Collaboration Needed to Improve Health IT Security

Posted At : October 2, 2014 10:12 AM | Posted By : Kyra Fussell
Related Categories: Critical Infrastructure Protection, Health IT, Health and Human Services, Health Care, Information Security, Cybersecurity, Department of Commerce

The Department of Health and Human Services' (HHS) Office for Civil Rights (OCR) and the Department of Commerce's National Institute of Standards and Technology (NIST) hosted the seventh annual conference on Safeguarding Health Information on September 23 and 24, 2014. Exploring information assurance through the Health Insurance Portability and Accountability Act (HIPAA) Security Rule, the event covered topics including breach management, technical assurance of electronic health records, and integrating security into health IT.

The keynote address that kicked off the event was delivered by Darren Dworkin, the chief information officer and senior vice president for of enterprise information systems for Cedars-Sinai Health System. Dworkin described major security events that have shaped security architecture. For example, 2003's Blaster RPC Worm led to better security patch management as well as improvements to antivirus deployment. More recently, Heartbleed resulted in enhancements to security scanning and inventory. Dworkin noted that hackers have not been the only threat. In fact, 35% of patient data breaches in 2013 were due to loss or theft of unencrypted laptops or other devices. The recent explosion of medical devices and mobile computing are further changing the landscape for health IT security. As new technologies change how data is accessed and shared, protecting health information becomes increasingly challenging.

Other speakers at the event stressed hurdles around risk assessments and promoting end-user awareness. One speaker from the HHS observed that it's impossible to achieve effective risk management if organizations don't know what their risks are. Another presentation (from industry) emphasized the importance of encrypting data at rest, in transit, or in process. One major takeaway from the event was the need for health care organizations to perform comprehensive security risk assessments. There's no such thing as eliminating vulnerability or being "risk proof." The key is managing risks, but first organizations need to know what those risks are.

While speakers described a broad range of challenges and setbacks related to safeguarding healthcare information, the burden of progress must be shared by the whole community. As the Food and Drug Administration's Suzanne Schwartz put it, "No one organization, no single government agency, no sole stakeholder, manufacturer, healthcare facility, provider, information security firm is going to be able to address and solve these issues on their own ." Schwartz's comments echoes **a recent blog entry** from the White House Cybersecurity Coordinator, which stressed the need for collaboration between government and industry to strengthen the nation's information security posture.

Vendors will find a number of opportunities to engage with government in the discussion around cybersecurity improvements. For example, NIST is **accepting comments** on its Framework for Improving Critical Infrastructure Cybersecurity until October 10, 2014. Later in October, the Food and Drug Administration will be holding **a public workshop** on adapting medical device cybersecurity. These discussions will help lay groundwork for partnerships, identify best practices, and may help shape requirements for future guidance.

---

*Originally published in the **GovWin FIA** Analysts Perspectives Blog. Follow me on Twitter **@FIAGovWin**.*