

Keeping mHealth Services Safe & Secure

Posted In: [Healthcare](#) | [Safety & Security](#) | [Wireless Week Magazine](#)

By Monica Allevan Sunday, July 18, 2010

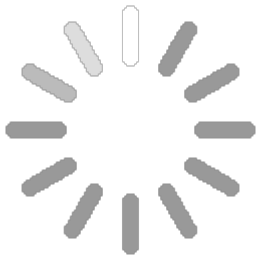


[Email](#)

[Print](#)

5
tweets

[retweet](#)



Security is a concern for everyone, but it's arguably most pronounced when it comes to the areas of financial services and healthcare, two places where a little breach can make for major catastrophes.

Cases of wireless security breaches continue making headlines. So far, they've steered away from the type that involves life or death situations, and a lot of experts are working hard to make sure it stays that way.

In a New England Journal of Medicine (NEJM) article earlier this year, co-authors Dr. William Maisel of Beth Israel Deaconess and Tadayoshi Kohno of the University of Washington raised the need for improving the security and privacy of implantable medical devices – the types of devices that perform complex analyses, store detailed personal medical information and communicate remotely and wirelessly.

“Although few patients are known to have been harmed by security breaches of medical computers or devices, the security of medical devices is not a luxury,” they wrote. “We must develop a security paradigm for medical devices that welcomes important technological advances while ensuring the well-being of millions of medical-device recipients.

“While the report specifically addresses implantable medical devices, others are concerned about other types of healthcare breaches. A study by Forrester Consulting and commissioned by Maas360/Fiberlink shows healthcare IT decision makers are concerned about security, and for good reason. In the study, 31 percent noted their data had been compromised at least once over the course of 2009 and more than 10 percent had more than one breach in just one year. Asked about mobile devices specifically, nearly 63 percent selected “understanding the risks and vulnerabilities” as their top challenge when dealing with mobile workers.

SOLUTIONS TO THE RESCUE

Security software companies like Diversinet intend to be there when healthcare organizations come knocking – and they're already doing so. The company started out on the financial services side of the house, developing authentication tools for secure financial transactions, but its focus now is squarely on healthcare, with its tagline: Healthcare. Connected & Protected.

While a lot of the company's financial solutions translated well into healthcare, there are some big differences between the two sectors, says Jay Couse, senior vice president at Diversinet. For one, health insurance companies are very

fragmented when compared with financial services. Banks immediately share intrusion information among themselves and “if you try to attack Citibank, by the time you show up at Bank of America, they already know you,” he says.

Not so with healthcare. When a thief steals someone’s identity and undergoes an expensive operation on another’s healthcare dime, thousands of dollars may have been spent before anyone catches it. “The amount of money obtained through health fraud is huge,” he says.

Toronto-based Diversinet has a growing list of patents designed to keep information safe for patients, healthcare providers and payers, and it recently added another one that provides what it calls “unprecedented” security for both mobile financial transactions and healthcare records. It helps licensees that transmit information wirelessly ensure compliance with industry best practices and security requirements in laws such as the Personal Health Information Protection Act (PHIPA) in Canada and the Health Insurance Portability and Accountability Act (HIPAA) in the United States. The company’s recent patent features pseudonymic digital identifiers, which are random strings of numbers that act as aliases for user names.

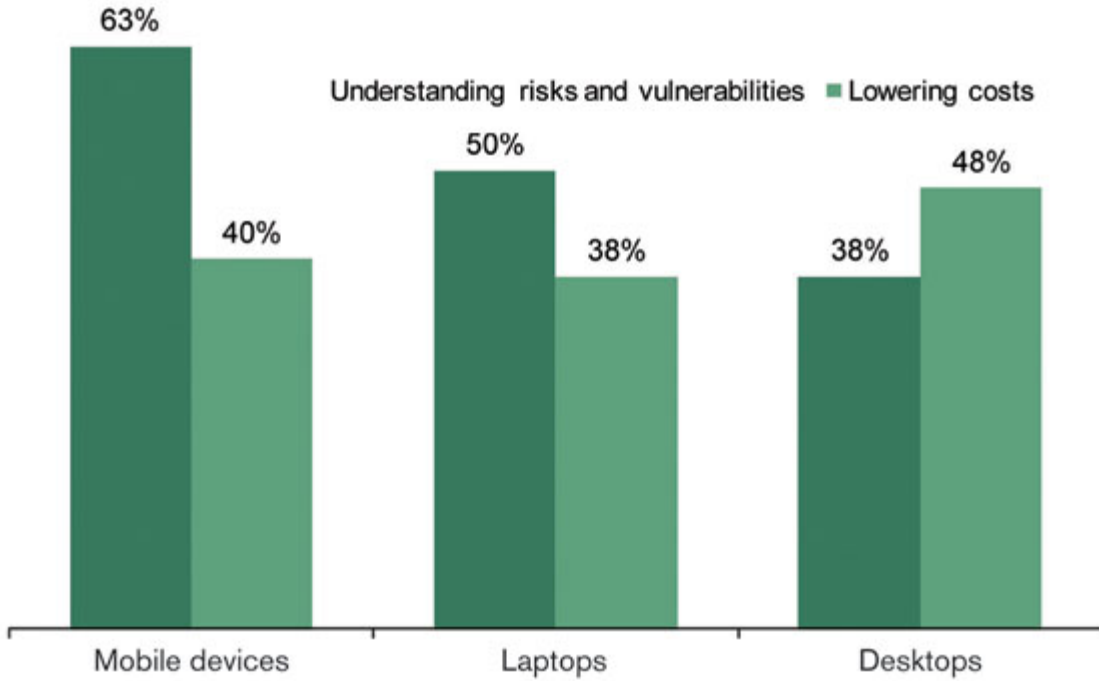
Diversinet also offers an SMS solution to healthcare institutions with employees who don’t own smartphones or subscribe to a data plan. In some ways, SMS is considered one of the least secure modes when compared with Web or application-based wireless delivery mechanisms. SMS messages travel “in the clear,” Couse says, from one carrier’s server to another carrier’s server, and users rarely clear out their in and out boxes, making them susceptible to the prying eyes of someone else who happens to pick up their device.

Diversinet devised ways to make the SMS route more secure by using strong encryption and authentication. Its MobiSecure SMS product also offers assurance that messages have been successfully received by the intended recipient, and a remote access wipe capability allows for erasing sensitive data in the event a device is lost or stolen.



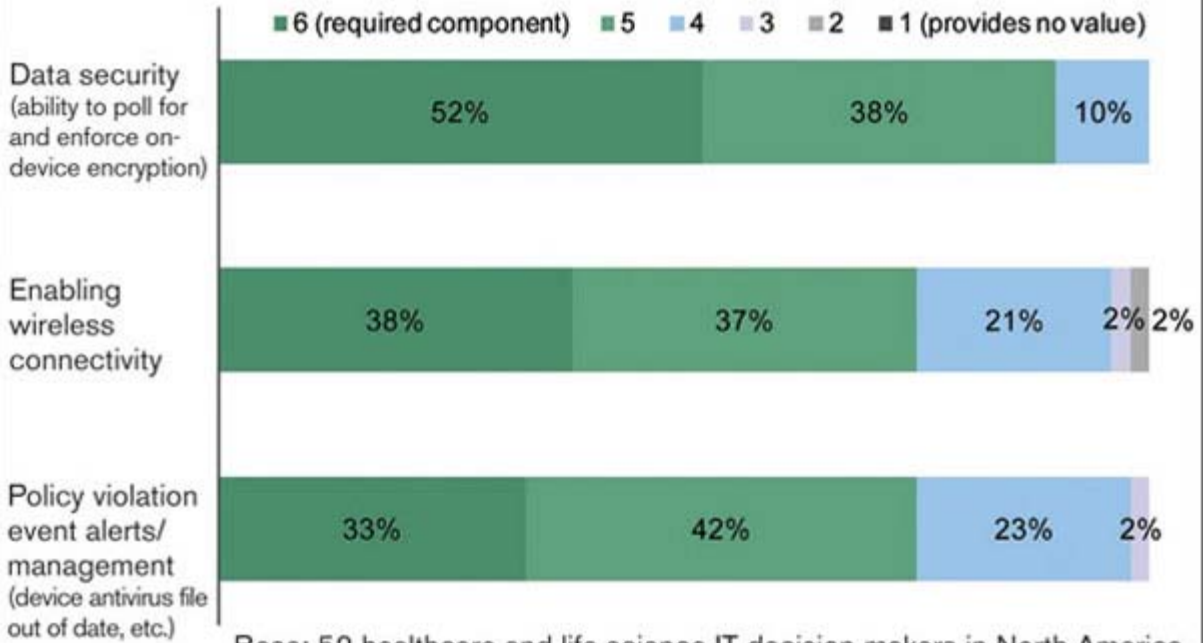
Diversinet provides security solutions for mobile healthcare services that run across device platforms. (Image courtesy of Diversinet.)

Which of the following are among the top three issues your organization faces in supporting a mobile device?



Base: 52 healthcare and life science IT decision-makers in North America

Rank the value of including the following features in a mobile user management tool



Base: 52 healthcare and life science IT decision-makers in North America

Source: A commissioned survey conducted by Forrester Consulting on behalf of MaaS360 by Fiberlink.

TAKING OWNERSHIP

The proliferation of smartphones and the amount of personal information they carry led Lookout to create a

consumer app that will detect mischievous apps, and it has seen some interest from folks in the healthcare industry, says CEO John Hering. A lot of doctors are asking about Android phones and want to know how Lookout can keep them safe, but the company isn't actively targeting the enterprise or healthcare sectors at the moment.

Until recently, mobile hacking has been about fame, but it's starting to move to "fortune," whereby criminals are getting into the act to make money, he says. And it's going to take ownership from everyone, including OEMs, operators and application developers, to provide security as hackers get more sophisticated, he says.

The authors of the NEJM article no doubt would agree, and add a few more participants when it comes to healthcare specifically. A specific regulatory framework for device security "should be developed through a multidisciplinary, collaborative initiative led by the FDA and involving device manufacturers, the computer-security community, regulators, medical practitioners, professional medical societies, patients and patient-advocacy groups," they wrote. "Ultimately, the required security controls should be commensurate with the potential risks to patients."

On the Road to Digitizing Records

The American Reinvestment and Recovery Act includes funding to get health records into electronic form, so how's that going?

For the ambulatory physician space, which involves medical care delivered on an outpatient basis, it depends on who you ask, says Patti Dodgen, CEO of healthcare information exchange Hielix. In one survey through the Texas Medical Association last year, about 43 percent of physicians reported they had implemented an electronic medical record (EMR) system.

But Hielix executives and other experts say that number is hyper-inflated with doctors who believe they have an EMR because they are e-prescribing or using a practice management software product. The actual percentage of ambulatory doctors fully using EMR software as of the fourth quarter of 2009? More like 4 percent to 6 percent, Dodgen says.

Dodgen, who notes that the healthcare industry is second only to mining in its resistance to information technology, says one of the reasons doctors didn't move faster is the software and solutions weren't that good. Doctors were told they would need to spend thousands of dollars on servers and software licensing – and some of them did, living to tell horror stories about costly installations that turned out to be as useful as a simple scanner.

However, the situation is changing as legitimate vendors offer hosted solutions. "It's very, very different today," she says.

More good news: The government's push to adopt EMR, backed by the stimulus dollars, is driving health-care IT spending. Compass Intelligence says healthcare organizations – including hospitals, doctors' offices, private practices, clinics and others – will spend an estimated \$73.1 billion this year on IT products, services and solutions. About \$705.8 million will be spent on mobile applications in 2010, according to Compass.

Wireless service providers typically don't construct separate call centers for handling questions about billing and service and another to field questions about healthcare. But that's what GreatCall, the San Diego, Calif., company behind the Jitterbug phone service, did.

Besides offering no-contract service plans, Jitterbug offers wellness services with daily health tips to keep people motivated. At a higher level of engagement, however, is its Jitterbug LiveNurse service, which for \$4 a month provides 24-hour access to live registered nurses. Of course, the company also needs to keep information about those kinds of calls separate from the regular customer care department.

A couple years ago, GreatCall started partnering with the likes of Meridian Health and others to measure and benchmark the benefits of wireless, both for people who are healthy and those under more constant care of a healthcare provider, explains Ray Morris, COO for GreatCall. "As we work through these initiatives, we also work through implications that wireless health brings, not just safeguarding customer data but patient data," he says.



Ray Morris

The privacy policy section of Jitterbug's website includes a section on how Jitterbug is required to protect customer proprietary network information (CPNI), a common practice in the wireless industry. But another section lists ways in which the company may use and disclose health information about customers, which fall into the following categories: reminders; health-related benefits and services; to avert a serious threat to health or safety; and "as required by law," which means when federal, state or local law dictates.

The company spent more than a year working with Health Insurance Portability and Accountability Act (HIPAA) and other experts in healthcare to learn the ropes. "It took us the better part of 18 months to get to where we are now," Morris says. "The liability is great and that makes everyone very careful."

That said, the healthcare industry already has addressed many privacy issues over the years, so relying on healthcare experts was a big part of the solution – and it helps that Southern California happens to be home to a lot of those experts.