

Five trends in healthcare IT – and their implications for security

Posted on **July 17, 2013** by **David Kotz**

In the [previous post](#) we described the current landscape for healthcare information technology. In this post, we note how healthcare information systems increasingly face daunting security challenges due to five economic and technological trends. First, the locus of care is shifting, as the healthcare system seeks more efficient and less-expensive ways to care for patients, particularly outpatients with chronic conditions. Second, strong economic incentives are pushing health providers to innovate by rewarding providers for keeping their patient population healthy, rather than paying only to fix patients when they are ill. Third, the treatment of chronic conditions and the implementation of prevention plans entail more continuous patient monitoring, outside of the clinical setting. Fourth, mobile consumer devices (smartphones and tablets) are quickly being adopted for health & wellness applications, both by caregivers and patients, in addition to their many other uses – making it difficult to protect sensitive health-related data and functions from the risks posed by a general-purpose Internet device. Finally, significant emerging threats are targeting healthcare information systems, while new regulations strive to protect medical integrity and patient privacy. Let's look at each of these five trends in more detail.

Trend 1: Shifting locus of care.

Efforts to reduce healthcare costs, improve treatment effectiveness, and encourage individual wellness are driving changes in the manner and location in which care is delivered to individuals. More healthcare is delivered through small clinics (witness the spread of satellite clinics developed by major hospitals), elder-care centers (witness the dramatic emergence of assisted-living communities), or at home with remote interactions between patients and caregivers (witness a flood of products for tele-healthcare and remote patient monitoring). Distributed clinics and centers will increasingly rely on cloud services to manage health data: federal incentives are pushing all clinical providers toward the use of electronic health records (EHRs), and small and medium-sized clinics and hospitals may find it easiest to adopt a cloud-based EHR [9, 10, for example]. Patients and clinical staff alike will move among hospital, clinic, and residence, using their mobile devices to collect, view, and act on health-related information from anywhere, any time.

Trend 2: Accountable care and patient engagement.

The Affordable Care Act of 2010 pointed to Accountable Care Organizations (ACOs) as one way to control costs by significantly reducing unnecessary medical care, improving health outcomes, and encouraging preventative health behaviors. ACOs are healthcare organizations that link payment (as well as revenue sharing) to providers contingent on meeting high-quality and low-cost targets for an assigned population of patients. (ACOs now serve approximately 31 million patients and their rate of growth is expected to explode in 2013.) With ACOs, payment shifts away from the traditional fee-for-service model, towards payments linked to evidence-based metrics of the health of the patients in the provider's area. This shift

immediately triggers two trends: first, the need to collect metrics about health of the patient population, even when they don't visit the clinic; second, a motivation to encourage the patients to manage chronic conditions and change behaviors so they remain healthy. Patient engagement will be critical; a recent report [1] "found that engaging consumers more fully in their own health and healthcare not only improves the experience of care for patients and their families, but also improves the quality and cost effectiveness of care" [2]. Ultimately, the Institute of Medicine hopes these shifts will lead to a "continuously learning health system, one that aligns science and informatics, patient-clinician partnerships, incentives, and a culture of continuous improvement to produce the best care at lower cost" [11].

Trend 3: Continuous patient monitoring outside the clinical setting.

Close monitoring of an individual's physiology, activity, and behavior seeks to enhance diagnosis, monitor treatment, and guide healthy behavior. Interest in continuous monitoring is driven by the shifting locus of care, for example, to monitor a post-surgical patient after he returns home; by the goal of accountable care, as providers gather data about patient wellness and health outcomes; by the goal of increasing patient engagement, to increase individual awareness of their health and to encourage healthy behaviors; and by the emergence of mobile devices that measure or collect such information. However, this pervasive monitoring of one's personal life, outside the clinical setting, emphasizes the need for secure systems and privacy-sensitive design.

One common use for continuous monitoring is the management of chronic conditions, into which clinical visits provide only a narrow window of observation. Consider an asthmatic child, who may be in the clinic only a few hours a year, but whose condition requires close monitoring on a daily basis. By better monitoring the child's condition outside the clinical setting – gathering more information about her symptoms, the progress of her treatment, the conditions of her environment, or her lifestyle – we can help the child and her caregivers to make better decisions. Clinical visits can be avoided when not needed, or encouraged when health indicators warrant – allowing interventions before the condition becomes an emergency-room visit. Mobile & cloud technologies are finally making this kind of monitoring possible.

A considerable fraction of US healthcare dollars addresses the effects of unhealthy "lifestyle" behaviors, such as poor diet, lack of exercise, smoking, drugs, or abuse of alcohol, which lead to obesity, heart disease, diabetes, and lung disease. Numerous mobile technologies aim to improve health and wellness by monitoring health-related behavior and providing immediate and continuous feedback. Such behavioral-health applications will become increasingly common as employers launch wellness initiatives and accountable care organizations seek to reduce cost through better prevention programs.

Trend 4: Advent of mobile devices and cloud services in health-related applications.

Smartphones and wearable devices to measure physiology, physical activity, and behavior herald the coming "mHealth" revolution. These technologies provide pervasive (often continuous) monitoring of an individual's physical and behavioral health, with remote telemetry provided to physicians, therapists, health coaches, family caregivers, and social support networks.

Furthermore, clinical staff and patients alike will be using smartphones and tablets as a primary means for collecting and viewing health information, communicating with each other, and configuring medical devices. Provider organizations will need to manage a fleet of such devices, but not all devices will be under their control: some will be personal devices used by their

staff, and others will be personal devices used by their patients and patient families. Indeed, provider organizations may not even be aware of all the personal devices communicating with their systems, and manipulating personal health information, let alone have administrative control over those systems. Furthermore, many of these devices will interact with cloud-based services operated by a variety of organizations. In one recent survey of healthcare organizations, however, more than 90% of respondents said their organizations were moving data into the cloud, yet nearly half said they lacked confidence in protecting that data [12].

Trend 5: Emerging threats and changing regulatory environment.

Information technology is being deployed broadly in the healthcare industry, encouraged by the above trends as well as the 2009 Health Information Technology for Economic and Clinical Health Act (the HITECH Act) [6], which provides strong incentives for health providers to shift to electronic health records. These deployments are expanding privacy, safety, and financial risks to both patients and providers, however. Privacy threats arise from unclear expectations and limited (or unusable) mechanisms for sharing data about individuals in an increasingly complex health information environment; examples include providers who intentionally or accidentally share patient information that the patients do not expect, and vendors who use health-related data for purposes like targeted advertising. Safety concerns arise from security breaches that affect the integrity of health records or medical devices; examples range from Internet-launched attacks that impact hospital information systems, whether as deliberate or inadvertent targets, to wireless attacks on safety-critical devices like defibrillators and insulin pumps [3]. Financial risks arise from personal information in health records, which often enable identity theft [7], and from large-scale fraud schemes where access to such information allows scams like spoofed insurance claims.

Particularly worrisome is the expanding incidence of medical identity theft, in which an individual pretends to be someone who has insurance, to steal their benefits; such a threat has an obvious safety risk to both the attacker and the victim. The regulatory environment is changing, but not adapting quickly enough to the shifting risks. In January, HHS released an update [4] to the privacy rules first spelled out after HIPAA [5]; although these rules clarify and strengthen the rules aimed at protecting patient privacy, they fall short of addressing the needs of mobile devices [13].

The popular press recognizes that security and privacy concerns are a dominant factor in the adoption of modern technology in healthcare; if such concerns slow adoption, we cannot reap the potential benefits of these technologies. Privacy and security were cited as the most important concerns in a recent survey of “27 key informants from across the health and mHealth sectors in the United States” [14]. Furthermore, a “year-long examination of cybersecurity by *The Washington Post* has found that healthcare is among the most vulnerable industries in the country, in part because it lags behind in addressing known problems” [8]; our JHU PI, Avi Rubin, was quoted extensively in this article.

Clinicians also have security concerns. While clinicians have rapidly adopted use of their own devices in hospitals, only half of those interviewed in one survey felt their workplace wireless access was secure [12]. Similarly, new remote-monitoring devices are being deployed in healthcare settings with little focus on security. Despite the recent attacks on wireless medical devices [3, for example], 69% of respondents said their organization’s IT security activities did not address security of FDA-approved medical devices [12].

Traditional approaches to securing healthcare systems have relied on isolation, using tools like firewalls and network access control. However, the trends described above make it unfeasible to simply ‘lock down’ medical devices or health-records systems, especially as patients and staff use part of the system outside the clinical context, and many of the wellness applications of this technology are entirely non-clinical. Instead, these trends demand “wide-spectrum” security technologies – that is, technologies that can be adjusted to fit the needs and expertise of the system user. An EHR provider has professional staff who can configure and monitor security settings in a cloud-based EHR service, but an individual patient must have intuitive and hassle-free security technologies for home-based devices. Our research aims to develop security technologies that work across many care settings, continuous collection of data, and increased use of multi-purpose mobile devices.

These five trends are powerful forces driving major changes in the healthcare IT landscape, and raise important research challenges we plan to address. In our posts over the next five years, we’ll describe our research and its results.

References

1. Bipartisan Policy Center. *Improving quality and reducing costs in health care: Engaging consumers using electronic tools*. Online at http://bipartisanpolicy.org/sites/default/files/BPC_Engaging_Consumers_Using_Electronic_Tools.pdf, December 2012. Last accessed January 26, 2013.
2. National eHealth Collaborative. *Liberating data and fostering innovation to engage patients*. Online at <http://www.nationalehealth.org/LiberatingData>, January 2013. Last accessed January 26, 2013.
3. Daniel Halperin, Thomas S. Heydt-Benjamin, Benjamin Ransford, Shane S. Clark, Benessa Defend, Will Morgan, Kevin Fu, Tadayoshi Kohno, and William H. Maisel. *Pacemakers and implantable cardiac defibrillators: Software radio attacks and zero-power defenses*. In *Proceedings of the IEEE Symposium on Security and Privacy (S&P)*, pages 129–142. IEEE Press, May 2008. DOI 10.1109/SP.2008.31.
4. Department of Health and Human Services. *Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules*. Online at <https://www.federalregister.gov/articles/2013/01/25/2013-01073/modifications-to-the-hipaa-privacy-security-enforcement-and-breach-notification-rules-under-the>, January 2013. Last accessed January 26, 2013.
5. Department of Health and Human Services. HIPAA website. Online at <http://www.hhs.gov/ocr/privacy/>, visited March 2010.
6. Coppersmith Gordon Schermer and Brockelman. *HITECH Act expands HIPAA privacy and security rules*. Online at http://www.azhha.org/member_and_media_resources/documents/HITECHAct.pdf, visited November 2009.
7. M. Eric Johnson and Nicholas Willey. *Usability failures and healthcare data hemorrhages*. *IEEE Security & Privacy Magazine*, 9(2):35–42, March 2011. DOI 10.1109/MSP.2010.196.
8. Robert O’Harrow Jr. *Health-care sector vulnerable to hackers, researchers say*. Online at http://articles.washingtonpost.com/2012-12-25/news/36015727_1_health-care-medical-devices-patient-care, December 2012. Last accessed January 26, 2013.
9. Steve Lohr. *Wal-Mart plans to market digital health records system*, March 2009. Last accessed January 26, 2013, Online at <http://www.nytimes.com/2009/03/11/business/11record.html>.

10. Shawn McKee. *5 Advantages of a Cloud-Based EHR for Small Practices*. Online at <http://www.poweryourpractice.com/5-advantages-of-a-cloud-based-ehr-for-small-practices/>, January 2012. Last accessed January 26, 2013.
11. The Institute of Medicine of The National Academies. *Best care at lower cost: The path to continuously learning health care in America*. Online at <http://www.iom.edu/Reports/2012/Best-Care-at-Lower-Cost-The-Path-to-Continuously-Learning-Health-Care-in-America.aspx>, September 2012. Last accessed January 26, 2013.
12. Ponemon Institute. *Third annual benchmark study on patient privacy & data security*. Online at http://www.ponemon.org/local/upload/file/Third_Annual_Study_Patient_Privacy_FINAL5.pdf, December 2012. Last accessed January 26, 2013.
13. Greg Slabodkin. *New HIPAA rule falls short in protecting mobile patient information*. Online at <http://www.fiercemobilehealthcare.com/story/new-hipaa-rule-needed-expand-its-reach-protecting-mobile-patient-information/2013-01-20>, January 2013. Last accessed January 26, 2013.
14. Robyn Whittaker. *Issues in mHealth: Findings From Key Informant Interviews*. Journal of Medical Internet Research, 14(5), 2012. DOI 10.2196/jmir.1989.

This entry was posted in **Trends** and tagged **healthcare**, **healthcare-IT**, **trends** by **David Kotz**. Bookmark the **permalink** [<https://thaw.org/2013/07/17/five-hit-trends-implications-for-security/>].



About David Kotz

David Kotz is the Provost, the Pat and John Rosenwald Professor in the Department of Computer Science, and the Director of Emerging Technologies and Data Analytics in the Center for Technology and Behavioral Health, all at Dartmouth College. He previously served as Associate Dean of the Faculty for the Sciences and as the Executive Director of the Institute for Security Technology Studies. His research interests include security and privacy in smart homes, pervasive computing for healthcare, and wireless networks. He has published over 240 refereed papers, obtained \$89m in grant funding, and mentored nearly 100 research students. He is an ACM Fellow, an IEEE Fellow, a 2008 Fulbright Fellow to India, a 2019 Visiting Professor at ETH Zürich, and an elected member of Phi Beta Kappa. He received his AB in Computer Science and Physics from Dartmouth in 1986, and his PhD in Computer Science from Duke University in 1991.

[View all posts by David Kotz](#) →

1 THOUGHT ON “FIVE TRENDS IN HEALTHCARE IT – AND THEIR IMPLICATIONS FOR SECURITY”



Chris Cavender

on **August 19, 2013 at 2:32 pm** said:

I look forward to hearing more about your research, and hope that you will also be examining the risks of automated malware that can jump from mobile platform to medical devices and back using the bluetooth capabilities and lack of A/V

