

V viewpoints

DOI:10.1145/2790830

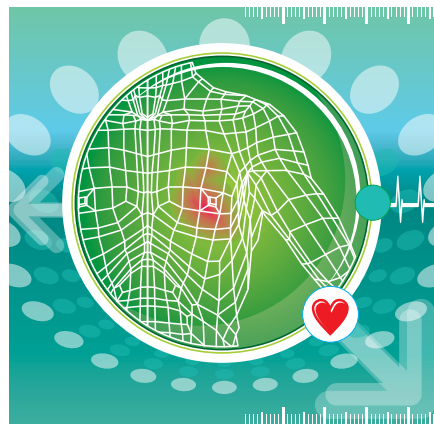
David Kotz, Kevin Fu, Carl Gunter, and Avi Rubin

Privacy and Security Security for Mobile and Cloud Frontiers in Healthcare

Designers and developers of healthcare information technologies must address preexisting security vulnerabilities and undiagnosed future threats.

I FEAR THE day when your security requirement kills one of my patients,” said a medical practitioner to the security professionals proposing improved security for the clinical information system. Every security professional is familiar with the challenge of deploying strong security practices around enterprise information systems, and the skepticism of well-intentioned yet uncooperative stakeholders. At the same time, security solutions can be cumbersome and may actually affect patient outcomes.

Information technology (IT) has great potential to improve healthcare, promising increased access, increased quality, and reduced expenses. In pursuing these opportunities, many healthcare organizations are increasing their use of mobile devices, cloud services, and Electronic Health Records (EHRs). Insurance plans and accountable-care organizations encourage regular or even continu-



ous patient monitoring. Yet *The Washington Post* found healthcare IT to be vulnerable and healthcare organizations lagging behind in addressing known problems.⁹ Recent breaches at two major health insurance companies¹⁷ underscore this point: the healthcare industry moves toward automation and online records, yet falls behind when addressing security and privacy, ranking below retail in terms of cybersecurity.³

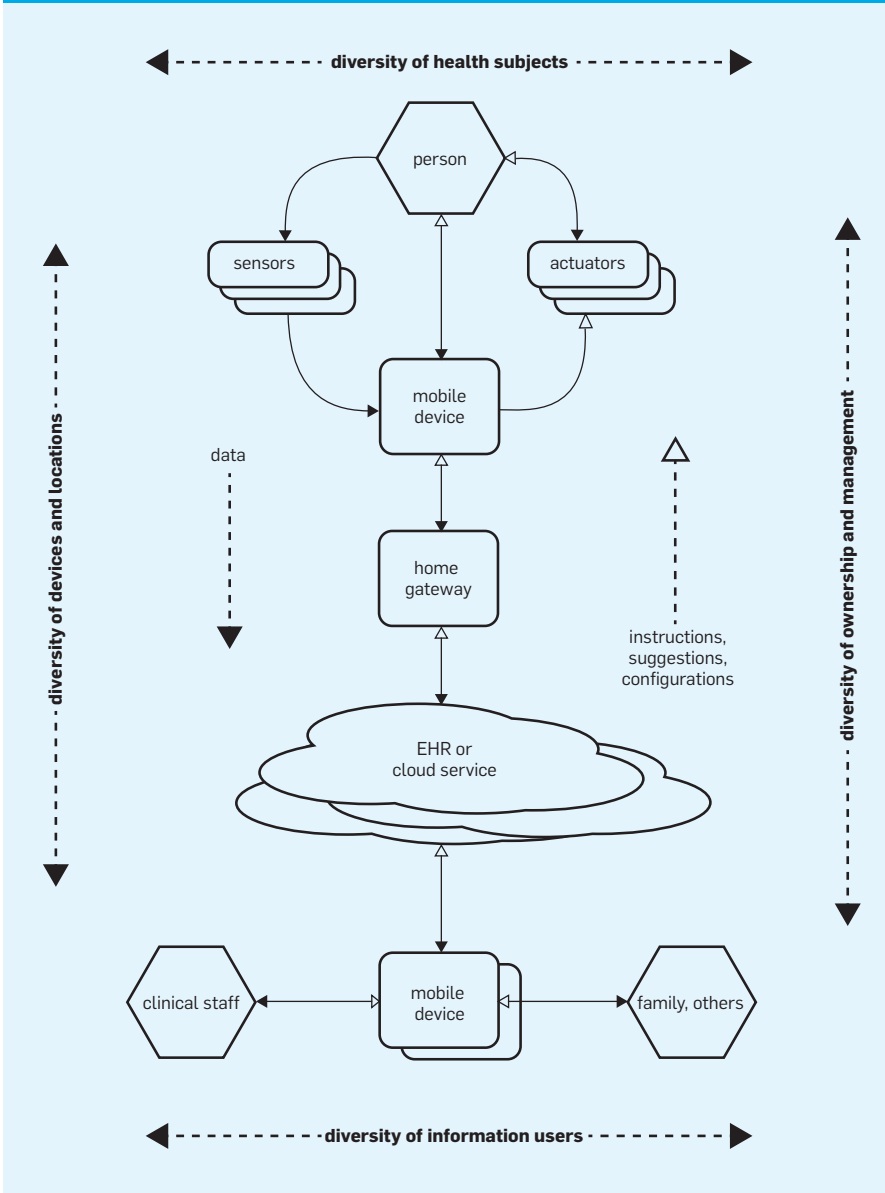
The benefits of healthcare IT will be elusive if its security challenges are not adequately addressed. Security remains one of the most important concerns in a recent survey of the health and mHealth sectors,¹² and research has illustrated the risks incurred by cyberattacks on medical devices such as pacemakers.⁵ More than two-thirds (69%) of respondents say their organization’s IT security does not meet expectations for FDA-approved medical devices.⁶

Privacy protection is also critical for healthcare IT; although this column focuses on security, it should be noted that many security breaches lead to disclosure of personal information and thus an impact on patient privacy.

Critical Research Challenges

The accompanying figure shows the complex trust relationships involved. Those who use medical information are diverse: families, clinicians, researchers, insurers, and employers are some

The complex trust relationships involved in healthcare information technologies.



examples. Those who provide information are also diverse: traditional patients, healthy athletes, children, the elderly, and so forth. The mobile devices and cloud systems are also diverse and are often managed by multiple organizations. The result is a complex mix of trust relationships with implications both for technology and the social, economic, and regulatory environment in which the technology operates.

Designers and developers of healthcare information technologies can help by designing security into all devices, apps, and systems, and by developing policies and practices that recognize the rights of individuals regarding information collected on them: where it will be stored, how it will be used,

and whom will have access. Researchers should develop new methods for authentication, identification, data anonymization, software assurance, device and system management—and human factors should play a critical role in all of these methods. Some of the most-critical research challenges are described here.

Usable authentication tools. Health IT presents many demanding problems for users in authenticating themselves to systems. Traditional authentication mechanisms like passwords can disrupt workflow and interfere with the primary mission of patient care. New authentication mechanisms must blend into the clinical workspace, recognize that staff often wear gloves and

masks (obviating solutions based on face and fingerprint recognition), and work with smartphones, tablets, desktops, and laptops.

EHR systems should not arbitrarily limit clinical staff from viewing an entire record—denying access in an emergency situation may lead to delayed care or even death. However, “break-the-glass” provisions of many EHRs to provide emergency access to patient records make more information available than necessary for care. Break-the-glass mechanisms should expose patient records in stages to provide needed information without providing too much information, and trigger automated and organizational audit mechanisms.

Patients are increasingly asked to use (or wear) mHealth technology outside the clinical setting, but might not want mHealth data to reveal detailed activities. They might want to suspend reporting for periods of time, or block systems from storing or sharing data that is not directly relevant to treating their condition. Mechanisms should separate data *collection*, *analysis*, and *presentation* to limit data that travels outside the patient’s trust circle. These mechanisms should be easy to understand and use, indicating how data may be collected, stored, and shared. Fine-grained consent descriptions should interoperate across mHealth systems and EHRs, and travel with data that flows from one system to another. The foundation of any privacy-supporting solution is a secure system with strong mechanisms for identifying and authenticating users.

The declining cost of gene sequencing enables a new generation of precision medicine.¹¹ Although this technology has great promise, basic issues have yet to be handled: how patients should access their own genomic information, how they control sharing with health professionals, and how best to provide “direct to consumer” services like support for genealogy explorations.⁸

Trustworthy control of medical devices. Today’s sophisticated medical devices like infusion pumps and vital-sign monitors are increasingly networked (possibly via the Internet) and run safety-critical software. Network-capable medical devices may have cyber-security vulnerabilities that can

have implications for patient safety. Medical devices must contain defenses against today's known vulnerabilities and tomorrow's anticipated threats.²

Medical devices must defend against conventional malware that attacks their outdated operating systems. For example, Conficker and bot-net malware can break into unmaintained systems easily; old operating systems provide large reservoirs for the Conficker worm, and medical devices can have long product life cycles that persist with outdated operating-system software. MRI machines running Windows 95, pacemaker programmers recently upgraded from OS/2 to Windows XP, and pharmaceutical compounders running Windows XP Embedded have been noted.

Medical devices must also withstand threats that match the future product life cycle, but it is difficult to secure a device for 20 years. The 1995 desktop computer could not withstand today's threats of spam, malware, drive-by-downloads, and phishing attacks. It is difficult to design medical devices for evolving threats. According to the Veterans Administration, modern malware can enter via USB drives used by contractors upgrading medical-device software. Better methods are needed to engineer secure software and ensure the correct software is running. Improvements are needed for detecting attempted network attacks (wired or wireless), and for dealing with attacks in progress without compromising patient safety. Solutions aimed at desktop computers and Internet servers might not work for medical devices. For more on this topic, see the recent *Communications* article by Sametinger et al.¹⁰


Trust through accountability. Health IT provides a foundation for diagnosis, treatment, and other medical decision making. This foundation must be both *dependable* and *trustworthy*. Technical security is essential, but trust also critically depends on social, organizational, and legal frameworks behind the technology. Health IT must be *accountable*, which means people and organizations must be held responsible for the ways the systems are used. Systems configured to provide access to many must be backed by responsible organiza-

The benefits of healthcare IT will be elusive if its security challenges are not adequately addressed.

tions that determine who has access and when. "Break-glass" mechanisms must be guided by protocols about who can break the glass, and for what purpose.

Audit logs of all health IT systems are needed to monitor for buggy or inappropriate behavior, and to support post-event analysis as well as the development of proper access controls.⁴ There has been considerable study of audit logs and accountability for hospital patient records, but mobile systems and devices also need rigorous auditing. Automated analysis of audit logs in medical systems would be useful, as would be the ability to detect anomalies (such as staff members looking at rarely examined records or device settings changed by a person not normally given access to the device). Access restrictions should be imposed according to workflow data and/or models trained via machine learning to diminish reliance on post-hoc accountability. There are many research opportunities in this space.

Conclusion

The research community must address many fundamental and practical challenges to enable healthcare IT to achieve the level of security essential for widespread adoption and successful deployment. For doctors and other caregivers to embrace more secure solutions, they need to be usable and fit within their clinical workflow. For patients and family members to accept these technologies, they need to be comfortable with the privacy of their personal information and able to effectively use the security solutions that support those privacy mechanisms. We call on the research community to tackle these challenges with us. 

References

1. Eastwood, B. Premera says data breach may affect 11 million consumers. *FierceMobileHealthcare* (Mar. 18, 2015); <http://www.fiercehealthit.com/story/premera-says-data-breach-may-affect-11-million-consumers/2015-03-18>.
2. Fu, K. Trustworthy medical device software. In *Public Health Effectiveness of the FDA 510(k) Clearance Process: Measuring Postmarket Performance and Other Select Topics*. IOM (Institute of Medicine) Workshop Report, National Academies Press, Washington, D.C., July 2011; <https://spqr.eecs.umich.edu/papers/fu-trustworthy-medical-device-software-IOM11.pdf>.
3. Gagliardi, N. Healthcare cybersecurity worse than retail: BitSight. (May 28, 2014); <http://www.zdnet.com/article/healthcare-cybersecurity-worse-than-retail-bitsight/>.
4. Gunter, C.A., Liebovitz, D.M., and Malin, B. Experience-based access management: A life-cycle framework for identity and access management systems. *IEEE Security & Privacy* 9, 5 (Sept./Oct. 2011); DOI 10.1109/MSP.2011.72.
5. Halperin, D. et al. Pacemakers and implantable cardiac defibrillators: Software radio attacks and zero-power defenses. In *Proceedings of the IEEE Symposium on Security and Privacy (S&P)*. IEEE Press (May 2008), 129–142; DOI: 10.1109/SP.2008.31.
6. Ponemon Institute. Third annual benchmark study on patient privacy and data security (Dec. 2012); http://www.ponemon.org/local/upload/file/Third_Annual_Study_Patient_Privacy_FINAL5.pdf.
7. Millions of Anthem customers targeted in cyberattack. *New York Times* (Feb. 5, 2015); <http://www.nytimes.com/2015/02/05/business/hackers-breached-data-of-millions-insurer-says.html>.
8. Naveed, M. et al. Privacy in the genomic era. *ACM Comput. Surv.* 48, 1, Article 6 (July 2015); DOI: <http://dx.doi.org/10.1145.2767007>.
9. O'Harrow, Jr., R. Health-care sector vulnerable to hackers, researchers say. *Washington Post* (Dec. 2012); http://articles.washingtonpost.com/2012-12-25/news/36015727_1_health-care-medical-devices-patient-care.
10. Sametinger, J., Rozenblit, J., Lysecky, R., and Ott, P. Security challenges for medical devices. *Commun. ACM* 58, 4 (Apr. 2015), 74–82; DOI 10.1145/2667218.
11. White House. FACT SHEET: President Obama's Precision Medicine Initiative (Jan. 30, 2015); <https://www.whitehouse.gov/the-press-office/2015/01/30/fact-sheet-president-obama-s-precision-medicine-initiative>.
12. Whittaker, R. Issues in mHealth: Findings from key informant interviews. *Journal of Medical Internet Research* 14, 5 (May 2012); DOI 10.2196/jmir.1989.

David Kotz (kotz@cs.dartmouth.edu) is a professor of computer science at Dartmouth College, principal investigator of the NSF-funded Trustworthy Health and Wellness (THaW.org) project, and former director of the Institute for Security, Technology, and Society (ISTS).

Kevin Fu (kevinfu@umich.edu) is an associate professor of electrical engineering and computer science at the University of Michigan, a member of the NIST Information Security and Privacy Advisory Board, a member of the ACM Committee of Computers and Public Policy, former ORISE Fellow at the FDA, and director of the Archimedes Center for Medical Device Security.

Carl Gunter (cgunter@illinois.edu) is a professor of computer science, a professor in the College of Medicine, and the director of the Illinois Security Lab and the Health Information Technology Center at the University of Illinois, Urbana.

Avi Rubin (rubin@jhu.edu) is a professor of computer science and technical director of the Information Security Institute at Johns Hopkins University, and principal investigator of one of the first NSF CyberTrust centers (on e-voting).

This research program is supported by a collaborative award from the National Science Foundation (NSF award numbers CNS-1329686, 1329737, 1330142, and 1330491). The views and conclusions contained in this material are those of the authors and should not be interpreted as necessarily representing the official policies, either expressed or implied, of NSF. Any mention of specific companies or products does not imply any endorsement by the authors or by the NSF.

Copyright held by authors.