



Software	Security	Cloud	Mobility	Social Business	Personal Tech	Hardware	Windows	Global CIO	Government	Healthcare	Financial	SMB		
Administration Systems	Clinical Information Systems	CPOE		Electronic Medical Records	Healthcare Blogs	Healthcare IT Buyers' Guide		Healthcare Stories	Interoperability	Leadership	Mobile & Wireless	The Patient	Policy & Regulation	Security & Privacy



41 [Like](#) [8](#) [Share](#) [0](#) [Print](#) [Permalink](#) [RSS](#)

Get InformationWeek Daily

Don't miss each day's hottest technology news, sent directly to your inbox, including occasional breaking news alerts.

Federal ID Strategy To Boost Health Data Security

Voluntary plan which seeks two-factor authentication and for online identity management should find wide application in healthcare.

By [Neil Versel](#) InformationWeek
April 26, 2011 11:38 AM

A federal plan to involve the private sector in beefing up online identity management and user authentication, while also making it easier for individuals to manage passwords, should find plenty of applications in healthcare—which is exactly what the Obama administration envisions.

The [National Strategy for Trusted Identities in Cyberspace](#), a roadmap released earlier this month for protecting consumers from fraud and identity theft, calls for the voluntary building of an "identity ecosystem" in which consumers can have a single, user-specific credential to log into any participating website. This, according to federal officials, will allow security-conscious sectors, including healthcare and finance, to make new online services available.



Slideshow: RFID In Healthcare

(click image for larger view and for full slideshow)

"[I]ndividuals and businesses need to be able to check each other's identity for certain types of sensitive transactions, such as online banking or accessing electronic health records," the 52-page [document](#) reads. Among other things, the strategy calls for wider adoption of two-factor authentication and unique security credentials for each user.

This is exactly the sort of thing healthcare needs, according to Hussam Mahgoub, senior VP for corporate development and research—and resident security specialist—at [Diversinet](#), creator of a secure platform for developing mobile healthcare applications. "There's a lot of confusion in the marketplace about security and privacy," Mahgoub said.

Of particular worry, according to Mahgoub, is that the Health Insurance Portability and Accountability Act's (HIPAA) privacy and security regulations don't address "strong authentication" for users when they access protected health information (PHI).

Diversinet, which is based in Toronto but does most of its business in the United States, recently published a white paper listing nine best practices for securing health data on mobile networks and devices, that in many ways dovetails with the federal strategy. Diversinet recommends installing apps on smartphones, tablets, and laptops to turn each device into a kind of "wallet" for PHI. Sensitive data should be encrypted and the app should be able to deactivate or delete PHI from lost or stolen devices, just as banks and retailers can deactivate lost credit cards, Mahgoub explained.

More Healthcare Insights

White Papers

- [Enabling Fast and Secure Clinician Workflow with One-Touch Desktop Roaming](#)
- [Creating smarter healthcare products: Balancing marketplace needs with strategic goals and profitability](#)

Analytics

- [Strategy: BI and Analytics in Healthcare](#)
- [Database Defenses](#)

Webcasts

- [Effective IT Inventory and Asset Management: From Quagmire to Quick Fix](#)
- [Outsourcing Security: What Every Potential Cloud Security Customer Should Know](#)

Videos

THIS WEEK'S ISSUE



[Back Issues](#)

- [Subscribe to InformationWeek](#)
- [Subscribe to Digital](#)
- [Read the Cover Story](#)
- [Download Current Issue](#)

CURRENT HEALTHCARE ISSUE



[Back Issues](#)

In this issue:

- **Cloud Rx:** Not every application is ripe for the cloud. We look at two case studies that offer insight into what does work.
- **HIPAA Pain:** Keeping patient data secure isn't all that hard.



HP's Chairman, Ray Lane, sat down for an exclusive fireside chat and discussed the company's strategy, product direction and some of the missteps in communicating all of that to its customers.

Jeff Sponaugle, chief security and technology officer for Beaverton, Ore. healthcare connectivity company Kryptiq, sees at least one recent change in healthcare that needs this kind of approach. Interim Drug Enforcement Agency (DEA) [regulations](#) that took effect in June 2010 allow the electronic prescribing of certain controlled substances such as narcotics, but only with enough security in place to satisfy the law enforcement community, which has a lot more pull with the DEA than does the health IT industry.

"With electronic prescribing of controlled substances, two-factor authentication will be coming to the desktop of physicians and staff," Sponaugle said in an email. "The requirements for [electronic prescriptions for controlled substances] are very clear and do provide a 'need' for the physician to get some kind of digital ID."

Sponaugle noted, however, that two-factor authentication and other "strong" forms of digital security have been around for years, but often place too high of a burden on users to encourage widespread adoption. Resistance may rise when the users happen to be time-crunched and technologically challenged physicians.

"The key for promoting two-factor is to make it integrated into the application the doctor uses most," reported Sponaugle, who said that Kryptiq tries whenever possible to integrate its platform for secure messaging and e-prescribing into other companies' electronic medical records (EMRs). "As the EMRs add front-facing, two-factor workflows, we will use that same infrastructure for messaging. It would be a disaster if you made a doctor use a different two-factor system for the EMR, and yet another different system for messaging or prescribing," Sponaugle said.

"In the end, the goal of the second factor is to provide some protection from the key problem in security, which is people. People choose poor passwords, reuse them, tell them to people, log in from a kiosk in a coffee shop with a key logger, etc.," Sponaugle added. "Coming up with good workflow usability of the two factors is what will make it succeed."

Read *InformationWeek Healthcare's first-ever compilation of the executives leading the digital transformation of the healthcare industry. They're the innovators and early adopters, and the visionaries for what comes next.* [Download it now.](#) (Free registration required.)

Comments [Quick View](#) [Full View](#) 1 Comments

Most recent comment

YEAH, I TRUST THEM

Comment by UberGoober Apr 26, 2011, 12:17 PM EDT

We're going to put all our security in a system brought to us by the same folks who make the Post Office and the DMV and the Passport Office work so well? And don't forget the Can-SPAM act. The same folks who send paper mail to you every year in a clearly identifiable envelope that contains your social security number and your name and address? I don't think so, Tim.

The government (at all levels, but particularly Federal) does very few things well, and far fewer in a cost efficient way, The overlap between these two tiny subsets is the null set. Keep that in mind when you find yourself thinking "The government ought to do something about so-and-so." You might get your wish.

[Reply To Comment](#) [Permalink](#)
[Share Email Report](#)

[Yeah, I trust them](#) Comment by UberGoober Apr 26, 2011, 12:17 PM EDT

Care to Comment?

Subject (max length: 75):

Comments:

But proposed new regulations could make it a lot harder.

- [And much more!](#)
- [Read the Current Issue](#)

TECHNOLOGY WHITEPAPERS

- [The Time Is Now for Considering Workload Automation](#)
- [Market Overview: IT Process Automation, Q3 2011](#)
- [Automating SAP System Copy](#)
- [Beyond Job Scheduling: The Road To Enterprise Process Automation](#)
- [Roadmap to Agility: Four Steps to Achieving Resiliency in the Data Center](#)

FEATURED WHITEPAPER

[A smarter approach to healthcare transformation: Becoming more agile, nimble and responsive to industry change](#)

Learn how your company can become more agile, nimble and responsive to change and transformation. [Learn More](#)

INFORMATIONWEEK ANALYTICS

FEATURED ANALYST BRIEF

[Why We Need Usage-Based Accounting](#)

FEATURED ANALYST REPORT

[Very Virtual: Storage For Highly Converged Networks](#)

[Subscribe to InformationWeek Analytics](#)

Find hundreds of reports featuring research from your peers, and best practices from top IT pros. Subscriptions \$39 per month or \$399 per year.

- Exclusive Research
- CIO Guides
- Best Practices
- Technology Adoption Trends
- ROI Methodologie

Don't get lost in the cloud!
FREE ANALYTICS REPORT
on cloud computing contracts
enterprise efficiency [Download it now!](#)

NEW YORK // OCTOBER 3-7, 2011 **INTEROP**
 See the Future of IT at Interop
[Register Today](#)

VIDEO