Niya T. McCray,

Putting a Finger on the Problem: An Update on U.S. Biometric Privacy Law:

Biometric technology is sweeping the nation in more ways than one. The inherently unique nature of the data collected by this technology unlocks a level of efficiency and identification that may have previously been impossible. As with every advancement, though, there are both notable positives and obvious negatives. The very facet that makes biometrics so powerful—its uniqueness—is also its biggest area of concern. Biometric data, unlike its traditional counterparts, cannot be replaced once it is compromised. From fingerprints to retina scans to hand and voice prints, a person's biometric identifiers are virtually irreplaceable. As the understanding grows, consumers and businesses, alike, have developed a sense of uncertainty and wariness as it relates to the collection, usage, and maintenance of biometric data. This presentation, then, will walk through the onset of biometric technology and focus on how its presence is revolutionizing the legal field. From Illinois' BIPA to Texas' CUBI, more and more states are attempting to adjust to biometric technology sources. This adjustment, though, has been rocky to say the least. Plaintiffs have flooded the Illinois' courts seeking redress for technical violations of the statute, and out-of state plaintiffs are testing the boundaries of biometric protections even now. This presentation will provide practical legal solutions and considerations on how counsel can prepare for the upcoming courtroom sparring destined to occur. Those solutions will also incorporate considerations under Coverage Part B, dedicated cyberliability policies, and the soon to be implemented GDPR. Biometric technology is boldly, and quickly, going where no one has gone before; our choice, to go with it or fall behind.

Steven W. Teppler, practitioner and NSU Adjunct Professor of Law

The MIRAI botnet and WannaCry ransomware attacks are the poster children for the ongoing spread of cyber-security vulnerability exploits facing the nation's health care infrastructure. These attack modalities are now being both commercialized and commoditized as "crime-as-a-service," which, in the health care arena, poses increasing potential for interruption of access and resulting adverse patient outcomes. Compounding this problem is the proliferation of connected devices commonly referred to as "smart devices" but also known as the "Internet of Things" or "IoT." In the medical arena, these connected devices are being increasingly deployed to provide or monitor the administration of health care services. The monoclonal nature of these "smart" or "connected" features of these devices also introduces new vectors for cyber-security incidents (and patient harm) on a potentially massive scale. This presentation will address potential liability issues, together with how a combination of technology and policy-based solutions can serve to address and prevent or mitigate these exploits.

Professor Stacey A. Tovino, UNLV

Mobile Application-Mediated Research: Privacy and Security Challenges and Opportunities (footnotes omitted)

Mobile applications (mobile apps) are a fast-growing category of software typically installed on personal smartphones and wearable devices.1 Mobile apps are used for a wide range of health-related activities, including fitness, health education, health prediction, patient-specific diagnosis, health care delivery, treatment support, chronic disease management, health research, disease surveillance, and epidemic outbreak tracking, among other activities. Mobile health apps, designed for contexts as diverse as maternal and child health,2 dermatology,3 mental health,4 and communicable and contagious diseases,5 have tremendous potential to enhance fitness, health knowledge, treatment, and research.

Due to the high volume and diversity of data gathered by mobile apps, mobile apps also raise a number of significant privacy and security concerns. Many federal and state statutes and regulations, including the federal HIPAA Privacy, Security, and Breach Notification Rules (HIPAA Rules), were promulgated to protect the privacy and security of individually identifiable health information and to assist patients, insureds, and other individuals protect themselves in the event of a privacy or security breach. However, not all individuals and institutions that develop and use mobile apps, and not all data storage companies that store health information collected by mobile apps, are regulated by these laws.

For example, the HIPAA Rules only regulate: (i) covered entities, including health plans, health care clearinghouses, and those health care providers that transmit health information in electronic form in connection with standard transactions, including health insurance claims; 6 and (ii) business associates, which access or use protected health information to provide certain services to, or to perform certain functions on behalf of, covered entities.7 The HIPAA Rules do not regulate a number of individuals and institutions that participate in the mobile app space, including mobile app developers and data storage companies, 8 as well as the many citizen scientists,9 independent, non-treating researchers,10 and patient researchers11 who use mobile apps to conduct research. Although some states have health privacy laws that extend to these non-federally regulated individuals and institutions,12 other states do not.13 Consequently, the voluminous and diverse data gathered by mobile apps may be at risk for privacy and security breaches, leading to dignitary, 2 psychological, and economic harms for which some affected individuals have no legally enforceable rights or remedies.

This presentation (and accompanying article) will focus specifically on the privacy and security challenges raised by mobile app-mediated research conducted by citizen scientists, independent researchers, and patient researchers as well as the mobile app developers and the data storage and processing companies that support them. Following a brief review of the reasons such individuals and institutions are seldom regulated by federal privacy, security, and breach notification laws, this presentation will report the results of a fifty-state survey investigating the regulation of mobile app-mediated research conducted by citizen scientists, independent researchers, and patient researchers.

In particular, this presentation will report those states that apply privacy, security, and breach notification provisions to non-federally regulated, mobile app-mediated researchers, the substance of those regulations, and the limitations of those regulations. This presentation will highlight the presence or absence in state law of industry-standard privacy, security, and breach notification rights and protections including, but not limited to, provisions requiring: (i) the research participant’s prior written authorization for the use and disclosure of the participant’s protected health information (PHI); (ii) the distribution, and acknowledgement of receipt of, a notice of privacy practices or similar document or information; (iii) the implementation of physical, technical, and administrative safeguards designed to protect the privacy and security of PHI; (iv) privacy and security training for mobile app-mediated researchers, mobile app developers, and data storage and processing company workforce members; (v) privacy and security complaint receipt and resolution processes; (vi) breach notification provisions; and (vii) civil, criminal, and/or administrative enforcement. This presentation will close with specific privacy, security, and breach notification guidelines for the conduct of mobile app-mediated research by citizen scientists, independent researchers, and patient researchers as well as the mobile app developers and data storage and processing companies that support them.