2019

Florida Law, Mobile Research Applications, and the Right to Privacy

Stacey A. Tovino, *University of Oklahoma College of Law*

FLORIDA LAW, MOBILE RESEARCH APPLICATIONS, AND THE RIGHT TO PRIVACY

STACEY A. TOVINO*

I. INTRODUCTION

This Article builds on the Author's prior work investigating the privacy and security implications of mobile application ("mobile app") mediated health research[1] conducted by "independent scientists,[2] citizen

* Stacey A. Tovino, JD, PhD, serves as the Judge Jack and Lulu Lehman Professor of Law and the Founding Director of the Health Law Program at the UNLV William S. Boyd School of Law. Professor Tovino thanks Dean Jon Garon, Professor Kathy Cerminara, and Professor Marilyn Uzdavines for the invitation to participate in *Nova Law Review's* Symposium—Progression 2018: Using Law to Facilitate an Efficacious Innovation Economy. Professor Tovino also thanks Lena Rieke, Law Library Fellow, Wiener-Rogers Law Library, UNLV William S. Boyd School of Law, for her outstanding research assistance and *Nova Law Review* for its careful editorial assistance.

1. *See* Sarah Moore et al., *Consent Processes for Mobile App Mediated Research: Systematic Review*, J. MED. INTERNET RES. MHEALTH & UHEALTH, Aug. 2017 at 3, 4 (discussing Apple's ResearchKit and Android's ResearchStack, two open source frameworks that any scientist can use to create a mobile research app); Vincent Tourraine, *List of All ResearchKit Apps*, SHAZINO: SCI. (Feb. 1, 2016), http://blog.shazino.com/articles/science/researchkit-list-apps/ (listing more than a dozen mobile research apps designed using ResearchKit); *About the Study*, MPOWER, http://parkinsonmpower.org/about (last visited May 1, 2019) (describing a mobile app mediated research study that monitors the symptoms and progression of Parkinson's disease).

2. *See* Amber Dance, *Solo Scientist*, 543 NATURE 747, 747 (2017) (reporting the story of Jeffrey Rose, an independent scientist who conducts research without the benefits of a traditional *bricks-and-mortar employer*); Carrie Arnold, *Going Rogue*, SCI. (May 17, 2013, 8:15 PM), http://www.sciencemag.org/careers/2013/05/going-rogue (reporting the story of Ethan Perlstein, an independent scientist who engages in scientific research without

scientists,[3] and patient researchers[4] (collectively, independent scientists)[5] as well as [the] mobile app developers and data storage companies that support them."[6] As background, mobile "apps are a fast-growing category of software typically installed on personal smartphones and wearable devices."[7] Used for a wide range of health-related activities, including fitness, health education, health predictions, diagnosis, health care delivery, treatment support, chronic disease management, disease surveillance, epidemic outbreak tracking, and health research, mobile apps have tremendous versatility and promise.[8]

---

university, pharmaceutical company, research institute, or government agency affiliation, and without public funding).

3. *See* Mark A. Rothstein et al., *Citizen Science on Your Smartphone: An ELSI Research Agenda*, 43 J.L. MED. & ETHICS 897, 897 (2015) (explaining that the term citizen scientist originally referred to "nonprofessionals who assist[ed] professional scientists by contributing observations and measurements to ongoing research enterprises;" also explaining that the term "now includes nonprofessionals who conduct scientific experiments of their own design independent from professional scientists;" clarifying that citizen science has been made possible by "online crowdsourcing, big data capture strategies, and computational analytics," among other technological developments); Todd Sherer, *Parkinson's Disease at 200*, SCI. AM.: BLOGS (Apr. 12, 2017), http://blogs.scientificamerican.com/guest-blog/parkinsons-disease-at-200/ (referencing technology that citizens use to participate in research investigating Parkinson's disease).

4. *See* Jenny Leese et al., *Evolving Patient-Researcher Collaboration: An Illustrative Case Study of a Patient-Led Knowledge Translation Event*, J. PARTICIPATORY MED., no. 1, 2017, at 3, 3 (discussing patient engagement in research).

5. Paul Wicks et al., *Accelerated Clinical Discovery Using Self-Reported Patient Data Collected Online and a Patient-Matching Algorithm*, 29 NATURE BIOTECHNOLOGY 411, 411–12 (2011) (analyzing data reported on a website by patient researchers with Amyotrophic Lateral Sclerosis ("ALS") who experimented with lithium carbonate).

6. Stacey A. Tovino, *Going Rogue: Mobile Research Applications and the Right to Privacy*, 95 NOTRE DAME L. REV. (forthcoming 2019) (manuscript at 4) (on file with author).

7. *See* Nicolas P. Terry & Tracy D. Gunter, *Regulating Mobile Mental Health Apps*, 36 BEHAV. SCI. & L. 136, 137 (2018) (providing background information regarding mobile health apps).

8. *See* Valerie Gay & Peter Leijdekkers, *Bringing Health and Fitness Data Together for Connected Health Care: Mobile Apps as Enablers of Interoperability*, J. MED. INTERNET RES., Nov. 2015, at 37, 37–38 (2015) (discussing fitness and health uses of mobile apps as well as the aggregation of such uses); Deborah Lupton & Annemarie Jutel, *"It's Like Having a Physician in Your Pocket!" A Critical Analysis of Self-Diagnosis Smartphone Apps*, 133 SOC. SCI. & MED. 128, 128–30 (2015) (analyzing diagnostic uses of mobile apps, including the effects such apps have on the physician-patient relationship and medical authority in relation to diagnosis); Elaine O. Nsoesie et al., *New Digital Technologies for the Surveillance of Infectious Diseases at Mass Gathering Events*, 21 CLINICAL MICROBIOLOGY & INFECTION 134, 134–35 (2015) (focusing on disease surveillance uses of mobile apps and other digital technologies); Ben Underwood et al., *The Use of a Mobile App to Motivate Evidence-Based Oral Hygiene Behaviour*, 219 BRIT. DENTAL J. 166, 166 (2015) (reporting the

This Article focuses on independent scientists, citizen scientists, and patient researchers who use mobile apps to conduct or participate in health research.[9] As background, an independent scientist—also known as a rogue or lone scientist—is an individual who engages in scientific research without university, pharmaceutical company, research institute, government agency, or other third-party affiliation.[10] A citizen scientist—also known as a community scientist, crowd scientist, or amateur scientist—is a member of the general public who engages in scientific work, often in collaboration with or under the direction of a professional, affiliated scientist and the scientist's academic or other institution.[11] Citizen scientists also include non-professionally trained scientists who independently conduct their own experiments, frequently with the assistance of mobile apps, online crowdsourcing, computational analytics, and other technologies made possible by big data.[12] A patient researcher is a current or former patient who initiates or assists research at any stage of the research process, including establishing the research agenda, designing the research protocol, collecting data, and disseminating research results.[13] Mobile apps have been tremendously helpful to independent scientists, citizen scientists, and patient researchers, as well as conventional scientists who fall outside traditional

---

results of a study assessing user perceptions of an oral health app that provides oral health education and oral health behavioral support); Sharon Parmet, *App Developed at UIC to Track Mood, Predict Bipolar Disorder Episodes*, UIC TODAY (Jan. 15, 2019, 2:32 PM), http://www.today.uic.edu/app-developed-at-uic-to-track-mood-predict-bipolar-disorder-episodes (explaining that the mobile app BiAffect "unobtrusively monitors keyboard dynamics metadata, such as typing speed and rhythm, mistakes in texts, and the use of backspace and auto-correct" and that such data is then "analyzed using an artificial intelligence-based machine learning approach to identify digital biomarkers of manic and depressive episodes in people with bipolar disorder"); Sarah Peddicord, *FDA in Brief: FDA Launches New Digital Tool to Help Capture Real World Data from Patients to Help Inform Regulatory Decision-Making*, FDA (Nov. 6, 2018), http://www.fda.gov/newsEvents/newsroom/FDAInBrief/ucm625228.htm ("announcing the MyStudies app, . . . a new mobile technology designed to foster the collection of real world evidence via patients' mobile devices" for health research and other purposes).

9. *See* discussion *infra* Parts II–IX.

10. *See* James Lovelock, *James Lovelock: We Need Lone Scientists*, INDEPENDENT: INDY/LIFE (Mar. 26, 2014, 1:00 PM), http://www.independant.co.uk/life-style/health-and-families/features/james-lovelock-we-need-lone-scientists-9215280.html (comparing affiliated scientists, who work in large corporations or for the government, with lone, or independent, scientists who work alone in their own laboratories).

11. *See* Rothstein et al., *supra* note 3, at 897; *Citizen Science*, OXFORD DICTIONARY, http://en.oxforddictionaries.com/definition/us/citizen_science (last visited May 1, 2019) (defining citizen scientist).

12. Rothstein et al., *supra* note 3, at 897 (explaining the development of the term citizen scientist).

13. *See* Leese et al., *supra* note 4, at 3 (discussing patient engagement in research).

regulation—collectively, independent scientists—in the conduct of a wide range of health research projects.[14]

As explained in the Author's other work, independent scientists who use mobile apps to conduct health research collect a wide variety of data regarding their research participants' health including, but not limited to, data regarding sexual health,[15] occupational health,[16] neurological health,[17] and cardiovascular health.[18] As one might imagine, this voluminous and diverse health data may be at risk of privacy and security breaches, leading to dignitary, psychological, and economic harms for which the mobile research participants have few legally enforceable rights or remedies due to a lack of regulation and applicable standards.[19]

In a forthcoming publication, the Author analyzes existing federal statutes and regulations designed to protect the privacy and/or security of health data, including data generated in the research context.[20] In that article, the Author shows that a variety of federal authorities, including the Health Insurance Portability and Accountability Act ("HIPAA") Administrative Simplification Rules,[21] the Common Rule,[22] and the Federal Trade

---

14. *See* Elizabeth Klemick, *Mobile Apps for Citizen Science*, SMITHSONIAN SCI. EDUC. CTR. (July 15, 2018), http://www.ssec.si.edu/stemvisions-blog/mobile-apps-citizen-science. "An abundance of mobile apps makes participation in citizen science projects easier than ever and allows data entry in the field." *Id.*

15. *See* Tovino, *supra* note 6, at 9 (discussing Kinsey Reporter, a mobile research app that collects sexual health data from research participants).

16. *See id.* at 10–11 (discussing Active Day and Fall Safety Pro, two mobile apps that collect fall data from workers, such as painters and roofers, who experience falls from height).

17. *See id.* at 11–12 (discussing Patients Like Me, a mobile app that collects all types of health data, including Parkinson's symptoms and other neurological health data, and discloses that data for research purposes).

18. *See id.* at 13 (discussing MyFitnessPal, a mobile app that collects health and fitness data and discloses that data for research purposes).

19. *See* Opperman v. Path, Inc., 205 F. Supp. 3d 1064, 1073 (N.D. Cal. 2016) (explaining that the mobile app Yelp exceeded the scope of its users' consent when it uploaded its users' contacts data without explicit permission); Mark A. Rothstein, *Ethical Issues in Big Data Health Research*, 43 J.L. MED. & ETHICS 425, 426–27 (2015) (discussing physical and dignitary harms associated with the loss of privacy in the context of big data health research); Zeynep Tufekci, *The Latest Data Privacy Debacle*, N.Y. TIMES (Jan. 30, 2018), http://www.nytimes.com/2018/01/30/opinion/strava-privacy.html (reporting the mobile exercise app Strava, which inadvertently revealed the secret locations of American military bases and service members).

20. *See* Tovino, *supra* note 6, at 16–17 (analyzing existing federal statutes and regulations designed to protect the privacy and/or security of health data).

21. *See id.* at 2–3, 16–17; Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, § 1, 110 Stat. 1936, 1936 (codified as amended at 42 U.S.C. § 201 (2012)); Health Information Technology for Economic and Clinical Health Act, Pub. L. No. 111-5, § 13001, 123 Stat. 226, 226 (2009) (codified as amended in scattered sections of

Commission Act,[23] either: (1) do not apply to mobile app mediated health research conducted by independent scientists; or (2) fail to establish comprehensive data privacy and security standards that will drive the implementation of privacy and security best practices by independent scientists.[24]

In response to these lapses in federal regulation, many academics and practitioners have suggested new federal laws or amendments to existing federal laws in an attempt to create comprehensive privacy and security standards that, once implemented, may help protect otherwise unprotected data.[25] It is not clear, however, whether the federal government has the

---

42 U.S.C.). HHS's privacy regulations, which implement section 264(c) of HIPAA, are codified at 45 C.F.R. §§ 164.500–.534 (2018). 45 C.F.R. §§ 164.500–.534 (2018). HHS's security regulations, which implement section 262(a) of HIPAA [42 U.S.C. § 1320d–2(d)(1)], are codified at 45 C.F.R. §§ 164.302–.318. *Id.* §§ 164.302–.318. HHS's breach notification regulations, which implement section 13402 of HITECH [42 U.S.C. § 17932], are codified at 45 C.F.R. §§ 164.400–.414. *Id.* §§ 164.400–.414. Collectively, the HIPAA Privacy Rule, the HIPAA Security Rule, and the HIPAA Breach Notification Rules are known as the HIPAA Administrative Simplification Rules. *See id.* §§ 164.302–.534.

22. *See* 45 C.F.R. 46.101–409 (2018); Federal Policy for the Protection of Human Subjects, 83 Fed. Reg. 28,497, 28,518 (June 19, 2018) (to be codified at 49 C.F.R. pt. 11) (showing changes to HHS's Common Rule with which compliance is required by July 21, 2019); Mark A. Rothstein, *Currents in Contemporary Ethics: Research Privacy Under HIPAA and the Common Rule*, 33 J.L. MED. & ETHICS 154, 155 (2005) (explaining the application of the Common Rule).

23. *See* 15 U.S.C. § 45(a)(1) (2012). "Unfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce, are hereby declared unlawful." *Id.*

> The FTC has brought legal actions against organizations that have violated consumers' privacy rights, or misled them by failing to maintain security for sensitive consumer information . . . [i]n many of these cases, the FTC has charged the defendants with violating Section 5 of the FTC Act, which bars unfair and deceptive acts and practices in or affecting commerce.

Privacy and Security Enforcement, FTC, http://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/privacy-security-enforcement (last visited May 1, 2019).

24. *See* FLA. STAT. § 501.171(1)(b) (2018); Sharona Hoffman, *Citizen Science: The Law and Ethics of Public Access to Medical Big Data*, 30 BERKELEY TECH. L.J. 1741, 1746 (2015); Tovino, *supra* note 6, at 15 (discussing the application of these federal authorities in detail and noting which apply and which contain privacy and security standards).

25. *See* David W. Bates et al., *Health Apps and Health Policy: What Is Needed?*, 320 JAMA 1975, 1975 (2018). "The FDA also needs to review apps specifically with respect to safety, protection of privacy, and false claims." *Id.* "[I am] sure there will be some major breaches that just might push the drive for national legislation over the top." James Swann, *That Apple Watch May Show Hackers Your Heart's Health*, BLOOMBERG L.: HEALTH L. & BUS. (Oct. 18, 2018, 6:15 AM), http://www.bloomberglaw.com/health-law-and-business/that-apple-watch-may-show-hackers-your-hearts-health [hereinafter *Apple Watch*] (quoting a prominent health care attorney); James Swann, *Video: Your Fitbit Steps May Not*

desire or capacity to enforce expanded or new laws in this area.[26] In an earlier publication, the Author found that a consumer complaint involving a violation of the HIPAA Administrative Simplification Rules has a 0.1% chance of triggering a government-imposed settlement or civil money penalty.[27] In that same article, the Author showed that in those few cases that go to settlement or penalty, the federal government takes a significant amount of time—more than seven years in some cases—to execute the settlement agreement or to impose the civil money penalty.[28] The Author concluded that the federal desire and/or capacity to enforce the HIPAA Administrative Simplification Rules is low, resulting in a lack of timely attention to the privacy and security rights of individuals.[29]

This Article furthers the line of research by investigating whether state law contains comprehensive privacy, security, and breach notification standards that could apply to independent scientists who conduct mobile app mediated health research.[30] Focusing only on Florida law, this Article assesses potentially relevant and applicable sources of privacy, security, and breach notification standards for health data of the type obtained during mobile app mediated health research studies.[31] This Article concludes that, with one exception, Florida law tends to fall into one of two categories: (1) the law contains at least one data privacy, security, or breach notification standard, but the standard is limited in application to certain actors, certain professions, or certain institutions and the law does not apply to independent scientists,[32] or (2) the law is not necessarily limited in application, but the law fails to establish comprehensive privacy, security, and breach

---

Be Protected by Federal Law, BLOOMBERG L.: NEWS (May 30, 2018), www.bna.com/video-fitbit-steps-n57982093031/ [hereinafter *Fitbit*]. "[It is] almost certain that the federal government will look to regulate health information [that is] not subject to HIPAA . . . ." *Fitbit, supra.*

26. *See* Sarah Fellay, *Changing the Rules of Health Care: Mobile Health and Challenges for Regulation*, AM. ENTERPRISE INST.: TECH & INNOVATION (Aug. 4, 2014), http://www.aei.org/publication/changing-the-rules-of-health-care-mobile-health-and-challenges-for-regulation/.

27. Stacey A. Tovino, *A Timely Right to Privacy*, 104 IOWA L. REV. (forthcoming 2019).

28. *Id.*

29. *See id.*

30. *See* discussion *infra* Part X.

31. *See* discussion *infra* Part X; Tovino, *supra* note 6, at 9–10, 12–13 (providing several examples of health data collected by mobile research apps).

32. FLA. STAT. §§ 282.318, 381.026, 395.001, 408.051, 456.003 (2018); *see also* FLA. CONST. art I, § 23.

notification standards that will drive the implementation of privacy and security best practices by independent scientists.[33]

As discussed in more detail below, Florida laws that fall into the first category include the Florida Constitution,[34] Florida's health institution licensing laws,[35] Florida's health professional licensing laws,[36] the Florida Electronic Health Records Exchange Act ("Health Records Act"),[37] the Florida Information Technology Security Act ("Florida ITS Act"),[38] and the Florida Patient's Bill of Rights and Responsibilities ("Patient Bill of Rights").[39] Florida laws that fall into the second category include the Florida Information Protection Act ("FIPA")[40] and Florida common law.[41] This Article concludes that FIPA, which contains data security and breach notification standards that will apply to some—but not all—independent scientists who conduct mobile app mediated research, is the best option for protecting mobile app mediated research data going forward.[42] This Article proposes amendments to FIPA that are designed to protect the privacy and security of all big data subjects, including mobile app mediated health research participants.[43]

II. THE FLORIDA CONSTITUTION

Article I, Section 23 of the Florida Constitution provides: "Every natural person has the right to be let alone and free from governmental intrusion into the person's private life except as otherwise provided herein."[44] Although the Florida Supreme Court has stated that the phrase *natural person* includes all Floridians, even minors and individuals who are incompetent, the phrase *governmental intrusion* makes clear that the Florida Constitution only protects individuals against governmental—not private—intrusions.[45] Although mobile app mediated research certainly can be

33. *See* FLA. STAT. § 501.171; *Florida Common Law*, WITHOUT MY CONSENT, http://www.withoutmyconsent.org/50state/state-guides/florida/common-law# (last visited May 1, 2019).

34. *See* FLA. CONST. art. I, § 23.

35. *See* FLA. STAT. § 395.001.

36. *See id.* § 456.003.

37. *See id.* § 408.051.

38. *See id.* § 282.318.

39. *See id.* § 381.026.

40. *See* FLA. STAT. § 501.171.

41. *See Florida Common Law*, *supra* note 33.

42. Discussion *infra* Part X; *see also* FLA. STAT. § 501.171.

43. Discussion *infra* Part X; *see also* FLA. STAT. § 501.171.

44. FLA. CONST. art. I, § 23.

45. *Id.*; *In re* Guardianship of Browning, 568 So. 2d 4, 12 (Fla. 1990) (in the context of a request for the discontinuation of medical treatment with respect to individuals

conducted by an agent of the Florida—or any other—government,[46] this Article focuses on private health research conducted or facilitated by mobile apps such as: Kinsey Reporter;[47] Active Day;[48] Patients Like Me;[49] and My Fitness Pal.[50] Described in detail in the Author's prior work,[51] these apps are neither sponsored, supported, nor affiliated with any governmental agency or agent thereof.[52] As a result, the Florida Constitution is inapplicable to the issue on which this Article focuses.[53]

Assuming for the moment that the Florida Constitution did apply to mobile app mediated research conducted by private, independent scientists, Floridians do have a constitutionally protected interest in their health-related data.[54] However, neither the Florida Constitution nor its interpretive case law sets forth particular privacy, security, and breach notification standards that could help protect that data, or that could minimize the risk of an

---

who are incompetent); *In re* T.W., 551 So. 2d 1186, 1193 (Fla. 1989) (in the context of abortion with respect to minors); Ben F. Overton & Katherine E. Giddings, *The Right of Privacy in Florida in the Age of Technology and the Twenty-First Century: A Need for Protection from Private and Commercial Intrusion*, 25 FLA. ST. U. L. REV. 25, 26 (1997). "[I]t is critical to recognize that this [constitutional] provision protects only against intrusions by the government. It does nothing to protect citizens from intrusions by private or commercial entities. . . . [T]he provision provides no protection from private or commercial intrusion because the present provision is limited to governmental intrusions." Overton & Giddings, *supra* at 26, 41.

46. *See* Peddicord, *supra* note 8 ("announcing the MyStudies app, a new mobile technology [designed] to foster the collection of real-world evidence via patients' mobile devices" for health research and other purposes).

47. *See* Clayton A. Davis et al., *Kinsey Reporter: Citizen Science for Sex Research*, ARXIV, http://arxiv/org/pdf/1602.04878.pdf (last visited May 1, 2019) (using Kinsey Reporter, "*[c]itizen sex scientists* submit reports, each consisting of one or more surveys, after participating in or observing sexual activity. Surveys cover topics such as flirting, sexual activity, unwanted experience, consumption of pornography, and hormonal birth control side effects"); *Kinsey Reporter*, APP STORE, http://itunes.apple.com/us/app/kinsey-reporter/id533205458?mt=8 (last visited May 1, 2019) [hereinafter *Kinsey Reporter: Apple Store*]; *Kinsey Reporter*, GOOGLE PLAY, http://play.google.com/store/apps/details?id=com.kinsey.android&hl=en_us (last visited May 1, 2019) [hereinafter *Kinsey Reporter: Google Play*].

48. *ActiveDay — Activity Study*, APP STORE, http://itunes.apple.com/us/app/activeday-activity-study/id1183046259?mt=8 (last visited May 1, 2019).

49. *PatientsLikeMe*, APP STORE, http://itunes.apple.com/us/app/patientslikeme/id955272281?mt=8 (last visited May 1, 2019).

50. *MyFitnessPal*, APP STORE, http://itunes.apple.com/us/app/myfitnesspal/id341232718?mt=8 (last visited May 1, 2019).

51. Tovino, *supra* note 6, at 9–14.

52. *See id.* at 9–14.

53. *See id.*; FLA. CONST. art. I, § 23.

54. *See* State v. Tamulonis, 39 So. 3d 524, 528 (Fla. 2d Dist. Ct. App. 2010). "An individual has a privacy interest in his or her prescription records." *Id.*

unconstitutional intrusion.[55] Florida case law simply makes clear that, in assessing a claim for an unconstitutional privacy intrusion, a court shall:

> [D]etermine whether the individual possesses a legitimate expectation of privacy in the information or subject at issue . . . [i]f so, the burden shifts to the State to show that . . . there is a compelling state interest warranting the intrusion into the individual's privacy, and . . . that the intrusion is accomplished by the least intrusive means.[56]

The keys to a constitutional inquiry, thus, are a legitimate expectation of privacy, a compelling state interest, and the means of the intrusion—not adherence to particular privacy, security, and breach notification standards.[57]

III. FLORIDA HEALTH INSTITUTION LICENSING LAWS

Although the Florida Constitution does not contain particular privacy, security, or breach notification standards, a number of other Florida laws do contain privacy standards applicable to physical and mental health data of the type collected by mobile health apps and mobile research apps.[58] That said, many of these additional laws only apply to licensed health care institutions, not independent scientists who, by definition, do not work for or within any type of institution.[59] For example, Florida's hospital licensing law, codified at Chapter 395 of the Florida Statutes, contains privacy standards applicable to patient records.[60] In particular, Chapter 395 defines a patient record as a system that includes the following elements: "[B]asic client data collection; a listing of the patient's problems; the initial plan with diagnostic and therapeutic orders as appropriate for each problem identified; and progress notes, including a discharge summary."[61] Chapter 395 then establishes individual rights requirements as well as use and disclosure requirements—similar to those set forth in the HIPAA Privacy Rule—

---

55. *See id.*; *compare* FLA. CONST. art. I, § 23, *with* Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, § 1, 110 Stat. 1936, 1936 (codified as amended at 42 U.S.C. § 201 (2012)) (setting forth particular privacy, security, and breach notification standards).

56. *Tamulonis*, 39 So. 3d at 528.

57. *See id.*

58. FLA. STAT. §§ 395.3015, .3025(4)–(11) (2018); *see also* FLA. CONST. art. I, § 23.

59. FLA. STAT. §§ 395.3015, 395.3025(1).

60. *Id.* §§ 395.3015, 395.3025(1).

61. *Id.* § 395.3015.

relating to these records.[62] For example, Chapter 395 gives Florida hospital patients the right to obtain a copy of their patient records.[63] By further example, Chapter 395 establishes that hospital patients' records are confidential and may not be disclosed without the prior consent of the patient.[64] However, Chapter 395 also establishes several exceptions to this prior consent requirement, including when the patient records are needed for treatment, risk management and quality assurance activities, trauma registry purposes, organ procurement activities, and epidemiological investigations.[65] Although the data collected and maintained by Florida hospitals in patient records are similar in type and kind to the data obtained by some independent scientists through some mobile health and mobile research apps, hospitals are heavily regulated by the privacy standards referenced in this paragraph but independent scientists—who, by definition, work independent of an institution—are not.[66]

By further illustrative example, Florida's nursing home licensing law, codified within Chapter 400 of the Florida Statutes, establishes certain nursing home patient rights, including the right of nursing home patients to privacy in treatment and to confidentiality of personal and medical records.[67] Although the information collected by nursing homes about their residents is similar in type and kind to that obtained by some independent scientists using some mobile health research apps,[68] nursing homes are required to comply with a variety of privacy standards set forth in the Florida nursing

---

62. *Compare* FLA. STAT. § 395.3015, *and* FLA. STAT. § 395.3025(1), *with* 45 C.F.R. § 164.520 (2018) (establishing the HIPAA Privacy Rule's individual rights requirements), *and* 45 C.F.R. § 164.502 (2018) (establishing the HIPAA Privacy Rule's use and disclosure requirements).

63. FLA. STAT. § 395.3025(1).

64. *Id.* § 395.3025(4).

65. *Id.* § 395.3025(4)(a), (4)(b), (4)(f), (4)(i), (5).

66. *Compare* FLA. STAT. § 395.3015 (defining the content of a patient record for purposes of the Florida hospital licensing law), *with PatientsLikeMe*, *supra* note 49 (collecting information regarding app users' diagnoses, symptoms, and treatments; charting users' daily and monthly symptom progress; disclosing such information to partners of PatientsLikeMe for research purposes).

67. FLA. STAT. §§ 400.011, 400.022(1)(m), 400.20.

68. *See Elderly Hip Fracture: Prevention and Treatment*, PLACE FOR MOM, http://www.aplaceformom.com/planning-and-advice/articles/hip-fractures-in-the-elderly (last visited May 1, 2019) (noting that individuals who are elderly may fall, sustain a hip fracture, and receive care for that fracture in a nursing home); *ActiveDay — Activity Study*, *supra* note 48 (a mobile research app that collects, among other information, information regarding whether an app user has fallen); *FallSafety Pro — Safety Alerts*, APP STORE, http://itunes.apple.com/us/app/fallsafety-pro-safety-alerts/id870864283?mt=8 (last visited May 1, 2019) (a mobile occupational safety and health app that collects information regarding whether a user has fallen, the number of time the user has fallen, and whether a first responder was called to assist the fallen user).

home licensing law, whereas independent scientists do not have the same obligations.[69]

As a final illustrative example, Florida's hospice licensing law, also codified within Chapter 400 of the Florida Statutes, defines and establishes uses and disclosure requirements relating to interdisciplinary records of hospice patients.[70] In particular, the hospice licensing law requires hospices to maintain an "up-to-date, interdisciplinary record of care being given and patient and family status. Records shall contain pertinent past and current medical, nursing, social, and other therapeutic information and such other information that is necessary for the safe and adequate care of the patient."[71] The hospice licensing law further provides that the interdisciplinary record as well as related billing records are confidential and may not be disclosed, although exceptions exist for certain situations, including those involving an authorization executed by the patient or an order by a court of competent jurisdiction ordering the release of the interdisciplinary record.[72] Although the information collected by hospices about their terminally ill patients is similar in type and kind to that obtained by some independent scientists through some mobile health research apps, hospices are required to comply with the privacy requirements set forth in Florida's hospice licensing law, whereas independent scientists are not.[73]

IV. FLORIDA HEALTH PROFESSIONAL LICENSING LAWS

In addition to health institution licensing laws, a number of additional Florida laws contain privacy standards applicable to physical and mental health data of the type collected by mobile health apps and mobile research apps.[74] However, many of these laws only apply to certain licensed health care professionals, not non-provider independent scientists whose

69. *See* Rothstein et al., *supra* note 3, at 897, 899; *Nursing Home Regulations — State Laws and Nursing Homes*, NURSING HOME ABUSE GUIDE, http://nursinghomeabuseguide.com/legal-action/nursing-home-regulations/ (last visited May 1, 2019).

70. FLA. STAT. § 400.611.

71. *Id.* § 400.611(1).

72. *Id.* § 400.611(3)–(4).

73. *See id.* § 400.611(1) (requiring hospice records to "contain pertinent past and current medical, nursing, social, and other therapeutic information . . . necessary for the safe and adequate care of [hospice] patient[s]," who, by definition, have a terminal illness); *ALS Mobilizer Analyzer*, GOOGLE PLAY, http://play.google.com/store/apps/details?id=com.prizeforlife.healthcare&hl=en_US (last visited May 1, 2019) (a mobile research app used to investigate disease progression in ALS, a progressive and terminal disease); *Nursing Home Regulations — State Laws and Nursing Homes*, *supra* note 69.

74. FLA. STAT. §§ 395.3015, 395.3025, 400.011, 400.611, 456.013, 456.059.

training is in software engineering, information systems, marketing, and communications.[75] For example, Chapter 456 of the Florida Statutes establishes general licensing requirements for physicians and other health care practitioners who practice a health profession in Florida.[76] With respect to practitioners who are psychiatrists, Chapter 456 specifically states that "[c]ommunications between a patient and a psychiatrist . . . shall be held confidential and shall not be disclosed except upon the request of the patient or the patient's legal representative."[77] Chapter 456 further explains, however, that a psychiatrist may disclose patient communications to the extent necessary to warn a potential victim or to communicate a threat to a law enforcement agency when:

> (1) A patient is engaged in a treatment relationship with a psychiatrist; (2) [the] patient has made an actual threat to physically harm an identifiable victim or victims; and (3) [t]he treating psychiatrist makes a clinical judgment that the patient has the apparent capability to commit such an act and that it is more likely than not that in the near future the patient will carry out that threat.[78]

The general rule requiring psychiatrist confidentiality is designed to encourage patients with mental health conditions to fully disclose their past diagnoses and treatments as well as their current "[m]ood, level of anxiety, thought content, . . . and perception and cognition" to enable the psychiatrist to accurately diagnose and treat the patient.[79] The general rule, combined with the three exceptions, is also designed to remind the psychiatrist that each patient's history, physical, and other information must be maintained in confidence and is not to be disclosed except in discrete situations in which

---

75. *See About Us*, FALLSAFETY, http://www.fallsafetyapp.com/about-us (last visited May 1, 2019) (noting that the FallSafety employees responsible for developing several occupational safety and health mobile apps, including the FallSafety Pro, Lone Worker Pro, and Worker Safety Pro apps, include "safety-oriented engineers, keen-eyed designers, disciplined quality assurance people, passionate marketers and business development professionals, advanced researchers and technology innovators," but not licensed health care professionals).

76. FLA. STAT. § 456.013.

77. *Id.* § 456.059.

78. *Id.*

79. *See* AM. PSYCHIATRIC ASS'N, PRACTICE GUIDELINES FOR THE PSYCHIATRIC EVALUATION OF ADULTS 6, 9 (3d ed. 2015) (stating as a guideline that a psychiatrist should obtain this information during an initial psychiatric evaluation of a patient; further stating, "[t]he goal of this guideline is to improve the quality of the doctor-patient relationship, the accuracy of psychiatric diagnoses, and the appropriateness of treatment selection.").

the public interest outweighs the patient's right to confidentiality.[80] Interestingly, the information obtained by psychiatrists—including information regarding past diagnoses and treatments as well as current mood, level of anxiety, and thought content—is very similar to the information obtained by a number of mobile health apps and mobile research apps.[81] Although Florida psychiatrists are heavily regulated by privacy standards set forth in Chapter 456 of the Florida Statutes, non-provider independent scientists who conduct mobile app mediated research are not.[82]

By further illustrative example, Chapter 490 of the Florida Statutes establishes licensure requirements for clinical psychologists who practice in Florida.[83] In the legislative intent section of Chapter 490, the Florida Legislature explains that:

> [A]s society becomes increasingly complex, emotional survival is equal in importance to physical survival. Therefore, in order to preserve the health, safety, and welfare of the public, the Legislature must provide privileged communication for members of the public or those acting on their behalf to encourage needed or desired psychological services to be sought out.[84]

To this end, Chapter 490 establishes a general rule that, "[a]ny communication[s] between [a psychologist] and her or his patient or client

---

80. *See* FLA. STAT. § 456.059.

81. *See* AM. PSYCHIATRIC ASS'N, *supra* note 79, at 5, 6; *compare* Parmet, *supra* note 8 (explaining that the mobile research app BiAffect "unobtrusively monitors keyboard dynamics metadata, such as typing speed and rhythm, mistakes in texts, and the use of backspace and auto-correct [and that such data is then] analyzed using an artificial intelligence-based machine learning approach to identify digital biomarkers of manic and depressive episodes in people with bipolar disorder"), *with* Olwen Glynn Owen, *Bipolar Disorder: Psychiatrists Are Taking a New Approach that Aims to Treat Not Just Symptoms but the Whole Person*, MED. NEWS TODAY (July 18, 2007), http://www.medicalnewstoday.com/articles/77227.php (discussing the traditional treatment of patients with bipolar disorder by psychiatrists); *compare Featured Conditions at PatientsLikeMe*, PATIENTSLIKEME: CONDITIONS, http://www.patientslikeme.com/conditions (last visited May 1, 2019) (noting that the PatientsLikeMe mobile app collects symptom data from patients who have a number of mental and behavioral health conditions, including drug addiction and alcohol addiction), *with* PSYCHOL. TODAY: YAHYA SAEED (Feb. 15, 2019), http://www.psychologytoday.com/us/psychiatrists/yahya-saeed-houston-tx/391190?sid=1545765952.5073_17507&city=San+Antonio&state=TX&spec=248&ref=1&tr=ResultsName (profiling a traditional psychiatrist who treats patients and collects information regarding patients with alcohol and drug addiction).

82. *See* FLA. STAT. § 456.059; *Who Regulates All These Health-Related Apps?*, HEALTHLINE, http://www.healthline.com/health-news/who-regulates-all-these-health-related-apps#1 (last visited May 1, 2019).

83. FLA. STAT. §§ 490.005–.006.

84. *Id.* § 490.002.

shall be confidential."[85] Chapter 490 allows the privilege to be waived in only three situations:

> (1) When the [psychologist] is a . . . defendant [in a legal] action arising from a complaint filed by the patient, . . . in which case the waiver [is] limited to that [legal] action; (2) [w]hen the patient . . . agrees to the waiver, in writing, or when more than one person in a family is receiving therapy, when each family member agrees to the waiver, in writing; [or] (3) [w]hen there is a clear and immediate probability of physical harm to the patient or client, to other individuals, or to society and the [psychologist] communicates the information only to the potential victim, appropriate family member, or law enforcement or other appropriate authorities.[86]

Although psychologists may obtain information that is similar in type and kind to that obtained by non-psychologist independent scientists through a mobile health or health research app, psychologists are heavily regulated by the privacy standards referenced in this section whereas independent scientists are not.[87]

Similarly, Chapter 490 and 491 of the Florida Statutes establishes licensure requirements for psychotherapists, clinical social workers, marriage and family therapists, and mental health counselors.[88] In the legislative intent section of Chapter 491, the Florida Legislature explains that:

> [A]s society becomes increasingly complex, emotional survival is equal in importance to physical survival. Therefore, in order to preserve the health, safety, and welfare of the public, the Legislature must provide privileged communication for members of the public or those acting on their behalf to encourage needed or desired counseling, clinical and psychotherapy services, or certain other services of a psychological nature to be sought out.[89]

---

85. *Id.* § 490.0147.

86. *Id.*

87. *See id.*; *compare* Parmet, *supra* note 8 (explaining that the mobile research app BiAffect "unobtrusively monitors keyboard dynamics metadata, such as typing speed and rhythm, mistakes in texts, and the use of backspace and auto-correct [and that such data is then] analyzed using an artificial intelligence-based machine learning approach to identify digital biomarkers of manic and depressive episodes in people with bipolar disorder"), *with* Culbertson v. Culbertson, 455 S.W.3d 107, 113 (Tenn. Ct. App. 2014) (discussing a child custody case involving a father with bipolar disorder and legal questions relating to waiver of the psychologist-patient privilege).

88. FLA. STAT. §§ 490.0051, 491.0046.

89. *Id.* § 491.002.

To this end, Chapter 491 provides that, "[a]ny communication between [a mental health counselor] and her or his patient or client shall be confidential."[90] Chapter 491 permits waiver of this secrecy only:

> (1) When the [mental health counselor] is a party defendant to a [legal] action arising from a complaint filed by the patient . . . in which case the waiver [is] limited to that [legal] action; (2) [w]hen the patient . . . agrees to the waiver in writing; or . . . (3) [w]hen, in the clinical judgment of the [mental health counselor], there is a clear and immediate probability of physical harm to the patient or client, to other individuals, or to society and the [mental health counselor] communicates the information only to the potential victim, appropriate family member, or law enforcement or other appropriate authorities.[91]

Although Florida's mental health counselors may obtain information that is similar in type and kind to that obtained by non-counselor independent scientists through a mobile health or mobile research app, mental health counselors are heavily regulated by the privacy standards set forth in this section whereas independent scientists are not.[92]

The examples above involve psychiatrists, psychologists, and mental health counselors.[93] As background for this initial focus, many mobile health apps are specifically designed to help individuals with their mental health.[94] However, non-mental health practitioners also are required to adhere to privacy standards set forth in Florida law.[95] Again, however, these standards apply only to health care practitioners, not non-practitioner independent scientists.[96] For example, one provision within Chapter 456 of the Florida Statutes regulates a *records owner*, defined as:

---

90. *Id.* § 491.0147.

91. *Id.*

92. *See id.* §§ 491.0147, 491.002; *Independent Scientists: Young Researchers Producing Remarkable Research*, MANA, http://www.nims.go.Jp/mana/about/independent.html (last visited May 1, 2019); *compare* Pooja Chandrashekar, *Do Mental Health Mobile Apps Work: Evidence and Recommendations for Designing High-Efficacy Mental Health Mobile Apps*, MHEALTH, Mar. 23, 2018, at 1, 3 (noting that mobile mental health apps "enable users to self-monitor their mood by periodically reporting their thoughts, behaviors, and actions"), *with* Gracey v. Eaker, 837 So. 2d 348, 357 (Fla. 2002) (noting that the defendant psychotherapist obtained—and then shared without consent—confidential mental health information).

93. FLA. STAT. §§ 456.059, 490.0051, 490.0147, 491.0046.

94. Terry & Gunter, *supra* note 7, at 136 (discussing mobile mental health apps).

95. FLA. STAT. § 456.057.

96. *Id.* § 456.057(1).

> [A]ny health care practitioner who generates a medical record after making a physical or mental examination of, or administering treatment or dispensing legend drugs to, any person; any health care practitioner to whom records are transferred by a previous records owner; [and] any health care practitioner's employer, including, but not limited to, group practices and staff-model health maintenance organizations, provided the employment contract or agreement between the employer and the health care practitioner designates the employer as the records owner.[97]

This provision then requires health care practitioners and records owners to give "copies of all reports and records relating to [their] examination [and] treatment" to patients upon request.[98] This provision also prohibits the furnishing of such records, or the discussion of a patient's medical condition, with any person other than the patient, without patient authorization, unless an exception applies.[99] To the extent an individual conducting mobile app mediated health research is a non-practitioner scientist, software engineer, or other businessperson, the provisions discussed in this paragraph will not apply.[100] Again, these privacy standards are limited in application to health care practitioners.[101]

V. THE HEALTH RECORDS ACT

In addition to Florida laws that impose privacy requirements on health care institutions and health care professionals as a condition of licensure, additional Florida laws seek to regulate the electronic exchange of health records.[102] However, these laws also only apply to licensed health care professionals, not to non-provider independent scientists.[103] For example, the Health Records Act, codified in Chapter 408 of the Florida Statutes, required the Florida Agency for Health Care Administration to develop, by the year 2010, a universal patient authorization form that "may be used by a health care provider to document patient authorization for the use or [disclosure] of an identifiable health record."[104] As background, the Health Records Act defines *health record* as "any information, recorded in any form or medium, which relates to the past, present, or future health of an

---

97. *Id.*
98. *Id.* § 456.057(6).
99. *Id.* § 456.057(7)(a).
100. *See* FLA. STAT. § 456.057(7)(a).
101. *Id.*
102. *See id.* § 408.051.
103. *Id.*
104. *Id.* § 408.051(4)(a).

individual for the primary purpose of providing health care and health-related services."[105] The Health Records Act further defines *identifiable health record* as "any health record that identifies the patient or with respect to which there is a reasonable basis to believe the information can be used to identify the patient."[106]

Pursuant to the terms of the Health Records Act, "[a] health care provider receiving [a universal] authorization form containing a request for the release of an identifiable health record [is required to] accept the form as a valid authorization to release an identifiable health record."[107] In addition, "[t]he exchange by a health care provider of an identifiable health record upon receipt of an authorization form completed and submitted in accordance with [the Health Records Act] creates a rebuttable presumption that the release of the identifiable health record was appropriate."[108] Moreover, "[a] health care provider that exchanges an identifiable health record upon receipt of an authorization form [is] deemed to have [not] violated or waived any privilege protected under [Florida law]."[109] Finally, the Health Records Act specifies that the release of an identifiable health record of a patient without the patient's authorization is permitted for "the treatment of the patient for an emergency medical condition."[110]

Although the health data collected by a mobile research app could easily fit within the definition of a *health record*, the privacy standards set forth within the Health Records Act only apply to health care providers, not non-provider scientists.[111] Stated another way, the Health Records Act's universal authorization form provisions have no application to the context of mobile app mediated health research conducted by independent scientists.[112]

VI. FLORIDA ITS ACT

Although many of the laws discussed above are limited in application to health industry participants, Florida has a number of additional laws that establish security standards that, in theory, could help protect physical and mental health data of the type collected by independent scientists who use mobile health apps and mobile research apps.[113] For

105. FLA. STAT. § 408.051(2)(d).
106. *Id.* § 408.051(2)(e).
107. *Id.* § 408.051(4)(c).
108. *Id.* § 408.051(4)(e).
109. *Id.* § 408.051(4)(f).
110. FLA. STAT. § 408.051(3).
111. *See id.* § 408.051(2)(d), (4).
112. *See id.* § 408.051(4).
113. *See id.* § 282.318(3)(b) (2018).

example, the Florida ITS Act requires the Florida Agency for State Technology ("Agency") to establish "standards and processes consistent with generally accepted best practices for information technology security, to include cybersecurity, and [to] adopt[] rules that safeguard an agency's data, information, and information technology resources to ensure availability, confidentiality, and integrity and to mitigate risks."[114]

In particular, the Florida ITS Act requires the Agency to:

> (a) Develop, and annually update . . . a statewide information technology security strategic plan that includes security goals and objectives for the strategic issues of information technology security policy, risk management, training, incident management, and disaster recovery planning.
>
> (b) Develop, and publish for use . . . an information technology security framework that, at a minimum, includes guidelines and processes for:
>
> (1) Establishing asset management procedures to ensure that an agency's information technology resources are identified and managed consistent with their relative importance to the agency's business objectives.
>
> (2) Using a standard risk assessment methodology that includes the identification of an agency's priorities, constraints, risk tolerances, and assumptions necessary to support operational risk decisions.
>
> (3) Completing comprehensive risk assessments and information technology security audits . . . .
>
> (4) Identifying protection procedures to manage the protection of an agency's information, data, and information technology resources.
>
> (5) Establishing procedures for accessing information and data to ensure the confidentiality, integrity, and availability of such information and data.
>
> (6) Detecting threats through proactive monitoring of events, continuous security monitoring, and defined detection processes.
>
> (7) Establishing agency computer security incident response teams and describing their responsibilities for responding to information technology security incidents, including breaches of personal information containing confidential or exempt data.
>
> (8) Recovering information and data in response to an information technology security incident . . . .
>
> (9) Establishing an information technology security incident reporting process . . . .

114. *Id.* § 282.318(1), (3).

> (10) Incorporating information obtained through detection and response activities into the agency's information technology security incident response plans.
>
> (11) Developing agency strategic and operational information technology security plans . . . .
>
> (12) Establishing the managerial, operational, and technical safeguards for protecting state government data and information technology resources . . . .[115]

The Florida ITS Act thus establishes comprehensive security standards similar to those set forth in the HIPAA Security Rule.[116] The catch is that only state agencies, defined as any "official, officer, commission, board, authority, council, committee, or department of the executive branch of [Florida] state government; the Justice Administrative Commission; and the Public Service Commission" are required to comply with these security standards.[117] By definition, independent scientists do not work for a state agency.[118] As a result, the Florida ITS Act has no application to the instant issue.[119]

VII. FIPA

Florida still has other laws that contain security standards, as well as breach notification standards that could, in theory, help protect physical and mental health data of the type collected by mobile health apps and mobile research apps.[120] For example, FIPA—codified within Chapter 501 of the Florida Statutes—applies to a *covered entity*, defined to include "a sole proprietorship, partnership, corporation, trust, estate, cooperative, association, . . . commercial entity, [or governmental entity] that acquires, maintains, stores, or uses personal information;" as well as a *third-party agent*, defined as "an entity that has been contracted to maintain, store, or process personal information on behalf of a covered entity or governmental entity."[121] Because an independent scientist could be a sole proprietor, or an independent scientist could form a commercial entity with other business, marketing, and communication professionals, FIPA has potential application

115. FLA. STAT. § 282.318(3)(a), (b)(1)–(12).
116. *Id.*; *see also* 45 C.F.R. §§ 164.302–.308 (2018).
117. FLA. STAT. § 282.0041(23).
118. *See* Lovelock, *supra* note 10.
119. *See* FLA. STAT. § 282.318(2)–(3).
120. *See id.* § 501.171.
121. *Id.* § 501.171(1)(b), (h).

to independent scientists, and/or their commercial entities, that develop and/or use mobile apps to conduct health research.[122]

The application of FIPA hinges, however, on whether the covered entity "acquires, maintains, stores, or uses personal information."[123] FIPA defines *personal information* as:

> (1) An individual's first name or first initial and last name in combination with any one or more of the following data elements for that individual: [a] social security number; [b] . . . driver['s] license or identification card number, passport number, military identification number, or other similar number issued on a government document used to verify identity; [c] . . . financial account number or credit or debit card number, in combination with any required security code, access code, or password that is necessary to permit access to an individual's financial account; [d] . . . information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional; or [e] [a]n individual's health insurance policy number or subscriber identification number and any unique identifier used by a health insurer to identify the individual; or (2) [a] user name or e-mail address, in combination with a password or security question and answer that would permit access to an online account.[124]

Some mobile research apps require the user to enter: (1) the user's first and last name; and (2) a user name or email address combined with a password or security question.[125] To the extent the user also provides the app with "information regarding [the] individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional," FIPA's security and breach notification standards, discussed below, would apply.[126] However, other mobile research apps allow research participants to supply health information without providing: (1) a first and last name; or (2) a user name or email address combined with a password or

---

122. *See id.*; Tovino, *supra* note 6, at 40; *About Us*, *supra* note 75 (referencing the commercial entity Fall Safety, which employs software engineers as well as marketing and communications professionals to develop occupational safety and health apps as well as occupational safety and health research apps).

123. FLA. STAT. § 501.171(1)(b).

124. *Id.* § 501.171(1)(g)(1).

125. *See Privacy Policy*, PATIENTSLIKEME, http://www.patientslikeme.com/about/privacy (last visited May 1, 2019). PatientsLikeMe is a mobile health app that requires the user to enter an email address, a user name, and a password before the user may enter health information. *Id.*; *PatientsLikeMe*, *supra* note 49.

126. FLA. STAT. § 501.171(1)(g)(IV); *What Is PII?*, U. MASS. MED. SCH., http://www.umassmed.edu/it/security/compliance/what-is-pii/ (last visited May 1, 2019).

security question.[127] In the case of these latter mobile research apps, FIPA's security and breach notification standards would not apply.[128]

To the extent FIPA applies, the law requires "[e]ach covered entity, governmental entity, or third-party agent [to] take reasonable measures to protect and secure data in electronic form containing personal information."[129] This provision may be referred to as a modest reasonable security standard.[130] FIPA also requires "[e]ach covered entity [and] third-party agent [to] take all reasonable measures to dispose, or arrange for the disposal, of customer records containing personal information within [their] custody or control when the records are no longer to be retained."[131] "Such disposal shall involve shredding, erasing, or otherwise modifying the personal information in the records to make it unreadable or undecipherable through any means."[132] These latter two provisions may be referred to as modest secure disposal standards.[133] These provisions are modest because they pale in comparison to the comprehensive security standards set forth in the HIPAA Security Rule,[134] as well as other state laws, including the Florida ITS Act.[135]

---

127. FLA. STAT. § 501.171(1)(g)(1); *see also Frequently Asked Questions*, KINSEY REP., http://www.kinseyreporter.org/#/faq (last updated May 1, 2019). Kinsey Reporter is a mobile sexual health research app that allows users to donate sexual health data, such as female hormonal birth control effects, for research purposes without the users identifying themselves or providing a user name or email address. *Frequently Asked Questions*, *supra*.

128. *See* FLA. STAT. § 501.171.

129. *Id.* § 501.171 (2).

130. *Id.*; Kevin L. Miller, *What We Talk About When We Talk About* Reasonable Cybersecurity*: A Proactive and Adaptive Approach*, FLA. B.J., Sept./Oct. 2016, at 23, 26.

131. FLA. STAT. § 501.171(8). Florida Statute § 501.171(1)(c) defines a *customer record* as:

> [A]ny material, regardless of the physical form, on which personal information is recorded or preserved by any means, including, but not limited to, written or spoken words, graphically depicted, printed, or electromagnetically transmitted that are provided by an individual in [Florida] to a covered entity for the purpose of purchasing or leasing a product or obtaining a service.

Id. § 501.171(1)(c).

132. *Id.* § 501.171(8).

133. *See* Charles H. Kennedy, *Secure Records Disposal: Is Not Shedding Ever a Good Idea?*, IRON MOUNTAIN, http://www.ironmountain.com/resources/whitepapers/s/secure-records-disposal-is-not-shredding-ever-a-good-idea (last visited May 1, 2019).

134. *See* Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191 § 201, 110 Stat. 1936, 1992 (codified as amended at 42 U.S.C. § 201 (2012)); FLA. STAT. §§ 282.318(3), 501.171(2), (4), (8).

135. *See* FLA. STAT. § 282.318.

In addition to these modest security standards, FIPA contains comprehensive breach notification provisions.[136] In particular, FIPA requires a covered entity to give notice to each individual in the state of Florida whose personal information was, or the covered entity reasonably believes to have been, accessed as a result of a breach of security, defined as "unauthorized access of data in electronic form containing personal information."[137] FIPA requires the notice to be made "as expeditiously as practicable and without unreasonable delay, taking into account the time necessary to allow the covered entity to determine the scope of the breach of security, to identify individuals affected by the breach, and to restore the reasonable integrity of the data system that was breached;" however, the notice may not be made later than thirty days after the determination of a breach or reason to believe a breach occurred.[138] When required, notice to an individual shall include, at a minimum:

> (1) [t]he date, estimated date, or estimated date range of the breach of security; (2) [a] description of the personal information that was accessed or reasonably believed to have been accessed as a part of the breach of security; (3) [i]nformation that the individual can use to contact the covered entity to inquire about the breach of security and the personal information that the covered entity maintained about the individual.[139]

In addition to notifying the individual who was the subject of the information breach, FIPA also requires the covered entity to provide notice to the Florida Department of Legal Affairs ("Department") of any breach of security affecting five hundred or more individuals in the state of Florida.[140] The covered entity must provide this notice to the Department *as expeditiously as practicable*, but not later than thirty days after the determination of the breach or reason to believe a breach has occurred.[141] A covered entity may, however, receive fifteen additional days if the covered entity provides the Department, in writing, *good cause for delay* within thirty days after determination of the breach or reason to believe a breach has occurred.[142] FIPA requires written notice to the Department to include:

---

136. *Id.* § 501.171(4).
137. *Id.* § 501.171(1)(a), (4)(a).
138. *Id.* § 501.171(4)(a).
139. *Id.* § 501.171(4)(e).
140. FLA. STAT. § 501.171(3)(a).
141. *Id.* § 501.171(3)(a).
142. *Id.*

> (1) [a] synopsis of the events surrounding the breach at the time notice is provided; (2) [t]he number of individuals in [Florida] who were, or potentially have been affected by the breach; (3) [a]ny services related to the breach being offered or scheduled to be offered, without charge, by the covered entity to individuals, and instructions as to how to use such services; (4) [a] copy of the notice . . . ; (5) [t]he name, address, telephone number, and e-mail address of the employee or agent of the covered entity from whom additional information may be obtained about the breach.[143]

"If a covered entity discovers circumstances requiring notice . . . of more than [one thousand] individuals at a single time," FIPA also requires the covered entity to "notify, without unreasonable delay, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, . . . of the timing, distribution, and content of the notices."[144]

Interestingly, FIPA provides that:

> Notice provided pursuant to rules, regulations, procedures, or guidelines established by the covered entity's primary or functional federal regulator is deemed to be in compliance with [FIPA's] notice requirement . . . if the covered entity notifies affected individuals in accordance with the rules, regulations, procedures, or guidelines established by the primary or functional federal regulator in the event of a breach of security.[145]

As discussed in the Author's prior work and above in this Article, most independent scientists do not have a primary or functional federal regulator.[146] Thus, FIPA, to the extent applicable, may be the primary—or actually only—form of regulation.[147]

FIPA provides that a violation of its reasonable security, secure disposal, or breach notification provisions "shall be treated as an unfair or deceptive trade practice" for which the Department may bring a legal action.[148] A covered entity that fails to notify affected individuals and the

---

143. *Id.* § 501.171(3)(b).
144. *Id.* § 501.171(5).
145. FLA. STAT. § 501.171(4)(g).
146. Stacey A. Tovino, *Incidental Findings: A Common Law Approach*, 15 ACCOUNTABILITY RES. 242, 242 (2008); *see also* discussion *supra* Parts I–VI (discussing the lack of application of many Florida laws to independent scientists who conduct mobile app mediated research).
147. *See* FLA. STAT. § 501.171.
148. *Id.* § 501.171(9)(a).

Department in accordance with FIPA's breach notification requirements shall also be liable for: (1) during the first thirty days following the violation, a civil penalty of $1,000 per day; (2) for each subsequent thirty-day period or portion thereof through the 180th day following the violation, a civil penalty of $50,000; and (3) after the 180th day following the violation, a civil penalty up to $500,000.[149] FIPA clarifies that these civil penalties apply *per breach*, not "per individual affected by the breach."[150] Notably, FIPA "does not establish a private cause of action."[151]

VIII. PATIENT BILL OF RIGHTS

None of the Florida laws discussed above have specific or express application to researchers.[152] However, the Patient Bill of Rights, codified in Chapter 381 of the Florida Statutes, provides that "a patient has the right to know if medical treatment is for purposes of experimental research and to consent prior to participation in such experimental research."[153] The Patient Bill of Rights further provides that, "[f]or any patient, regardless of ability to pay or source of payment for his or her care, participation must be a voluntary matter; and a patient has the right to refuse to participate. The patient's consent or refusal must be documented in the patient's care record."[154] If applicable to mobile app mediated research, these provisions create some privacy protections for research participants; that is, they prohibit the collection of an individual's information by an app for research purposes without the individual's prior consent.[155] Nothing in the quoted language set forth in this paragraph limits the application of this privacy prohibition to just health care providers or health care facilities.[156] That said, the stated intent of the Patient Bill of Rights is to protect "patients of health care providers and health care facilities."[157] In addition, the prefatory statement in the beginning of the Patient Bill of Rights suggests that the enumerated obligations only apply to health care providers and health care

149. *Id.* § 501.171(9)(b).
150. *Id.* § 501.171(9)(b)(2).
151. *Id.* § 501.171(10).
152. *See* discussion *supra* Parts I–VII.
153. FLA. STAT. § 381.026(4)(e).
154. *Id.*
155. *See id.*
156. *See id.*
157. *Id.* at § 381.026(3). "It is the purpose of this section to promote the interests and well-being of the patients of health care providers and health care facilities and to promote better communication between the patient and the health care provider." FLA. STAT. § 381.026(3).

facilities.[158] As such, these privacy protections probably would not apply to a non-provider independent scientist, who does not work within or for a Florida-licensed health care facility.[159]

IX. FLORIDA COMMON LAW

Florida recognizes a number of common law causes of action that involve duties relevant to confidentiality and privacy.[160] For example, Florida recognizes a cause of action for breach of fiduciary duty when a fiduciary impermissibly discloses a confidence.[161] Under Florida law, the elements of the cause of action for breach of fiduciary duty include: (1) the existence of a fiduciary duty; (2) a breach of such duty; (3) proximate causation; and (4) damages.[162] The first element, which is the crucial element for the issue at hand, requires an actor to have a fiduciary relationship with the person who is claiming damages.[163] Fiduciary duties have been recognized in cases involving an attorney/client, executor/heir, guardian/ward, agent/principal, trustee/beneficiary, corporate officer/shareholder, psychiatrist/patient, psychotherapist/patient, mental health counselor/patient, and other similar relationships where great trust is imposed on one person for the benefit of another.[164] Some courts, however, have imposed fiduciary duties on other, less-classic actors, including lenders, clerics, and wives.[165] The question in the instant case is whether a court would impose a fiduciary duty on an independent scientist who conducts mobile app mediated research and, to a lesser extent, whether that scientist could breach that duty in a case involving a privacy or security breach of confidential research data.[166]

---

158. *Id.* § 381.026(4). "Each health care facility or provider shall . . . ." *Id.*

159. *See id.*

160. *See Florida Common Law*, *supra* note 33.

161. Gracey v. Eaker, 837 So. 2d 348, 353 (Fla. 2002).

162. *Id.*

163. *Id.*

164. John F. Mariani et al., *Understanding Fiduciary Duty*, FLA. B.J., March 2010, at 21, 21; *see also Gracey*, 837 So. 2d at 353; DeVaughn v. DeVaughn, 840 So. 2d 1128, 1132 (Fla. 5th Dist. Ct. App. 2003); Barnett Bank of Marion Cty. v. Shirey, 655 So. 2d 1156, 1158 (Fla. 5th Dist. Ct. App. 1995); Cohen v. Hattaway, 595 So. 2d 105, 107 (Fla. 5th Dist. Ct. App. 1992); Hoopes v. Hammargren, 725 P.2d 238, 242 (Nev. 1986); Eckhardt v. Charter Hosp. of Albuquerque, Inc., 953 P.2d 722, 727–28 (N.M. Ct. App. 1997).

165. Mariani et al., *supra* note 164, at 21 (providing an outstanding overview of Florida law governing the fiduciary relationship and fiduciary duties).

166. *See* Suthers v. Amgen Inc., 372 F. Supp. 2d 416, 429 (S.D.N.Y. 2005); Greenberg v. Miami Children's Hosp. Research Inst., Inc., 264 F. Supp. 2d 1064, 1072 (S.D. Fla. 2003); Tovino, *supra* note 6, at 25 (discussing the application of fiduciary duties in the

As the Author explained in a prior work, "fiduciary relationships may be expressly or impliedly created."[167] Because it is unlikely that an independent scientist who conducts mobile app mediated research would expressly identify as a fiduciary in any electronic or other policies related to the mobile app, the concept of an implied fiduciary relationship is discussed.[168] "Implied fiduciary relationships are premised on the specific facts and circumstances surrounding the transaction and the relationship of the parties. These relationships have been found when confidence is reposed by one individual, the principal, and trust is accepted by the other individual, the fiduciary."[169] Although research participants have sought to impose fiduciary duties on researchers, these attempts are usually unsuccessful.[170] As the Author explained elsewhere:

> In *Moore v. Regents of the University of California*,[171] a patient, Moore, who underwent treatment for hairy-cell leukemia, and whose treating physician used the patient's cells to establish and patent a new cell line without his permission, sued the physician, Dr. Golde, the Regents of the University of California ("Regents"), a researcher employed by the Regents, Quan, and other parties for breach of fiduciary duty and twelve additional causes of action . . . The California Supreme Court applied the fiduciary duty to Dr. Golde, but summarily dismissed the breach of fiduciary cause of action with respect to the other defendants: "The Regents, Quan [and others] are not physicians. In contrast to [Dr.] Golde, none of these defendants stood in a fiduciary relationship with Moore or had the duty to obtain Moore's informed consent to medical procedures."
>
> Other courts have dismissed breach-of-fiduciary-duty causes of action when the research participant failed to present sufficient evidence of the formation of the fiduciary relationship. In *Greenberg v. Miami Children's Hospital Research Institute*,[172] the plaintiffs sued a researcher, hospital, and research institute for breach of fiduciary duty based on the defendants' alleged failure to disclose material information relating to their disease research. When the defendants argued that the plaintiffs failed to allege any

---

context of researchers who conduct neuroimaging studies and who may discover incidental neurological findings).

167. Tovino, *supra* note 146, at 250; *see also Greenberg*, 264 F. Supp. 2d at 1071.

168. *See Suthers*, 372 F. Supp. 2d at 429; Tovino, *supra* note 146, at 250.

169. Tovino, *supra* note 146, at 250; *see also Greenberg*, 264 F. Supp. 2d at 1071.

170. Tovino, *supra* note 146, at 251.

171. 793 P.2d 479 (Cal. 1990).

172. 264 F. Supp. 2d 1064 (S.D. Fla. 2003).

facts showing that the defendants had recognized or accepted the trust, as required to form the fiduciary relationship, the plaintiffs responded by alleging that the defendants impliedly accepted the trust by undertaking research that they represented as being for the benefit of the plaintiffs. The court disagreed, reasoning that the plaintiffs had not sufficiently alleged the second element of a fiduciary relationship—acceptance of trust by the researchers—and that this element cannot be assumed from the subjects' research participation: "There is no automatic fiduciary relationship that attaches when a researcher accepts medical donations and the acceptance of trust, the second constitutive element of finding a fiduciary duty, cannot be assumed once a donation is given."

Other courts also have considered, at least in dicta, the question of whether researchers owe their participants fiduciary duties. *Suthers v. [Amgen Inc.]*,[173] involved an investigation of an experimental Parkinson's treatment—glial-derived neurotrophic factor ("GDNF")—at several sites, including New York University ("NYU"). Amgen, the trial sponsor, discontinued the trials after data indicated that GDNF was neither safe nor effective. Two of the research participants who received GDNF in an extended version of the study conducted at NYU sued Amgen to compel the provision of GDNF, which the participants believed relieved their Parkinson's symptoms. One of their causes of action was breach of fiduciary duty, which the court refused to impose on Amgen: "[T]here is no basis in fact or law to impose a fiduciary duty running from the sponsor of an independent study to participants who it does not select, has not met, and about whom it may not know the details of their medical conditions." Because the participants did not name NYU or its researchers as defendants, the court did not address the applicability of the fiduciary duty to the research team, although the court noted in dicta one bioethicist's criticism of the application of fiduciary duties to researchers.

Notwithstanding these cases, the nature of the relationship between researchers and participants continues to be debated. Some plaintiffs' lawyers argue that researchers are fiduciaries vis-à-vis their participants. Attorney Alan Milstein, who successfully represented University of Pennsylvania gene therapy participant, and decedent, Jesse Gelsinger, recently stated [that once a research participant] signs . . . [an] informed consent [to research document, the fiduciary relationship has been established].

. . . .

173. 372 F. Supp. 2d 416 (S.D.N.Y. 2005).

> Other attorneys and scholars take a middle ground and admit that there are important distinctions between the researcher–participant relationship and the types of relationships traditionally governed by fiduciary principles, although they use the concept of the fiduciary relationship as a framework for thinking about the researcher–participant relationship. Finally, some attorneys and scholars expressly oppose the application of fiduciary duties to researchers, reasoning that the relationship between researcher and participant differs fundamentally from that between physician and patient, that clinical research should not be conflated with medical care, and that the purpose of research is not to benefit individuals.[174]

In summary, it is certainly possible for a mobile app mediated research participant to claim that an independent scientist has a fiduciary duty that favorably runs towards the research participant.[175] However, it is unlikely that a court would agree absent an express assumption of trust by the independent scientist or other facts not contemplated by this Article.[176] Even if an independent scientist were found by a court to have a fiduciary relationship with the scientist's research participants, the case law discussed above does not establish privacy, security, or breach notification standards compliance with which would establish proper fiduciary behavior.[177]

In addition to breach of fiduciary duty based on breach of trust or confidence, Florida also recognizes four invasion of privacy torts, including:

> (1) appropriation, [which is] the unauthorized use of a person's name or likeness to obtain some benefit; (2) intrusion, [which is the] physical[] or electronic[] intru[sion] into one's private quarters; (3) public disclosure of private facts, [which] is the dissemination of truthful private information [that] a reasonable person would find objectionable; and (4) false light in the public eye, [which is the] publication of facts [that] place a person in a false light even though the facts themselves may not be defamatory.[178]

---

174. Tovino, *supra* note 146, at 251–53 (citations omitted) (first quoting *Moore*, 793 P.2d at 486; then quoting *Greenberg*, 264 F. Supp. 2d at 1072; then quoting *Suthers*, 372 F. Supp. 2d at 429).

175. *See id.*

176. *Id.* at 254.

177. *Id.*; *see Suthers*, 372 F. Supp. 2d at 429; *Greenberg*, 264 F. Supp. 2d at 1072.

178. Allstate Ins. Co. v. Ginsberg, 863 So. 2d 156, 162 (Fla. 2003) (listing the four invasion of privacy torts recognized in Florida).

"All of these actions are tied together by the common thread of privacy, but otherwise they have little in common."[179] Absent extraordinary facts not contemplated by this Article, the first and the last torts—appropriation and false light—have little application to the issue at hand.[180] Appropriation would require, for example, the independent scientist—or, perhaps, a person who received personal data from the independent scientist—to use the research participant's name, image, or other comparable research data for commercial or other advantage without the research participant's prior authorization.[181] False light would require the independent scientist—or, perhaps, a person who received personal data from the independent scientist—to publish in a widespread manner facts that place the research participant in a highly offensive, false light.[182] Although one could certainly create a fact pattern involving an independent scientist and mobile research participant that satisfies the elements of one or both torts, such a fact pattern is unlikely.[183]

The second tort—intrusion—has still unlikely but potential application to the issue at hand.[184] "Intrusion involves 'the unreasonable and highly offensive intrusion upon the seclusion of another.'"[185] Examples of intrusion found to be actionable include "the illegal diversion or interception and opening of one's mail, peeping into one's home, the viewing of a department store's changing room by someone of the opposite sex where no adequate notice has been provided, persistent and unwanted telephone calls, wiretapping, or prying into a plaintiff's bank account."[186] An independent scientist who obtains personal data from a research participant's mobile phone and uses that data for research purposes without providing prior notice to, and without obtaining the authorization of, the research participant could arguably be a proper defendant in an intrusion case.[187] On the other hand, an independent scientist whose mobile app—through an electronic privacy policy or otherwise—notifies the potential research participant of the types of data that will be collected for research purposes and who obtains the individual's prior and express electronic authorization to such research participation should be able to defeat an intrusion claim.[188]

---

179. Overton & Giddings, *supra* note 45, at 41.
180. *See id.* at 41–43.
181. *See id.* at 41 (explaining the appropriation tort under Florida law).
182. *See id.* at 43 (explaining the false light tort under Florida law).
183. *See id.* at 41–43.
184. Overton & Giddings, *supra* note 45, at 42.
185. *Id.* (quoting W. PAGE KEETON ET AL., PROSSER AND KEETON ON THE LAW OF TORTS § 117, at 854 (5th ed. 1984)) (explaining the intrusion tort under Florida law).
186. *Id.*
187. *See id.*
188. *See id.*; Moore et al., *supra* note 1, 3–4.

The third tort—public disclosure of private facts—also has unlikely but potential application to the issue at hand.[189] In a case based on public disclosure of private facts, "[t]he plaintiff must allege that facts were made public that would normally [be] kept hidden from the public eye. Moreover, the facts disclosed must be facts that would be highly offensive to a reasonable person."[190] One can imagine that an independent scientist who made public highly offensive facts collected during research—perhaps sexual behavior or sexual disease information[191]—might be named as a defendant in a public disclosure of private facts case if the scientist had promised the research participant confidentiality.[192] The case law interpreting both the second and third torts does not contain particular privacy, security, or breach notification standards, compliance with which would defeat the torts.[193] That said, the privacy concepts of prior notification and prior authorization are referenced in the case law and, if adequately pled by the independent scientist, should be sufficient to defeat a claim.[194]

X. CONCLUSION AND PROPOSALS

This Article has carefully examined a variety of provisions within Florida law to determine whether Florida law contains comprehensive privacy, security, and breach notification standards that could apply to independent scientists who conduct mobile app mediated health research.[195] This Article has concluded that Florida law tends to fall into one of two categories—that is: (1) the law contains at least one data privacy, security, and/or breach notification right or standard, but the right or standard is limited in application to certain actors, certain professions, or certain institutions and does not apply to independent scientists; or (2) the law is not necessarily limited in application but the law fails to establish comprehensive privacy, security, and breach notification standards that will drive the implementation of privacy and security best practices by independent scientists.[196] Florida laws that fall into the first category include the Florida

189. Overton & Giddings, *supra* note 45, at 42.

190. *Id.* (discussing the public disclosure of private facts tort under Florida law).

191. *See id.*; *Frequently Asked Questions*, *supra* note 127.

192. *See* Overton & Giddings, *supra* note 45, at 40–42.

193. *Id.* at 42; Allstate Ins. Co. v. Ginsberg, 863 So. 2d 156, 160–62 (Fla. 2003); Doe v. Univision Television Grp., Inc., 717 So. 2d 63, 64 (Fla. 3d Dist. Ct. App. 1998).

194. *See Ginsberg*, 863 So. 2d at 160–62; *Doe*, 717 So. 2d at 64.

195. *See* discussion *supra* Parts II–IX.

196. Discussion *supra* Parts II–IX; *see also* FLA. CONST. art. I, § 23; FLA. STAT. §§ 282.318, 381.026, 395.0197, 408.051, 464.0095, 501.171 (2018); *Florida Common Law*, *supra* note 33.

Constitution (privacy), Florida's health institution licensing laws (privacy), Florida's health professional licensing laws (privacy), the Health Records Act (privacy), Florida ITS Act (security), and the Patient Bill of Rights (privacy).[197] Florida laws that fall into the second category include FIPA (security and breach notification) and Florida common law (privacy).[198]

FIPA, which contains security and breach notification standards that will apply to some, but not all, independent scientists who conduct mobile app mediated research studies may be the best option for protecting mobile app mediated research data going forward.[199] Several amendments to FIPA would be necessary, however, to make the law apply to all independent scientists who conduct mobile app mediated research.[200] First, as currently written, FIPA applies to a *covered entity*, defined to include "a sole proprietorship, partnership, corporation, trust, estate, cooperative, association . . . commercial entity [or governmental entity] that acquires, maintains, stores, or uses personal information."[201] Because many independent scientists are simply natural persons, an amendment to FIPA's definition of covered entity to include natural person would be helpful to ensuring coverage of all independent scientists.[202]

Second, the application of FIPA hinges on whether the *covered entity* acquires, maintains, stores, or uses personal information.[203] Recall that FIPA defines *personal information* as:

> "a. [a]n individual's first name or first initial and last name in combination with any one or more of the following data elements for that individual: (I) [a] social security number; (II) [a] driver['s] license or identification card number, passport number, military identification number, or other similar number issued on a government document used to verify identity; (III) [a] financial account number or credit or debit card number, in combination with any required security code, access code, or password that is necessary to permit access to an individual's financial account; (IV) [a]ny information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional; or (V) [a]n individual's health insurance

197. *See* FLA. CONST. art. I, § 23; FLA. STAT. §§ 282.318, 381.026, 395.0197, 408.051; 464.0095.

198. *See* FLA. STAT. § 501.171; *Florida Common Law*, *supra* note 33.

199. *See* FLA. STAT. § 501.171(1)(b).

200. *See id.* § 501.171; *Independent Scientists: Young Researchers Producing Removeable Research*, *supra* note 92.

201. FLA. STAT. § 501.171(1)(b).

202. *See id.*; *Independent Scientists: Young Researchers Producing Removeable Research*, *supra* note 92.

203. FLA. STAT. § 501.171(1)(b).

> policy number or subscriber identification number and any unique identifier used by a health insurer to identify the individual; [(V)(b)] a user name or e-mail address, in combination with a password or security question and answer that would permit access to an online account."[204]

Some mobile apps, including PatientsLikeMe, require the user to enter: (1) the user's first and last name; and/or (2) a user name or email address combined with a password or security question.[205] To the extent the user also provides the app with information regarding the individual's "medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional," FIPA would apply.[206] Other mobile research apps, such as Kinsey Reporter, allow research participants to supply health information without providing: (1) a first and last name; or (2) a user name or email address combined with a password or security question.[207] In the case of these latter mobile research apps, FIPA would not apply.[208] In order to cover all mobile research apps, FIPA's definition of *personal information* should be amended such that a first and last name, or a user name or email address combined with a password or security question, are not required for FIPA to apply.[209] One might think that these are the only identifiers that could be used to identify a research participant; however, electronically—and publicly—accessible property records, for example, make it such that other identifiers, such as street number or address, could be used to identify a research participant or a research participant's family.[210]

---

204. *Id.* § 501.171(g).

205. *See PatientsLikeMe*, *supra* note 49.

206. FLA. STAT. § 501.171(1)(g)(1)(a)(IV); *see also What Is PII?*, *supra* note 126.

207. *See Kinsey Reporter: Apple Store*, *supra* note 47; *Kinsey Reporter: Google Play*, *supra* note 47.

208. *See* FLA. STAT. § 501.171(1)(g)(1)(a).

209. *See id.*

210. *See Guidance Regarding Methods for De-Identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule*, HHS, http://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html#rationale (last visited May 1, 2019); Cameron F. Kerry, *Why Protecting Privacy Is a Losing Game Today — And How to Change the Game*, BROOKINGS (July 12, 2018), http://www.brookings.edu/research/why-protecting-privacy-is-a-losing-game-today-and-how-to-change-the-game/.

> To most people, *personal information* means information like social security numbers, account numbers, and other information that is unique to them. [United States] privacy laws reflect this conception by aiming at *personally identifiable information*, but data scientists have repeatedly demonstrated that this focus can be too narrow. The aggregation and correlation of data from various sources make it increasingly possible to link supposedly anonymous information to specific individuals and to infer characteristics and information about them. The result is

In summary, "[t]he aggregation and correlation of data from various sources make it increasingly possible to link supposedly anonymous information to specific individuals and to infer characteristics and information about them."[211]

Once FIPA applies, the law contains a modest reasonable security standard, a modest secure disposal standard, and a comprehensive breach notification standard.[212] One option is to elevate FIPA's modest security provisions to the level of comprehensive security standards.[213] Other states that have established comprehensive security standards in this context that could serve as a guide include Oregon and Massachusetts.[214] Florida's own ITS Act, which also establishes comprehensive security standards, could be used as a guide.[215] Because FIPA contains no privacy standards, including individual rights provisions or use and disclosure requirements, the Author further recommends that FIPA be amended to include such standards.[216] The privacy standards set forth within the federal HIPAA Privacy Rule as well as California's Consumer Privacy Act of 2018 may be used as a guide.[217]

This Article has demonstrated that many Florida laws contain some type of privacy, security, or breach notification standard applicable to health data of the type collected by mobile research applications.[218] However, these laws tend to be traditional, intra-industry laws that are limited in application to certain individuals—usually licensed health care professionals—and certain institutions—usually licensed health care facilities.[219] Today,

---

> that today, a widening range of data has the potential to be personal information, i.e. to identify us uniquely. Few laws or regulations address this new reality.

Kerry, *supra*.

211. *Id.*

212. *See* FLA. STAT. § 501.171(2), (4), (8) (reviewing FIPA in detail; noting that FIPA's security provisions are modest because they pale in comparison to the comprehensive security standards set forth in the HIPAA Security Rule as well as other state laws, including the Florida ITS Act); Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, § 201, 110 Stat. 1936, 1992 (codified as amended at 42 U.S.C. § 201 (2012)); FLA. STAT. § 282.318(3).

213. *See* Health Insurance Portability and Accountability Act of 1996, § 201, 110 Stat. 1936 at 1992; FLA. STAT. § 501.171(2), (4), (8).

214. Tovino, *supra* note 6, at 54 (discussing the comprehensive data security provisions of Oregon and Massachusetts); *see also* MASS. GEN. LAWS ch. 93H, § 2 (2018); OR. REV. STAT. § 182.122 (2018).

215. *See* FLA. STAT. § 282.318.

216. *See id.* § 501.171(2).

217. *See* Health Insurance Portability and Accountability Act of 1996, § 201, 110 Stat. 1936 at 1992; CAL. CIV. CODE § 1798.120 (West 2018) (this law will be effective on Jan. 1, 2020); Tovino, *supra* note 6, at 52 (discussing the comprehensive privacy standards set forth within the California Consumer Privacy Act of 2018).

218. *See* FLA. STAT. §§ 282.318(3), 395.3025(4), 456.057(4), 501.171(2).

219. *See id.* §§ 395.3025, 456.057.

however, health data is generated not only by individual and institutional members of the health care industry, but also by independent scientists who conduct mobile app mediated research studies as well as a range of other individuals and institutions that are based outside the health care industry.[220] The significant economic, dignitary, and psychological harms associated with health data breaches and the lack of generally applicable federal and state regulations suggests a need for reform in this area.[221] It is the Author's hope that the changes recommended to FIPA will better protect the privacy and security of mobile research participant data as well as other forms of health-related big data.*

220. *See* Klemick, *supra* note 14; Rothstein, *supra* note 19, at 425.
221. *See* Rothstein, *supra* note 19, at 425–26.