Alert | Cybersecurity, Privacy & Crisis Management

August 2018

Securing EHRs on Mobile Devices According to NCCoE at NIST

After years of collaboration, the National Cybersecurity Center of Excellence (NCCoE) at the National Institute of Standards and Technology (NIST) has published a cybersecurity guide for electronic health record (EHR) applications on mobile devices (see "Securing Electronic Health Records on Mobile Devices," SP 1800-1, published July 27, 2018). Even if your organization has prioritized mobile application cybersecurity, it is worth comparing the guide recommendations to your current mobile application cybersecurity posture to identify any potential gaps.

The guide was developed by industry and academic cybersecurity experts, with the input of health care providers who first identified the challenge in a 2012 U.S. Department of Health & Human Services (HHS) Mobile Devices Roundtable. At the roundtable, some of the security concerns included general data loss and theft, unauthorized access to enterprise networks via unsecured mobile devices or untrusted network connections, and vulnerabilities associated with routine operations (e.g., data synchronization and storage, etc.) due to interactions with mobile devices.

The purpose of the guide is to address the concerns voiced in the roundtable and to demonstrate the types of tools that can be used to increase the security of health information as it is collected, stored, processed, and transmitted on mobile devices, particularly in the context of mobile applications and systems that review, update, and exchange EHRs. To develop the guide's recommendations, the NCCoE built a virtual environment to simulate interactions between mobile devices and EHRs, such as sending referrals between physicians or electronic prescriptions to a pharmacy, and used commercially available and open source technologies to improve the privacy and security protections of its mobile device EHR solution.

The guide incorporates standards and best practices contained in the NIST Cybersecurity Framework and Health Insurance Portability and Accountability Act (HIPAA) Security Rule. In addition to mapping to the NIST and HIPAA standards, the guide also:

- **Utilizes best practices for areas where there are no standards.** The guide makes best practice recommendations such as malware prevention and detection of antivirus, use of security technical implementation guides for hardening systems, and use of production-ready reporting servers.
- **Provides detailed architecture and capabilities that address security controls.** The guide identifies the use case architecture components (i.e., mobile devices/client side, networks, back end/server side, and secure infrastructure) and 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.
- **Promotes automated configuration of security controls for ease of use.** The guide provides recommendations for automating security configurations so the configuration management tools can provide recovery capabilities in the event a configuration becomes corrupt or unusable.
- **Recommends both in-house, commercial and/or open source implementation to help organizations build on existing infrastructure**. The NCCoE uses a layered strategy to achieve its results in the guide, and the implementations offered in the guide are easily available and interoperable with commonly used IT infrastructure and investments.
- **Provides a how-to for organizations to recreate the NCCoE design**. The guide dives into great detail for security engineers and implementers, allowing them to pick and choose recommendations to build a solution based on their unique circumstances.

While the guide is quite lengthy at 260 pages, it offers bite-size sections targeted at different privacy and security stakeholders of an organization. For example, the executive summary is targeted towards an organization's leaders (e.g., chief security or technology officer), while technology or security program managers are much more likely to focus on the approach and risk management sections of the guide.

Authors

This GT Alert was prepared by **Gretchen A. Ramos** and **Zerina Curevac**. Questions about this information can be directed to:

- Gretchen A. Ramos | +1 415.655.1319 | ramosg@gtlaw.com
- Zerina Curevac | +1 415.655.1275 | curevacz@gtlaw.com
- Or your Greenberg Traurig attorney

Albany. Amsterdam. Atlanta. Austin. Boca Raton. Boston. Chicago. Dallas. Delaware. Denver. Fort Lauderdale. Germany.¬ Houston. Las Vegas. London.* Los Angeles. Mexico City.+ Miami. New Jersey. New York. Northern Virginia. Orange County. Orlando. Philadelphia. Phoenix. Sacramento. San Francisco. Seoul.∞ Shanghai. Silicon Valley. Tallahassee. Tampa. Tel Aviv.^ Tokyo.¤ Warsaw.~ Washington, D.C. West Palm Beach. Westchester County.

This Greenberg Traurig Alert is issued for informational purposes only and is not intended to be construed or used as general legal advice nor as a solicitation of any type. Please contact the author(s) or your Greenberg Traurig contact if you have questions regarding the currency of this information. The hiring of a lawyer is an important decision. Before you decide, ask for written _information about the lawyer's legal qualifications and experience. Greenberg Traurig is a service mark and trade name of Greenberg Traurig, LLP and Greenberg Traurig, P.A. ¬Greenberg Traurig's Berlin office is operated by Greenberg Traurig Germany, an affiliate of Greenberg Traurig, P.A. and Greenberg Traurig, LLP. *Operates as a separate UK registered legal entity. +Greenberg Traurig's Mexico City office is operated by Greenberg Traurig, S.C., an affiliate of Greenberg Traurig, P.A. and Greenberg Traurig, LLP. ∞Operates as Greenberg Traurig LLP Foreign Legal Consultant Office. ^Greenberg Traurig's Tel Aviv office is a branch of Greenberg Traurig, P.A., Florida, USA. ¤Greenberg Traurig Tokyo Law Offices are operated by GT Tokyo Horitsu Jimusho, an affiliate of Greenberg Traurig, P.A. and Greenberg Traurig, LLP. ~Greenberg Traurig's Warsaw office is operated by Greenberg Traurig Grzesiak sp.k., an affiliate of Greenberg Traurig, P.A. and Greenberg Traurig, LLP. Certain partners in Greenberg Traurig Grzesiak sp.k. are also shareholders in Greenberg Traurig, P.A. Images in this advertisement do not depict Greenberg Traurig attorneys, clients, staff or facilities. No aspect of this advertisement has been approved by the Supreme Court of New Jersey. ©2018 Greenberg Traurig, LLP. All rights reserved._