By: Debra N. Diener, J.D., CIPP/G; blog at Privacy Made Simple

Consumers have access to ever increasing numbers of mobile apps providing health, fitness and wellness information. Many consumers might assume that entering personal information, and especially personal health information, to gain access to the information would be very protected. That assumption needs to be reconsidered in light of excellent reports recently issued by the Privacy Rights Clearinghouse (PRC).

PRC has just finished a nine month project analyzing 43 popular mobile health, wellness and fitness apps–23 free and 20 paid. The PRC performed a technical risk assessment to learn what data the apps were collecting, storing and transmitting over the network. The apps are ones geared for consumers' use on a wide-range of the above topics. PRC does not identify the apps by name; however, they are ones that can be found in the Apple App Store for iOS and the Google Play Marketplace for Android apps. The reports and a helpful summary "Fact Sheet" can all be found on the PRC's website

The reports provide in-depth findings on a range of issues. I've selected just a few of PRC's key consumer-oriented findings:

- Privacy policies are found in the app or on the developer's website for 74% of the free apps and 60% of the paid apps; however, that means that 26% of the free apps and 40% of the paid apps do not have a privacy policy;
- Only 13% of the free apps and 10% of the paid apps encrypt all connections to the developer — the rest are sending consumer data in the clear without any encryption;
- 39% of the free apps and 30% of the paid apps send data to someone not covered in their privacy policy;
- 52% of the free apps and 30% of the paid apps notify consumers that they might share data with advertisers; and
- 72% of the apps analyzed presented medium to high risk in terms of personal privacy; paid apps presented the lowest privacy risk to users.

All of the above-findings present different consumer concerns. However, the finding that personal data is being sent unencrypted and in the clear is particularly troubling. Personal, financial and health data could be disclosed to others on that network. What could that lead to? Consumers could be embarrassed or become identity theft victims if their information is stolen.

PRC offers several excellent “consumer tips” on their website based on the various findings. An important threshold “tip” is that consumers need to research an app before downloading it and gauge their comfort level with the personal information being requested before being able to use the app.