



mHealth Anti-Cloning Encryption Method Gets U.S. Patent

By Renee Boucher Ferguson

TORONTO, Ont.—Diversinet Corp, an R&D-based mobile communications company, has received a new U.S. Patent for an encryption method that looks to address mHealth data security concerns.

Announced November 2, Diversinet's Anti-Cloning Encryption Method, or U.S. Patent #8,051,297, uses encryption methods to prevent unauthorized access to sensitive medical data on a mobile device—a smartphone or tablet, for example—and prevents access to the data if its transferred to another mobile device. Unlike some encryption methods that use a PIN number to lock and unlock data, Diversinet's technology uses characteristics of a mobile device's unique identity—its serial number—to create the encryption passkey.

The idea with the Anti-Cloning Encryption Method is that it offers a layer of security that enables healthcare payers and providers to safely utilize information that patients carry on their mobile devices. The information is accessible even when patients are temporarily out of network coverage areas.

The company develops and sells two major products, its MobiSecure Communicator, an application that enables healthcare organizations to deploy HIPPA-compliant mHealth apps on any mobile device, supporting secure data messaging, for example, in the form of alerts, question/response and advanced questionnaires. It also lets users manage healthcare data from a mobile phone, tablet or desktop computer.

At the same time Diversinet markets its MobiSecure Gateway SDK (software development kit) that helps healthcare developers build MobiSecure functionality into their mHealth applications. The security functionality includes encryption and OATH-standards based One-Time Password for authentication.

This latest encryption patent—Diversinet has 16 security and mobility patents from the US, Canada and Israel, with 32 applications in the works—is integrated into the company's MobiSecure mHealth products.

Mobile Use Growing

The use of mobile technology is growing in healthcare organizations—and among consumers—at a rapid clip, according to several recent studies. In its annual "Taking the Pulse" study of physicians and health care technology, Manhattan Research found that as of April 2010, 72 percent of doctors use smartphones personally and professionally. That number is expected to jump to 81 percent in 2012.

A separate study by Springer Publishing, Nursing eBook & Smartphone Survey, released in September 2011 found that of more than 1,000 nurses surveyed, 75 percent own a smartphone. Nearly 50 percent of the nurses surveyed have downloaded and used a medical application, while close to 30 percent have purchased a nursing or medical eBook.

On the consumer front, it's estimated that between 80 percent and 90 percent of the U.S. population has a mobile phone.

While there are a number of factors driving a convergence of medical professionals and patients through mHealth devices—from regulatory mandates and economic incentives to consumer interest and ease of use—the actual deployment of mHealth applications and secure data transmission falls to healthcare IT.

In a recent white paper sponsored by Diversinet, "Ten Questions You Should Ask Before Implementing An mHealth Solution," the company suggests healthcare IT pros come armed with a list of questions before implementing any vendor's security solutions. That list includes two seemingly relevant questions as the nascent mHealth field takes hold: 'Can you provide reference accounts that have moved beyond pilot projects?'; and 'Does your solution provide all the Technical Safeguards listed in the HIPAA Security Rule?'