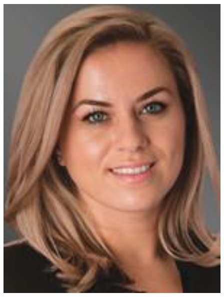
Securing Mobile Health Data — NIST Weighs In

By **Gretchen Ramos and Zerina Curevac** (August 28, 2018)

Gretchen Ramos



Zerina Curevac

Over the last couple of years, the number of mobile health applications have doubled, with hundreds of thousands of such apps available today. The digital health market is anticipated to exceed $379 billion by 2024, and a large chunk of that market size is attributable to increased use of mobile communications technology and devices by consumers and health care professionals.[1] Until recently, there has been little guidance in terms of mobile health security frameworks. However, last month, the National Cybersecurity Center of Excellence at the National Institute of Standards and Technology published a cybersecurity guide for electronic health record applications on mobile devices.[2] The 260-page guide is an important step to making mHealth apps more secure, especially considering hackers tend to target mHealth apps. Regulators and companies will need to prioritize mHealth security to ensure health care professionals and consumers can benefit from the new technology without fear of jeopardizing consumer privacy.

Security Concerns Are Limiting the Growth of the Digital Health Market

While hundreds of new mHealth apps and devices are introduced to the market every month, many are lagging behind on the security front and consumers, health care professionals and other stakeholders are aware of it. In a survey conducted by Change Healthcare Inc. on consumer attitudes toward digital and mobile health tools, nearly half of consumers cited security and privacy concerns as their top concerns limiting the widespread adoption of mobile and digital health tools.[3]

Concerns in relation to security and privacy were the impetus for the new NIST guide, which was developed by industry and academic cybersecurity experts, with the input of health care providers who first identified the security challenges of mHealth apps and devices in a 2012 U.S. Department of Health and Human Services Mobile Devices Roundtable. Attendants of the roundtable cited security concerns such as unauthorized access to enterprise networks via unsecured mobile devices or untrusted network connections, general data loss and theft, and vulnerabilities associated with routine operations (e.g., data synchronization and storage, etc.) due to interactions with other mobile devices.

Thus, developers who prioritize security and employ privacy-by-design principles in creating their mHealth apps or devices will likely have a longer shelf life than developers who do not. Secure mHealth apps and devices will undoubtedly be the ones favored and utilized by consumers, healthcare professionals and other stakeholders.

In the Context of LabMD v. FTC Ruling and Security Breaches

The case for prioritizing privacy and security in mHealth apps and devices is not just a good business case, but it also helps reduce legal risks. With the recent ruling by the Eleventh Circuit in LabMD Inc. v. Federal Trade Commission,[4] the FTC's enforcement of security issues is at the forefront. In this case, the court vacated the FTC’s consent order against LabMD in a dispute about an alleged security incident because the order was not specific enough as to the changes LabMD should make in its data security program.

The FTC has not published a formal approach on how it will enforce security issues after this ruling; however, it seems likely that entities can anticipate having to work more closely with the FTC on specific security measures rather than having the flexibility to adopt security programs based on their business model. This can create more burdens for organizations as they work towards compliance and minimizing risks, especially where there is not a universally adopted security framework to rely on. In a survey conducted by the Health Information and Management Systems Society, the majority of respondents (57.9 percent), which identified as health care organizations, indicated that they used NIST for their security framework, closely followed by HITRUST (26.4 percent), Critical Security Controls (24.7 percent), and International Organization for Standardization (18.5 percent).[5] Where there is not an established framework, use of the most common security framework is the next best thing.

Moreover, the rising costs of data breaches stress the importance of enterprise and mHealth security. According to the Ponemon Institute, the average data breach cost per record per capita can vary drastically depending on industry classification — the overall average is $148, but health organizations pay $408 per record due to the sensitive and highly regulated data they collect.[6] And even though email-based attacks are the most common attack vector for security incidents, mobile devices are still in the top five.[7]

The Mobile EHR Cybersecurity Framework Proposed by NCCoE

In drafting the guide, the National Cybersecurity Center of Excellence's objective was to address the 2012 roundtable concerns by building a simulated virtual environment with mobile devices, electronic health records and information technology infrastructure interacting together. The guide demonstrates how a combination of open-source and commercially available tools and technologies can secure mobile devices and apps, providing security experts with some ideas on the types of characteristics and capabilities to look out for.

The guide incorporates standards, such as the NIST Cybersecurity Framework and the Health Insurance Portability and Accountability Act Security Rule, and best practices applicable to health care apps and devices. For example, the guide lists technologies — such as key management — with a corresponding table of applicable standards and links.

Furthermore, the guide offers bite-sized pieces of information for different stakeholders, such as executive summaries for the executive team and nitty-gritty controls for the security and IT implementers. The overarching purpose of the guide is to provide a how-to for organizations to recreate the National Cybersecurity Center of Excellence design, which includes:

- Using best practices for areas where there are no standards. The guide encourages use of security technical implementation guides for hardening systems, use of production-ready reporting servers, and malware prevention;

- Having automated configuration of security controls. The guide recommends automating security configurations so the configuration management tools can provide recovery capabilities in the event a configuration becomes corrupt or unusable;

- Creating detailed architecture and capabilities that address security controls. In addition to identifying use case architecture components (i.e., mobile devices/client side, networks, back end/server side, and secure infrastructure), the guide lists the high-level requirements for their build, including access control, audit controls and monitoring, device integrity, person or entity authorization, transmission security, security incidents, and recovery;

- Use of in-house, commercial and/or open source tools and technology. The guide uses easily available and interoperable tools and technologies so that organizations can effortlessly implement such tools and technologies into commonly used IT infrastructure and investments.

More mHealth Security Guidance on the Horizon

In addition to the guide, more mHealth security guidance is anticipated. On June 20, the FTC announced hearings on “Competition and Consumer Protection in the 21st Century” running from September 2018 through January 2019. The purpose of the hearings is to make time for “serious reflection and evaluation” on a range of issues, including competition and consumer protection issues in communication, information, and media technology networks, and the FTC’s remedial authority to deter unfair and deceptive conduct in privacy and data security matters. After the hearings, there may be additional guidance from the FTC on security matters, including other privacy and consumer protection topics.

In addition, a number of health care stakeholder groups led by the American Medical Association, the Health Information and Management Systems Society, the American Heart Association, ex-officio members from the U.S. Food and Drug Administration and the Office of the National Coordinator for Health Information Technology, and others, started a collaborative initiative called “Xcertia.” The group will be developing a set of guidelines that will give consumers and clinicians standards to able to judge mHealth apps based on content, privacy, operability and security. They are set to release a technical guideline later this year, followed by clinical guidelines early next year.

Gretchen Ramos is a shareholder and Zerina Curevac is an associate at Greenberg Traurig LLP.

The opinions expressed are those of the author(s) and do not necessarily reflect the views of the firms, their clients, or Portfolio Media Inc., or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.

[1] Global Market Insights, Inc, "Digital Health Market Technology [Telehealthcare {Telecare (Activity Monitoring, Remote Medication Management), Telehealth (LTC Monitoring, Video

Consultation)}, mHealth {Wearables (BP Monitor, Glucose Meter, Pulse Oximeter, Sleep Apnea Monitor, Neurological Monitor), Apps (Medical, Fitness)}, Digital Health System (EHR, e-prescribing System)], Industry Analysis Report, Regional Outlook (U.S., Canada, Germany, UK, Spain, Italy, Russia, Poland, Japan, China, India, Australia, Brazil, Mexico, South Africa), Application Potential, Price Trends, Competitive Market Share & Forecast, 2016 – 2024," available at https://www.gminsights.com/industry-analysis/digital-health-market?utm_source=ireach.prnewswire.com&utm_medium=referral&utm_campaign=Paid_ireach.prnewswire.com, published March 2018; Accenture, LLP, "Accenture 2018 Consumer Survey on Digital Health," available at https://www.accenture.com/us-en/insight-new-2018-consumer-survey-digital-health, published in 2018.

[2] National Institute of Standards and Technology, "Securing Electronic Health Records on Mobile Devices," SP 1800-1, available at https://csrc.nist.gov/publications/detail/sp/1800-1/final, published July 27, 2018.

[3] Change Healthcare, Inc., "The 8th Annual Industry Pulse Report," available at www.ChangeHealthcare.com/2018Results, published in 2018.

[4] LabMD, Inc. v. Fed. Trade Commission, 894 F.3d 1221 (11th Cir. 2018).

[5] HIMSS North America, "2018 HIMSS Cybersecurity Survey," available at https://www.himss.org/sites/himssorg/files/u132196/2018_HIMSS_Cybersecurity_Survey_Final_Report.pdf.

[6] Ponemon Institute, "2018 Cost of a Data Breach Study," available at https://www.ibm.com/security/data-breach, published July 2018.

[7] 2018 HIMSS Cybersecurity Survey.