Cal. Aug. 30, 2017).

56. *Id.* at *2.

57. As of March 3, 2019, the United States District Court for the Northern District of California, San Jose Division denied the parties' preliminary class action settlement agreement. *In re Yahoo!* Inc. Customer Data Sec. Breach Litig., No. 16-MD-02752-LHK, 2019 WL 387322,*5 (N.D. Cal. Jan. 30, 2019).

58. *Id.*

Of noteworthy mention is at the time the *Yahoo* breaches took place, *Yahoo*'s Privacy Policy stated the company adopted "commercially reasonable standards," similar to the privacy policies of current Femtech applications.[59] This indicates that either *Yahoo* failed to meet modern commercially reasonable standards or that industry-wide, commercially reasonable standards are insufficient guarantees of security, and therefore, the industry as a whole needs stricter regulations. Publicly available company privacy policies therefore present a myriad of issues surrounding the validity, efficacy and veracity of company privacy practices. Companies must be held accountable for failure to comply with industry standard regulations and evermore, for flagrantly disregarding such standards.

The Femtech industry faces impending data breaches similar to that of *Yahoo*'s. With the rise of Femtech technology, comes an even greater risk of industry-wide privacy and data protection issues.[60] Femtech companies adopt commercially reasonable standards when it comes to privacy and data security. But by current law, Femtech mobile applications are left unregulated because the laws in place are constructed in such a way that Femtech companies need not comply with any sort of security or data privacy requirements. There is no legal requirement for companies to implement updated and adequate privacy and data safeguards nor is there any recourse for companies that fail to adopt "commercially reasonable standards." Therefore, stricter privacy and data security regulations surrounding PHI are necessary now more than ever, specifically as it relates to Femtech mobile applications.

III. LEGAL ANALYSIS: THE CURRENT STATE OF THE LAW IS INADEQUATE BECAUSE IT DOES NOT ADDRESS PHI AS IT RELATES TO FEMTECH MOBILE APPLICATIONS

Much of the problem surrounding Femtech privacy and data security issues pertains to the fact that the personal health information collected, stored, and analyzed by Femtech mobile applications qualifies as PHI yet is unregulated. Protected Health Information is defined in Title 45 of the Code of Federal Regulations, Section 160.103 as "individually identifiable health. . . that is transmitted by electronic media; maintained in electronic

59. *In re Yahoo!*, 2017 WL 3727318 at *2.

60. Steven Roosa, *A Deep Dive into the Privacy and Security Risks for Health, Wellness, and Medical Apps*, IAPP (Apr. 6, 2015) https://iapp.org/news/a/a-deep-dive-into-the-privacy-and-security-risks-for-health-wellness-and-medical-apps/ [perma.cc/G7EF-LE74].

media; or transmitted or maintained in any other form or medium."[61] "Individually identifiable health information" is

> [I]nformation that is a subset of health information, including demographic information collected from an individual, and: (1) Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and (2) 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; and (i) That identifies the individual; or (ii) With respect to which there is a reasonable basis to believe the information can be used to identify the individual.[62]

Simply stated, PHI is "personally identifiable information in medical records, including conversations between doctors and nurses about treatments . . . [and] also includes billing information and any patient-identifiable information in a health insurance company's computer system."[63]

Femtech mobile applications encourage users to input their health history into the applications to provide more accurate analytics. Some applications encourage users to voluntarily input similar information that is listed in a patient's medical records. Due to the nature of the data collected and analyzed, the application monitors a user's health status to the same extent a physician or gynecologist would. In effect, the Femtech mobile applications and medical records often contain the same level of personal health information.

The right to privacy covers patients' medical records by requiring physicians and similar personnel to protect patients' personal health information from being disclosed or stolen.[64] Much of the intent surrounding a physician's duty to ensuring that a patient's medical records remains confidential stems from the Hippocratic Oath.[65] However, as technology advances and various mobile applications provide users with similar health metrics and analysis, so too should Femtech mobile applications be subject to similar duties of confidentiality. Therefore,

61. 45 C.F.R § 160.103 (2014).

62. 45 C.F.R § 160.103 (2014).

63. *What is Protected Health Information (PHI)?*, TRUE VAULT https://www.truevault.com/protected-health-information.html [perma.cc/S8A4-5XME].

64. *See generally* 45 C.F.R § 160 (2014).

65. Mark A. Rothstein, *The Hippocratic Bargain and Health Information Technology*, J.L. & MED. ETHICS (Spring 2010).

Femtech mobile applications that collect, store, and analyze users' personal health information should be subject to PHI regulations under Title 45 of the Code of Federal Regulations, Section 160.103.

Accordingly, Femtech mobile applications should be subjected to similar laws that regulate PHI. The Health Insurance Portability and Accountability Act ("HIPAA")[66] and the Federal Trade Commission Act ("FTC Act")[67] regulate PHI and health information to varying degrees. Thus, HIPAA and the FTC Act should regulate Femtech mobile applications as well.

A. HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT

HIPAA is a federal law that promulgates regulation of PHI by setting forth compliance requirements for data privacy and security purposes.[68] It was enacted in 1996 in response to patients' inherent privacy concerns following the medical care industry's digitization of medical records.[69] When enacted, the legislature solely addressed the prospect of healthcare providers, clearinghouses and intermediaries accessing patients' PHI, and therefore HIPAA's scope was narrowly tailored.[70] HIPAA only regulates and applies to specific entities referred to as "Covered Entities."[71]

Covered Entities[72] includes three categories of persons or entities that fall under the purview of HIPAA: healthcare providers or health care plans, clearinghouses, and business associates.[73] Examples of healthcare providers and health plans include physicians, clinics, nursing homes, health insurance companies, HMOs, and Medicaid and Medicare.[74] Clearinghouses include entities that process nonstandard health information received by another entity into a standard electronic format.[75] Examples of clearinghouses include payment systems and technology infrastructures.[76]

66. 45 C.F.R § 160 (2014).

67. 15 U.S.C. § 45 (2006).

68. 45 C.F.R § 160 (2014).

69. *The History of HIPAA & The Consequences of a HIPAA Violation*, RECORD NATIONS, https://www.recordnations.com/articles/history-hipaa/ [perma.cc/TB5W-CRBW].

70. Jamie Lynn Flaherty, *Digital Diagnosis: Privacy and the Regulation of Mobile Phone Health Applications*, 40 AM J.L & MED. 416, 423–24 (2014).

71. 45 C.F.R § 160 (2014).

72. 45 C.F.R § 160.103 (2014).

73. *Id.*

74. *Are You a Covered Entity?*, CENTERS FOR MEDICARE & MEDICAID SERVICES https://www.cms.gov/Regulations-and-Guidance/Administrative-Simplification/HIPAA-ACA/AreYouaCovered Entity.html [perma.cc/A6UD-BS4K].

75. 45 C.F.R § 160.103 (2014).

76. *Are You a Covered Entity?*, *supra* note 74.

Business associates refers to "a person or entity that performs certain functions involving the use or disclosure of PHI on behalf of, or provides services to, a covered entity."[77] Examples of business associates include a CPA firm whose accounting services to a health care provider involve access to [PHI][78] or an "independent medical transcriptionist that provides transcription services to a physician."[79] Only those persons or entities falling under the statute's definition of a covered entity" must comply with HIPAA regulations.[80]

In general, Femtech mobile applications do not fall under HIPAA's definition of a covered entity. Hence, Femtech mobile applications need not comply with HIPAA regulations. Femtech mobile applications do not fall under the first category of "physician or health care provider" because the applications are not operated by physicians or health care providers. Most Femtech companies are independent companies that create specialized technologies to serve a niche demographic—like women seeking to get pregnant naturally and without the use of in-vitro fertilization or hormones, or women addressing issues of incontinence through pelvic floor strengthening. Femtech mobile applications do not fall under the second category of "clearing houses" because they are neither payment systems nor technology infrastructures. HIPAA's business associate category is the only potential category that could sweep a Femtech mobile application under HIPAA regulation. However, Femtech companies tend to find ways to avoid such categorization.

For the most part, Femtech companies function independently from physicians or health care providers and restrict the disclosure of the information collected by the application. Some company policies state, however, that in the event a user chooses to disclose the information collected, stored, and analyzed by the application, the company will not be responsible for transmitting nor disclosing any information to a third-party, such as a physician. Such a restriction severs any cross-functioning between the Femtech mobile application and a physician or healthcare provider. This subsequently allows the company to skirt around HIPAA requirements.

Arguably the most important provisions of HIPAA's requirements are embodied in the HIPAA Administrative Simplifications Regulations.[81]

77. 45 C.F.R § 160.103 (2014).

78. *Business Associates*, HEALTH INFORMATION PRIVACY, https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/business-associates/index.html [perma.cc/3P8R-NQSV].

79. *Are You a Covered Entity?*, *supra* note 74.

80. 45 C.F.R § 160.103 (2017). *See* Flaherty, *supra* note 70 at 416; Nicholas P. Terry, *Regulatory Disruption and Arbitrage in Health-Care Data Protection*, 17 YALE J. HEALTH POL'Y L. & ETHICS 143 (2017).

81. Flaherty, *supra* note 70 at 416.

HIPAA's Privacy Rule, Security Rule, and Breach Notification Rule outline parameters for PHI disclosure and safeguards that a covered entity must implement,[82] establish patient rights pertaining to their PHI records,[83] and provide notice requirements for breaches of PHI.[84]

The Privacy Rule "sets national standards for when [PHI] may be used and disclosed."[85] Generally, disclosure of PHI requires patient authorization.[86] In limited situations, disclosure without authorization may be permitted.[87] The Privacy Rule also establishes rights that a patient may exercise to examine PHI records, obtain a paper trail of where the patient's PHI has been sent, and to request corrections.[88]

The Security Rule "requires appropriate administrative, physical and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information."[89] To meet this requirement, covered entities must "[c]onduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information."[90] An entity may then be required to implement physical[91] or technical[92] safeguards to ensure the protection of PHI. One technical safeguard addressed in the Security Rule is the implementation of encryption.[93] While not a required safeguard, "the encryption implementation specification is addressable, and must therefore be implemented if, after a risk assessment, the entity has determined that the specification is a reasonable and appropriate safeguard in its risk management of the confidentiality, integrity and availability of

82. *Id.*; *see also* The *Security Rule*, HEALTH INFORMATION PRIVACY https://www.hhs.gov/hipaa/for-professionals/security/index.html [perma.cc/QUS6-752S].

83. *The HIPAA Privacy Rule*, HEALTH INFORMATION PRIVACY https://www.hhs.gov/hipaa/for-professionals/privacy/index.html [perma.cc/AEK7-PDTR].

84. *HIPAA Basics For Providers: Privacy, Security, and Breach Notification Rules* https://www.cms.gov/Outreach-and-Education/Medicare-Learning-Network-MLN/MLNProducts/Downloads/HIPAAPrivacyandSecurityTextOnly.pdf [perma.cc/PPC9-3B3K].

85. *Id.*

86. *The HIPAA Privacy Rule*, HEALTH INFORMATION PRIVACY https://www.hhs.gov/hipaa/for-professionals/privacy/index.html [perma.cc/AEK7-PDTR].

87. Instances of required disclosures absent authorization include when the U.S. Department of Health & Human Services is undertaking a compliance investigation or review or enforcement action. *Id.*

88. *HIPPA Privacy Rule*, *supra* note 83.

89. HHS, *The Security Rule*, Health Information Privacy https://www.hhs.gov/hipaa/for-professionals/security/index.html [perma.cc/A64P-JDPQ].

90. 45 C.F.R. § 164.308(a)(1)(II)(A) (2017).

91. 45 C.F.R. § 164.310 (a)(2)(ii) (2017).

92. 45 C.F.R. § 164.312(a)(1) (2017).

93. 45 C.F.R. § 164.312(a)(2)(iv) (2017).

[PHI].”[94] An entity may choose to not implement a specification after a risk assessment but must document that determination and implement an equivalent alternative measure to meet the safeguard standard (and include documentation of the rationale for this decision).[95]

The Breach Notification Rule “requires covered entities to notify affected individuals, U.S. Department of Health & Human Services (“HHS”), and in some cases, the media, of a breach of unsecured PHI.[96] Breach notification obligations differ depending on the number of individuals affected by the breach.[97] Breach notifications must be provided without unreasonable delay.[98] Such a requirement would ensure that Femtech policies provide users with the necessary notices and affirmative action necessary after a breach. *Kindara*’s Privacy Policy, for example, merely indicates that the company “may attempt to notify [a user or] . . . may post a notice on the Website or the App”[99] in the event of a data breach. Users who do not live in a jurisdiction that otherwise provides them with the legal right to receive written notice of a data breach must notify the company to elect such protection.[100] The Breach Notification Rule requirements would resolve problematic breach notification policies that are currently in place by Femtech companies.

The Privacy Rule, Security Rule, and Breach Notification Rule are effectively meaningless as they relate to Femtech mobile applications because Femtech companies fall outside HIPPA’s purview. The most important of the three rules that pertains the Femtech mobile applications is the Security Rule. Data breaches of highly sensitive personal health information collected, stored, and analyzed by these applications should be a top of mind concern for users. However, as Femtech companies are not required to implement any specific security and data protection technical

94. *FAQ*, Health Information Privacy, https://www.hhs.gov/hipaa/for-professionals/faq/2001/is-the-use-of-encryption-mandatory-in-the-security-rule/index.html [perma.cc/PN3D-D6LB]; 45 C.F.R. § 164.312(a)(2)(iv) (2017); 45 C.F.R. § 164.312(e)(2)(ii) (2017).

95. *Id.*

96. HIPAA Basics For Providers: Privacy, Security, and Breach Notification Rules https://www.cms.gov/Outreach-and-Education/Medicare-Learning-Network-MLN/MLNProducts/Downloads/HIPAAPrivacyandSecurityTextOnly.pdf [perma.cc/X6PE-GJQE].

97. 45 C.F.R. § 164.406(a) (2017) (“[f]or a breach of unsecured protected health information involving more than 500 residents of a State or jurisdiction, a covered entity shall, following the discovery of the breach as provided in § 164.404(a)(2), notify prominent media outlets serving the State or jurisdiction”).

98. HIPAA Basics For Providers: Privacy, Security, and Breach Notification Rules, https://www.cms.gov/Outreach-and-Education/Medicare-Learning-Network-MLN/MLNProducts/Downloads/HIPAAPrivacyandSecurityTextOnly.pdf.

99. *Privacy Policy*, KINDARA, https://www.kindara.com/privacy-policy [perma.cc/6PWM-C5ZF].

100. *Id.*

safeguards, Femtech mobile application users face a high risk of data theft.

B. THE FEDERAL TRADE COMMISSION ACT ("FTC ACT")

The FTC also promulgates regulation of health information by prohibiting companies from engaging in "unfair or deceptive acts or practices in or affecting commerce."[101] Specific to companies who collect and use personal health information, companies may not mislead consumers about the companies' privacy and data security policies as it relates to collected and used personal health information.[102] The FTC Act establishes disclosure and notice requirements regarding a company's practices thereby promoting the access of information consumers have in relation to the use of their health information.[103] One way a health company can comply with the FTC Act is by not burying key facts in a privacy policy, terms of use, or HIPAA authorization form.[104] Compliance with the FTC Act can also be met by informing the consumer about the full scope of how personal health information can or will be used prior to the consumer making a material decision to send or disclose personal information.[105] Companies required to abide by the FTC Act requirements may not be subject to HIPAA compliance and vice versa.

While the FTC Act serves an important purpose by mandating that companies fully inform users of company policies, the FTC Act does not regulate the manners, mechanisms, and means of how a company's technological infrastructure must operate to ensure consumer's privacy rights are upheld. For example, the FTC Act does not outline the parameters of technological safeguards a company must implement to ensure privacy and data security remains optimal. The FTC Act, therefore, does not adequately address the risks of privacy and data breaches among Femtech mobile applications.

C. SOLUTION: HIPAA MUST BE FURTHER REFORMED TO REDEFINE "COVERED ENTITIES" AND REQUIRE COMPANIES TO IMPLEMENT ENCRYPTION AS A TECHNICAL SAFEGUARD.

Many of the risks posed by Femtech mobile application privacy and

101. 15 U.S.C. § 45 (2006).

102. *Sharing Consumer Health Information? Look to HIPAA and the FTC Act*, FED. TRADE COMM'N https://www.ftc.gov/tips-advice/business-center/guidance/sharing-consumer-health-information-look-hipaa-ftc-act [perma.cc/WT9G-VAAB].

103. 15 U.S.C. § 45 (2017).

104. FED. TRADE COMM'N, *supra* note 102.

105. *Id.*

data security issues can be addressed by expanding the definition of "covered entities" under HIPAA and by specifying certain technical safeguard requirements codified in the Security Rule.

i. HIPAA's Covered Entities Definition Should Include Femtech Applications Synced with Biosensing Devices.

Recent proposals for HIPAA reform call for a broad sweeping of mHealth applications, which would include Femtech applications, under the covered entity umbrella. However, such expansion would deter innovation and entry of Femtech and mHealth applications from entering the market. For example, simple, inexpensive applications such as step-trackers and food-log applications would be subjected to meeting an unnecessarily high, technical safeguard threshold. Instead, Femtech applications should be categorized into two distinct groups: (1) biosensing devices synced with companion applications and (2) general health trackers. Covered entities should be expanded to include the former because of the highly sensitive information collected and analyzed by such products.

Biosensors are devices that convert biological recognition element into a signal output.[106] Biosensing technologies allow for continuous physiological monitoring in a wide range of products.[107] Biosensing products include those like *Ava*, the fertility tracking bracelet, and more commonly, blood glucose biosensors for people with diabetes or other related health issues. Other biosensing products that will soon enter the market include NextGen Jane's "smart tampon."[108] This smart tampon will use biosensors to collect and analyze a woman's biological changes predictive of disease. The device will also be able to screen a woman for sexually transmitted infections.[109] Similar to current Femtech products like the Elvie Trainer, *NextGen Jane*'s 'smart tampon' and other biosensing products rely on the devices' biosensors to monitor personal health information. Their companion applications likewise store and analyze users' personal data that is collected.

These sorts of applications differ from traditional health trackers that merely log the number of steps a person takes in a day. The food a person eats at each meal would hardly constitute personal health information in

106. Malay Gandhi & Teresa Wang, *The Future of Biosensing Wearables*, ROCK HEALTH, https://rockhealth.com/reports/the-future-of-biosensing-wearables/ [perma.cc/S35Y-2AQY].

107. *Id.*

108. *NextGen Jane*, http://www.nextgenjane.com/ [perma.cc/A33H-UG8Q].

109. *Id.*

comparison to the metrics offered by a smart tampon. Traditional health logs do not store and analyze a high volume of personal data to the extent emerging biosensing products do.[110] By identifying this stark difference, regulation can better address the inherent privacy concerns among users of these two groups of Femtech applications. In turn, applications with low-privacy concerns would not need to implement technical safeguards like data encryption. This will then allow these applications to better succeed on the market because they will not need to expend resources to implement technical safeguards. Due to the advanced technology inherent in biosensing devices, it is not unreasonable to require that sophisticated products implement technical safeguards like data encryption.

States are looking to adopt privacy and data security legislation as a means to regulate emerging technologies because of the very reason that with the advent of sophisticated technologies comes the inherent expectation that heavier regulations will be imposed.[111] For example, Illinois and Texas have adopted state laws that regulate employers who collect biometric data from their employees.[112] This is in response to emerging technologies that are replacing traditional clock-in methods using time-stamp cards by replacing it with biometric identification. Biometric data includes identifying information from a person's fingerprint, voiceprint, or the scan of a person's retina, iris, face or hand.[113] Specifically, Illinois' Biometric Information Privacy Act ("BIPA"),[114] requires employers who collect biometric data to implement physical and technical safeguards pertaining to the collection, retention, and destruction of such information. While the cost of such safeguards is of relevance, state and federal legislatures anticipate the growth of technology and understand the risks that such growth poses without adequate legislative oversight.[115] Requiring employers—who wish to utilize, collect and store biometric data—to comply with BIPA regulations is of a similar essence to requiring Femtech companies—who wish to collect and store personal

110. *See generally 7 Wearables That Go Beyond Fitness Trackers and Smart Watches* ELYSIUM HEALTH (Mar. 31, 2018), https://endpoints.elysiumhealth.com/next-generation-wearables-2018-b0c8be461151 [perma.cc/7LT6-VZTV].

111. Lily Hay Newman, *Medical Devices are the Next Security Nightmare*, WIRED (Mar. 2, 2017 10:30 AM), https://www.wired.com/2017/03/medical-devices-next-security-nightmare/ [perma.cc/6K9P-MT2E].

112. Jay Hux, *Collecting Employee Biometric Data Could Prove Costly in Illinois, Society for Human Resource Management*, SOC'Y FOR HUM. RESOURCE MGMT. (Sept. 19, 2017) https://www.shrm.org/ResourcesAndTools/legal-and-compliance/state-and-local-updates/Pages/Collecting-Employee-Biometric-Data-Could-Prove-Costly-in-Illinois.aspx [perma.cc/68TC-TREU].

113. *Id*.

114. Biometric Information Privacy Act, 740 ILCS 14/15 (2017).

115. Hux, *supra* note 112.

health information—to comply with HIPAA regulations.

Employees have already begun to rely on BIPA regulations to ensure that companies who capture, collect, and store, employees' biometric data fully comply with recent laws that are in place.[116] United Airlines became one of the latest companies hit with a putative class action in November 2017 for failure to comply with BIPA regulations. United Airlines employees alleged the company failed "to inform workers in writing that their biometric data was being captured, collected, and stored."[117] Further, the plaintiffs allege that the biometric clocking systems that United Airlines has implemented puts the workers at great risk of data theft.[118] Many of these concerns mirror those of Femtech mobile users face because companies who choose to capture, collect, store, or analyze users' personal information put users at a high risk of data theft. The putative class action against United Airlines is another example of why companies must be held to a higher standard to ensure that privacy and data security risks are mitigated. Regulatory compliance provides users with adequate protection.

ii. The Accessibility of Encryption Software Merits Its Requirement under HIPAA.

While expanding the definition of "covered entity" is of paramount importance, the effects of HIPAA can only be of value if adequate security requirements are likewise adopted and enforced. Specifically, in addressing data breach concerns similar to those of *Yahoo*'s, HIPAA must be amended to require that biosensing devices and companion mobile applications implement encrypted data.

In its current form, the HIPAA Security Rule allows companies to implement various technical safeguards to protect PHI but does not mandate that companies encrypt collected data.[119] The Security Rule impliedly acknowledges the vast array of privacy and data security issues a specific company may face but the Security Rule was implemented at a time when certain technological safeguards were costly or viewed as extraneous.[120] However, technological solutions now exist that can enable every mHealth and Femtech application to meet HIPAA requirements through data encryption software.

116. Hannah Mansiel, *United Airlines Latest to be Sued Under Illinois Biometric Law*, LAW360 (Nov. 8, 2017), http://www.law360.com/articles/983384/ [perma.cc/EZN2-GKVA].

117. *Id.*

118. *Id.*

119. Snell, *supra* note 50.

120. *Id.*

Technology platforms, such as *Aptible*[121] and *Amazon Web Services* ("AWS"),[122] enable companies to more easily implement modernized technical safeguards, like cryptography. *Aptible* is specifically on a mission to bring companies in full HIPAA compliance by helping companies builds private, secure software systems. The company's goals are to transform the experience of digital health engineers and application developers while reducing the costs and impediments typically associated with integrating data encryption software.[123]

Amazon Web Services provides extensive cloud computing services including data protection and storage. *Amazon Simple Storage Service* (S3) allows a company to encrypt data either through server-side encryption or client-side encryption. This data protection includes in-transit and at-rest protection. An AWS user can select its desired services and thereby only needs to pay for whichever individual product it uses. This enables a company to customize its technology infrastructure and provides a company with inexpensive encryption options.[124]

The existence of these technologies, juxtaposed with the lack of Femtech companies' utilization of such technologies, illustrates the unwilling nature of companies to freely implement available safeguards. This exemplifies the trend of unregulated industries who typically take the less costly and more profitable approach at the expense of user protection.[125] As was the case with the telecommunications industry, only through regulation can technological safeguard standards be raised industry wide.[126] The Smartphone Bill is a prime example of such regulation.[127]

In 2014, San Francisco District Attorney George Gascon and New York Attorney General Eric Schneiderman introduced a smartphone "kill-switch" bill in response to the rise of smartphone theft. The bill required smartphone manufacturers to implement a "kill-switch" in every device that would render the device inoperable if stolen. At the time, the kill-switch, an anti-theft technology, existed but was not integrated on every

121. APTIBLE, https://www.aptible.com [perma.cc/4EDB-KXJM].

122. AMAZON WEB SERVICES, https://aws.amazon.com/ [perma.cc/C2H2-AS6Z].

123. APTIBLE, *supra* note 121.

124. AMAZON, *supra* note 122.

125. George Skelton, *Smartphone "Kill Switch" Bill Mugged by Telecom Industry*, L.A. TIMES (Apr. 30, 2014), http://www.latimes.com/local/politics/la-me-cap-kill-switch-20140501-column.html [perma.cc/88RD-F7E8].

126. Ellen Huet, *As California Kill-Switch Law Takes Effect, Smartphone Theft Already Down 32%*, FORBES (July 1, 2015) https://www.forbes.com/sites/ellenhuet/2015/07/01/as-california-kill-switch-laws-takes-effect-smartphone-theft-already-down-32/#719021ad641f [perma.cc/H5PG-HW2R].

127. *Id.*

device or if it was integrated, required the user to opt-in.[128] The telecommunications industry adamantly opposed such technology claiming it was unnecessary and an undue burden on manufacturers. However, once major telecommunications companies' hidden financial incentives were exposed, the Smartphone Bill eventually passed and mandated that all smartphones and tablets manufactured after July 2015 come equipped with a kill-switch.[129] Reports indicate a substantial decline in smartphone theft in recent years attributed to the passage of this bill.[130]

Similar outcomes can be expected by requiring Femtech and mHealth applications to use data encryption. But an important distinction exists between telecommunications manufacturing companies and Femtech companies: financial stability. Telecommunications companies were required to implement kill-switches because the technology existed and the purported financial burdens caused by such implementation were of low and questionable concern. Telecommunications companies feared a loss in revenue sales because cellphone users would no longer need to buy brand new smartphones every time theirs were stolen. Furthermore, there was minimal concern addressing these companies' increased expenditures on the actual implementation of the anti-theft technology. However, a financial concern does exist regarding Femtech and health companies' integration of encrypted data. Many of these companies are start-ups that do not have the financial prowess like that of AT&T, Sprint, and Apple. In order to promote prosperous innovation, Femtech and mHealth companies must not be stifled by undue financial burdens.

To address this concern, the law must find a fine balance between protecting users' personal health information and promoting innovation. The distinction between the information collected by two Femtech categories, biosensing devices and their companion mobile applications and simple tracking applications, balances these interests. Such a distinction best serves femtech companies' financial interests while furthering innovation because as companies develop and rely on highly-advanced biosensing devices, in congruence with companion applications, the information collected is inherently more comprehensive and personal. Therefore, it is not unreasonable to require high-tech companies who collect, store and use highly-sensitive personal information to implement high-tech safeguards. Thus, I propose, that to resolve mobile health applications' privacy and data security concerns, the law must require

128. *Id.*

129. Katy Steinmetz, *Kill Switches on Smartphones Now Mandatory in California*, TIME (Aug. 25, 2014), http://time.com/3178077/kill-switch-smartphones-mandatory-california/ [perma.cc/R2R8-364J].

130. Huet, *supra* note 126.

sophisticated Femtech companies to implement cryptography.

IV. CONCLUSION

An underlying concern addressed by requiring certain Femtech applications to implement technical safeguards such as encryption is the proposition advanced by Moore's Law.[131] Moore's Law, an axiom in the computing industry, provides that technology will double every two years.[132] Recent innovations in the Femtech and mHealth industry illustrate the accuracy of this axiom. With the speed of technological advancements comes the even greater need for reform to combat the risks posed by such technology. Technology regulations are not intended to stifle technological advancements and achievements but rather provide guidelines that foster technological growth. Regulations should be viewed as imperative because there is little use in a technology that poses exponential risks that outweigh any benefits derived from use of the technology.

In response to TrumpCare proposals, the health industry is creating technology that outweighs the risks of conservative proposals that leaves millions of Americans without adequate care.[133] Through the use of Femtech devices, the health industry is shifting and patients are taking health matters into their own hands,[134] figuratively and literally. Femtech and mHealth applications enable users to receive health care from the comfort of their own homes, without the intervention of a physician or health care provider. But as the health industry shifts from physician-focused care to technologies that enable patients to self-monitor their health, duties of confidentiality likewise shift. A patient's right to privacy and a physician's duty to keep her digital health records confidential is an extension of the Hippocratic Oath.[135] The Femtech and mHealth companies need to be held to similar, if not the same, standards and should be accountable for protecting users' privacy and data information.

To ensure that Femtech and mHealth companies are held to higher standards, these companies must be regulated. Likewise, Femtech mobile application users need adequate legal protection to rely on when companies

131. Hux, *supra* note 106.

132. *Id.*; MOORE'S LAW, http://www.mooreslaw.org/ [perma.cc/J5K5-8NZE].

133. Magistretti, *supra* note 2.

134. *Id.*

135. *See generally* Rothstein, *supra* note 65; *Hippocratic Oath*, ENCYCLOPEDIA BRITANNICA, https://www.britannica.com/topic/Hippocratic-oath [perma.cc/6JMQ-QK4J]; *The Hippocratic Oath*, PBS (Mar. 27, 2001) http://www.pbs.org/wgbh/nova/body/hippocratic-oath-today.html [perma.cc/DLA9-ZWZ9].

fail to protect their personal health information. As technology continues to advance and the metrics provided by these Femtech companies becomes of greater societal value, personal health information should continue to be appropriately protected. By expanding the definition of "covered entities" and requiring encryption as a means of ensuring technical safeguards are up-to-date, HIPAA will better serve users of Femtech mobile applications to ensure users receive the necessary protection that pertains to security and data privacy.

***