



onemedSENTINEL

LATEST TECHNOLOGY DEVELOPMENTS

Protecting Healthcare Data In a Mobile World

[HIPAA Security Guide](#)

Mobile Healthcare Data Poses A Risk Learn More, Download The Whitepaper



[ADT@ Security Test](#)

Get An ADT@ Security System - Only \$99 Installed After \$150 Rebate!

Ads by Google



It's not paranoia, the saying goes, if they're really out to get you. Experts have predicted that [medical identity theft will increase](#) as more healthcare providers switch to electronic medical records. As if to punctuate the point, someone recently [hacked into 957 patient records](#) at Connecticut's Griffin Hospital and downloaded image files from 339 patients. No financial or Social Security data was contained in the records, but someone did call the patients soliciting business for a competing hospital. A disgruntled radiologist who was fired from Griffin Hospital in February stands accused of the crime.

Mobile healthcare devices, too, are susceptible to hacking. A [2008 study](#) found that defibrillators can be hacked wirelessly. Devices such as heart monitors and glucose infusion pumps transmit data to doctor's offices and mobile devices. Smartphones can monitor patient health and hold electronic medical records. Research and advisory firm NERAC [estimates](#) that by 2020, at least 160 million Americans will be monitored remotely for at least one chronic condition. Between the trend toward remote monitoring and the growing use of smartphones, that's a lot of private data flying back and forth. How to ensure that it stays private?

According to Jay Couse, Senior Vice President of mobile security provider [Diversinet](#), the healthcare industry is harmed by an underfunded, disorganized approach to security. Couse says that it takes significantly longer to catch medical identity theft than financial identity theft. That's because financial institutions use the same software to check for unauthorized or aberrant use of credit cards. They cooperate and communicate with each other. In contrast, the medical industry spends 10 times less on security, and there's less sharing between healthcare organizations, which exposes patient records to attack.

Couse believes that [Diversinet](#) has the solution to mobile health hacks. The Toronto-based company markets its products to providers, payers and employers. [Diversinet](#) utilizes multiple levels of security to ensure that patient records stay private. Once a patient has been authenticated, he or she is given a unique activation code and asked to select a PIN number. The system utilizes bilateral authentication in data transmission: the mobile device authenticates the server, and the server authenticates the mobile device. All data is double-encrypted to add an extra layer of security.

[Diversinet](#) is partnered with an Ontario medical clinic to test Mihealth, a mobile health solution that gives patients 24/7 access to their medical information. The three-month project is intended to help patients more effectively manage their healthcare, reduce physician workload, and improve patient compliance. Patients can edit their personal health records, although all data must be verified by the physician. The program has been so successful that the trial has been extended by another three months. [Diversinet](#) was also recently selected by the U.S. Army for secure authentication between wounded warriors and their case managers. The Army has a 40 percent no-show rate for appointments, and the government is hoping to increase compliance among soldiers. Couse says that the market opportunity for [Diversinet](#) security is huge. "If you look in the U.S., just under 300 million phones—every one of those is a potential user of our application," says Couse.

Traditional, non-mobile EMRs require security as well. Companies such as Venyu and CynergisTek are known for providing security solutions to the healthcare industry. No matter the device, data protection is a critical part of a strong healthcare IT infrastructure. The ideal security solution strikes a balance between convenience and privacy, ensuring that incidents like the security breach at Griffin Hospital don't have a chance to occur.

What's your take on mobile device security? What will it take to create an environment where medical devices and patient records are safe from outside interference?

7 April 2010 | [Blog, feature2](#) | [vanderson](#) | [Comments](#)



Search

Navigation

- [OneMedPlace](#)
- [Med Tech Sentinel](#)
- [Twitter](#)

Meta

- [Subscribe by Feed](#)
- [Subscribe to Newsletter](#)

Archives

- [August 2010](#)
- [July 2010](#)
- [June 2010](#)
- [May 2010](#)
- [April 2010](#)
- [March 2010](#)
- [February 2010](#)
- [January 2010](#)
- [December 2009](#)
- [November 2009](#)
- [October 2009](#)
- [September 2009](#)
- [August 2009](#)
- [July 2009](#)
- [June 2009](#)
- [May 2009](#)
- [April 2009](#)
- [March 2009](#)
- [February 2009](#)
- [January 2009](#)
- [December 2008](#)
- [November 2008](#)
- [October 2008](#)
- [September 2008](#)
- [August 2008](#)
- [July 2008](#)
- [June 2008](#)
- [May 2008](#)
- [April 2008](#)
- [March 2008](#)
- [February 2008](#)
- [January 2008](#)
- [December 2007](#)

November 2007

October 2007

September 2007

August 2007

July 2007

June 2007

May 2007

April 2007

March 2007



CONTRIBUTOR TO BLOGS ON DEMAND



© 2010 OneMedPlace

[About Us](#) | [Advertise](#) | [Contact](#) | [Log In](#) | [Sign Up](#) | [TV](#) | [Companies](#) | [Resources](#) | [Sentinel](#) | [Digest](#)