Security and Privacy in Health IT

Kelly Caine | Clemson University
Michael Lesk | Rutgers University

For hundreds of years, physicians have recognized the importance of maintaining health information privacy and security. Healthcare providers who swear the Hippocratic oath promise to keep what they learn about patients' health "secret." When patients fear that the trust they place in providers to keep this oath might be violated, they sometimes resort to potentially dangerous health behaviors such as refusing to reveal important information, avoiding tests, or avoiding care altogether.[1,2]

As we move toward a healthcare system that embraces IT because of the opportunities it affords for increasing quality of care and decreasing costs, how do we ensure that patients are guaranteed the privacy they require? The benefits of health IT include improvements in the collection, processing, and interpretation of health data; coordination of care; and even increased patient engagement with projects such as the Blue Button initiative that give patients access to their health data. However, all these benefits depend on patients' willingness to share health information, which in turn depends on their perception of health IT privacy and security. How do we ensure that patients maintain the same confidence in the privacy of their health information as health IT continues to expand?

Fortunately, researchers from a variety of disciplines have been working to understand health IT's unique security and privacy issues. They study validation methods to improve the accuracy of records, encryption techniques to conceal information in transit, anonymization to permit distribution of health data without revealing identities, and access control policies to enforce who sees what. They build technologies for interoperability to enable record exchange between healthcare providers, create visualizations to improve interpretation of records, invent mobile technologies to transmit data from personal devices and sensors, use data mining and searching

 Copublished by the IEEE Computer and Reliability Societies

to deduce information from large medical databases, and design user interfaces that can bring urgent information to the foreground for patients and providers alike.

The articles we selected for this special issue touch on many of these topics, including

- privacy-enhanced decision support methods that present doctors with the most relevant details of an emergency medical situation while preserving patient privacy (Mark Chignell and his colleagues' "Nonconfidential Patient Types in Emergency Clinical Decision Support");
- the tension between vendor confidentiality, anonymity in medical records, and the data needed for epidemiology (Michael Lesk's "Electronic Medical Records: Confidentiality, Care, and Epidemiology");
- multidisciplinary, workshop-based approaches to securing information technology in healthcare (Denise Anthony and her colleagues' "Securing Information Technology in Healthcare");
- reputation systems using mobile devices to allow patients safe remote interaction with their medical records (Ginés Dólera Tormo and his colleagues' "Identity Management: In Privacy We Trust. Bridging the Trust Gap in eHealth Environments"); and
- how the design of electronic health record systems affects patient privacy, the physician-patient relationship, and who should control patient information (Deborah C. Peel and Deven McGraw's Point/Counterpoint discussion).

This special issue represents only some of the most exciting areas of research on protecting privacy and strengthening the security of patients' health information in an electronic and interconnected healthcare system. Because this topic is inherently multidisciplinary, drawing from medicine, computer science, law, policy, and human factors, it was impossible to cover all the areas we wished to. We trust readers will find the articles in this issue a valuable introduction to an ever-growing area of research.

We look forward to seeing new research and technologies that both protect health information security and privacy and lead to better health. ■

References

1. L. Bishop, B.J. Holmes, and C.M. Kelley, "National Consumer Health Privacy Survey 2005," Forrester Research, 2005; www.chcf.org/publications/2005/11/national-consumer-health-privacy-survey-2005.
2. I.T. Agaku, "Concern about Security and Privacy, and Perceived Control over Collection and Use of Health Information Are Related to Withholding of Health Information from Healthcare Providers," *J. Am. Medical Informatics Assoc.*, 23 Aug. 2013; www.ncbi.nlm.nih.gov/pubmed/23975624.

Kelly Caine is an assistant professor of human-centered computing at Clemson University. Contact her at caine@clemson.edu.

Michael Lesk is a professor of library and information science at Rutgers University. Contact him at lesk@acm.org.

Selected CS articles and columns are also available for free at http://ComputingNow.computer.org.