Securing Information Technology in Healthcare

Denise Anthony, Andrew T. Campbell, Thomas Candon, Andrew Gettinger, David Kotz, Lisa A. Marsch, Andrés Molina-Markham, Karen Page, and Sean W. Smith | Dartmouth College
Carl A. Gunter | University of Illinois
M. Eric Johnson | Vanderbilt University

Dartmouth College's Institute for Security, Technology, and Society conducted three workshops on securing information technology in healthcare, attended by a diverse range of experts in the field. This article summarizes the three workshops.

Information technology has great potential to improve healthcare quality and efficiency and thus has been a major focus of recent US healthcare reform efforts. However, developing, deploying, and using IT that is both secure and genuinely effective in the complex clinical, organizational, and economic environment of healthcare are significant challenges, particularly in the US with its mix of public and private providers and insurers. The US healthcare system differs from all other industrialized countries in that it spends the most per capita on healthcare[1] but, despite such spending, is mostly behind other countries in healthcare IT use.[2–4] However, over the past few years, the US federal government has been investing heavily in encouraging health providers to adopt electronic health records (EHRs) and other healthcare IT.

The US system must consider patients' and providers' privacy concerns resulting from IT use as well as the ability of current technologies, policies, and laws to adequately protect privacy.[5,6] Communicating with various healthcare stakeholders (patients, clinicians, administrators, policy makers, public health advocates, and so on) about the privacy risks as well as solutions involved with IT will be as important to the successful implementation of IT as the technology itself. Securing an IT infrastructure that supports the complex and distributed healthcare ecosystem, particularly in the face of increased digitization and records sharing, will be essential to both system integrity and consumer confidence. Lessons learned in the US might inform other systems, even those that are far ahead of the US in IT adoption. Furthermore, new mobile health technologies are being developed across the globe, and there is great opportunity for countries like the US to learn from experiences in low-income countries as well as other industrialized systems.[7]

The Securing Information Technology in Healthcare (SITH) workshops, hosted by Dartmouth College's Institute for Security, Technology, and Society (ISTS), were created to provide a forum for experts from a broad range of perspectives—from officers at large healthcare companies, startups, and nonprofits to physicians, researchers, and policy makers—to discuss health information security and privacy. The first SITH workshop was held in May 2010. This workshop and

1540-7993/13/$31.00 © 2013 IEEE Copublished by the IEEE Computer and Reliability Societies November/December 2013

the following SITH2 workshop in May 2012 focused on the security and privacy challenges of healthcare IT in a variety of healthcare settings. SITH3, which took place in May 2013, focused on mobile health (mHealth), considering its security and privacy implications as well as a range of other relevant challenges. We outline the workshop series, with an emphasis on the recent SITH3.

SITH1

In 2010, the US government committed up to US$1.2 billion to support conversion to EHRs. Researchers recognized that advances in mobile medical devices, including embeddable medical sensors that enable long-term continuous medical monitoring of patient medical conditions (for example, blood sugar sensors for diabetics) and behavior (for example, diet and smoking trackers), were increasing the amount and type of information that could be included in EHRs and used to improve patient care. As the first forum to address these issues, the inaugural SITH workshop examined three related challenges for healthcare IT: security and usability of mobile, sensor, and implantable technologies that monitor patient health; EHR security and usability; and privacy and security risks as perceived by various stakeholders.

> **Security failures in a hospital setting often result from usability failures of both systems and embedded security.**

As in so many other domains, increased use of IT in healthcare can be a double-edged sword, both helping and hindering. In his keynote, Elliot Fisher of the Dartmouth Institute for Health Policy and Clinical Practice discussed one aspect of this problem: the paradox that increased healthcare spending doesn't necessarily lead to better outcomes. In one panel, researchers examined the considerable benefits of mobile technology but also considered the risks of accumulating such sensitive data in distributed computing environments. In another panel, researchers and practitioners discussed EHR challenges and lamented problems of authentication and deauthentication while emphasizing the importance of focusing on being in "the trust business." The workshop concluded by considering how stakeholders (especially patients) fail to appreciate the complexity of how information flows in healthcare IT as well as how technologists fail to appreciate security usability and privacy risks.

More information about the SITH1 workshop is available at www.ists.dartmouth.edu/events/sith.

SITH2

SITH2 took guidance from feedback from SITH1 participants and focused on the immense challenges in safeguarding patient information. It considered usability and healthcare data breaches, access control methodologies in clinical systems, mobile health, secure audits, and policy and technical approaches to healthcare IT privacy and security.

More information about the SITH2 workshop is available at www.ists.dartmouth.edu/events/sith2.

Keynote

David Blumenthal, former National Coordinator for Health Information Technology, presented the SITH2 keynote address in which he discussed current challenges to EHR adoption. Citing healthcare IT as a practical solution for capturing and processing patient information, exchanging health information, and improving care decisions, Blumenthal noted several barriers to physician and hospital adoption of EHRs such as inadequate capital for purchase, unclear return on investment, physicians' resistance to EHRs, and inadequate IT staff. He endorsed privacy and security as the foundation for successful EHR implementation and reviewed the federal government's actions to safeguard privacy and create fair information practices.

Panel 1: Usability and Healthcare Data Breaches

Panel chair M. Eric Johnson kicked off the first discussion, noting that security failures in a hospital setting often result from usability failures of both systems and embedded security. Furthermore, difficulties in using electronic systems have resulted in an epidemic of workarounds in the clinic and the office, creating information risks and patient data breaches. The panelists agreed, each sharing stories of workarounds that included passwords taped onto equipment and sharing patient information by insecure means such as Gmail and Dropbox. A common theme throughout the panel was that secure systems do not take into account the realities of working in a healthcare setting. Paul Connelly of the Hospital Corporation of America argued that, to reduce workarounds and increase security, we must build secure systems that help clinicians get their jobs done. Specifically, we need to design for speed, new technologies, and consistency. By studying the current workarounds and workflows, we can develop secure technologies to support clinician workflow in a flexible manner that allows data migration as needs and technologies change.

Panel 2: Access Control Methodologies in Clinical Systems

Why is healthcare information security at such odds with traditional security engineering? Ross Koppel of the University of Pennsylvania noted two problems we must address: security, which prevents people from gaining access to information they should not have, and access, which is critical to the healthcare industry. Other difficulties arise from the fact that healthcare is an exception-driven business. When system engineers design information systems and security policies, they define normal cases, yet there are more ambiguities and unknowns in medicine than any other field. And, although software engineers have enough difficulty implementing functional requirements, there's yet more difficulty in implementing legal requirements, which they are not trained to do.

Would the creation of a set of standards for recording patient data improve security and data access? The panelists reiterated that the ambiguity inherent in healthcare makes requiring data standardization extremely difficult. In addition, the value of patient health data creates a disincentive for EHR software vendors to create ways to share information.

The healthcare industry is immature in regard to IT and, in some places, needs to leap multiple generations to move to all-electronic systems. Complicating this move are data mobility, cloud services, and consumerization trends. Furthermore, the industry must make this technology leap while supporting archaic legacy systems that, for instance, do not support basic encryption, while the owners of these legacy systems lobby policy makers against tighter security regulations. Cost is another major factor in determining patient data security: to reduce cost, organizations often must settle for less secure options.

Panel 3: Mobile Health

Panel chair David Kotz began the session by providing a definition for mobile health: the use of mobile computing and communications technology in the delivery of healthcare or collection of health information. Kotz further set the stage for the discussion by highlighting aspects of mHealth that demonstrate its difference from the rest of the mobile computing industry: the data's sensitive nature, the amount and variance of the data being collected, and the personal and immediate impact that security problems can have on the patient. Panelist Kevin Fu, then of the University of Massachusetts, Amherst, backed these points by noting that although wireless capabilities might make devices more appealing and convenient, they also increase privacy and security risks. He noted that improved security for medical devices will enable medical device innovation.

Panel 4: Secure Audit

Currently, EHR privacy breaches are often discovered through audits of medical records that are examined for evidence only when a complaint is made. This ad hoc approach is not suitable to handle problems such as large-scale identity theft. Carl A. Gunter explained, "The hope is to get around this reactive model and shift to a proactive model to better respond to emerging threats." The risks of both large-scale data theft and small-scale unauthorized breaches—for example, to gain information on celebrities or acquaintances—create a need to tightly control access to these records. This is where experience-based access management design is valuable. EBAM starts with an ideal vision of access control policies—that is, how the system should be locked down. We then modify this ideal to deal with the inevitable real-world constraints. This is a cyclic process—we continually modify and improve the system until we reach equilibrium between the envisioned model and the constraints imposed by reality. The key to monitoring access is identifying an effective way to use audit logs to pull out different patterns and employ these patterns to enforce the rules. A lack of standards, archaic models of reactive logging, insufficient patient involvement in system design, and numerous policy and enforcement issues all contribute to a variety of problems with the current audit-logging approach. Developers are creating access control methods like EBAM, patient notification tools, and machine-learning techniques for abuse detection to counteract these concerns.

Panel 5: Policy and Technical Approaches to Health IT Privacy and Security

Given the difficulties in creating secure healthcare IT systems and maintaining patient privacy, what public policy tools could most effectively guide the industry? Denise Anthony maintained that trade-offs exist between policy and technical approaches in thinking about privacy and security; it is important to realize how these different approaches contradict one another and how they fit together. Anthony's study on current privacy perceptions of healthcare IT showed that patients do not ask as strongly for access to their records as expected. And despite the Health Insurance Portability and Accountability Act (HIPAA) and state-mandated privacy policies, providers are guided more by professional norms and environmental demands than regulations. Mark Suchman of Brown University furthered this idea. His research showed that policy implementation and success depends on the cultural environment of hospitals.

According to Mark Frisse of Vanderbilt University, tools are necessary to combine technical and policy approaches, for instance, applications that can produce

formal software language based on policies from federal and state regulators as well as healthcare providers. On the patient side, Kelly Caine, then of Indiana University, showed that patients appear to want—and software can provide—more control over how and with whom their healthcare data is shared. Deven McGraw of the Center for Democracy & Technology concluded that better informing patients about information flows, promoting trust, and reducing stigma would help facilitate a trade-off between provider needs and patient concerns but would require a delicate balance from the policy standpoint.

> **mHealth technologies' distinct advantage is that they can expand health research and healthcare beyond the lab or hospital into the person's environment.**

SITH2 Summary

By 2012, the promotion of healthcare IT was in full swing in the US, with the federal government providing extensive resources to support IT adoption by hospitals and doctors. As EHRs and innovative mHealth technologies became more widespread, the SITH2 workshop brought together computer scientists, clinicians, social scientists, providers, vendors, and policy experts to discuss both technical and policy approaches to electronic health information security and privacy. Workshop participants concluded that delivering high-quality care supported by the effective use of data while protecting patient privacy and preventing data breaches will require fresh thinking. Flexible regulation to promote privacy-by-design technical standards for usable systems that enable providers to deliver high-quality care to patients is a tall order. No simple industry standard or regulatory policy will address all concerns, so the real challenge is to promote greater collaboration across stakeholders to produce IT systems that enable the common interests of producing the best patient care.

SITH3

Advances in mobile medical devices and the proliferation of applications for handheld devices have given rise to the exciting and ever transforming field of mHealth. mHealth includes any wireless device carried by or on the person that accepts or transmits health information, such as sensors (for example, implantable miniature sensors and "nanosensors") and monitors (for example, wireless accelerometers, blood pressure and glucose monitors, and mobile phones), as well as clinical decision support tools that healthcare providers use.

SITH3 included two exciting keynote speakers and four in-depth panel discussions: Intersection of mHealth and Behavioral Health, Evolving Business Models in mHealth, Opportunities for mHealth in the Developing World, and Challenges in Securing mHealth Infrastructure.

More information about the SITH3 workshop, including videos of most workshop sessions, is available at www.ists.dartmouth.edu/events/sith3.

Evening Keynote

The SITH3 workshop began with a dinner keynote speech by Patricia Mechael, executive director of the mHealth Alliance, which is hosted by the United Nations Foundation. Her talk centered on the increased risk of misuse of digital medical data that has accompanied the rapid growth in mHealth worldwide. As she stated, "Our understanding of how to handle patient data privacy, or the best ways to regulate the collection of medical data, has not kept pace with the changing technology." She believes that protecting personal health information collected and transmitted over mobile devices is essential to bringing mHealth to scale.

To this end, the mHealth Alliance partnered with the Thomson Reuters Foundation, Merck, and the law firm Baker & McKenzie to increase the understanding of how privacy and security policies relate to mobile technology use in healthcare.[8] Complicating the process of regulating data privacy are cultural variations in the meaning of privacy, security, and confidentiality in different parts of the world. Thus, developing global policies or laws addressing mHealth privacy and security issues is unlikely. After researching privacy and security policies around the world, Mechael concluded, "any effort at legislative reform to address mHealth privacy and security concerns must first take stock of the cultural, technological, and legal context at play. Such efforts must acknowledge the effect that these and other factors could have on mHealth privacy and security, and on the success of any new policies."

Morning Keynote

The day of panel presentations began with a keynote speech from Wendy Nilsen, health scientist administrator at the National Institutes of Health's (NIH) Office of Behavioral and Social Sciences Research. Nilsen's focus is on the science of human behavior and behavior change, including the use of mobile technology to improve the understanding, treatment, and prevention of disease. In her talk, she emphasized that cellular network penetration, now at 96 percent in the US and 78 percent of the world, allows mHealth to develop expo-

nentially around the world by leveraging the existing mobile technology infrastructure for data collection, health monitoring, and intervention.

Nilsen described mHealth as a "leapfrog technology," allowing access to populations that could not before have been accessed, such as sub-Saharan Africa. mHealth technologies' distinct advantage is that they can expand health research and healthcare beyond the lab or hospital into the person's environment. mHealth technologies can change the questions we ask and the way we do research and offer new possibilities for remote clinical trials. mHealth is about revolutionizing measurement, which in turn changes diagnostics and treatment and ultimately impacts global health.

Although there is currently a proliferation of mHealth applications on the market, Nilsen stressed that the industry will build whatever sells and will test only as much as it has to. Industry is unlikely to develop mHealth tools for research or use these tools to optimize health in low-resource settings. NIH's goal is to fund rigorous science in mHealth that directly addresses its priorities and targets health across the missions of all of the institutes and centers. She described some of the funded mHealth research, including

- measurement and assessment, such as implantable biosensors and a specially developed lens that fits to a cell phone to create a microscope;
- chronic disease management, such as remote monitoring of cardiac activity and personalized real-time monitoring and feedback to target obesity among urban, minority youth; and
- global mHealth initiatives to improve adherence to chronic disease medication and allow patients to report adverse events to medications.

Despite its huge potential, Nilsen highlighted the challenges that mHealth faces. Of major concern are researchers' costly and time-consuming efforts to work with incompatible devices (for example, Android, iPhone, and feature phones) from multiple carriers, requiring them to develop interfaces for multiple cellular platforms or to buy phones for participants. In addition, researchers are constantly warned about mobile privacy and security concerns, but little guidance is available. Finally, although recruiting and retaining people for research is crucial, remote engagement, including micro-incentives and social rewards, is a huge knowledge gap.

Panel 1: Intersection of mHealth and Behavioral Health

Lisa A. Marsch commenced the first panel session by providing an overview of the joint significance of mHealth and behavioral health. Marsch discussed the vast prevalence and impact of behavioral health disorders, the wide application of mHealth to behavioral health initiatives, and the great promise of mHealth for future behavioral health efforts (particularly in light of evolving healthcare systems focused on the integration of behavioral and physical health).

The first panelist, David Gustafson, Emeritus Research Professor at the University of Wisconsin-Madison, presented on the A-CHESS smartphone application, a mobile recovery support tool for people with substance use disorders. Gustafson presented impressive results from a randomized clinical trial as well as a field test featuring A-CHESS and discussed its current integration with the Therapeutic Education System, a Web-based skills training/lifestyle restructuring program for addiction recovery. He also modeled a newer application of the CHESS framework, E-CHESS, a support tool to assist elderly individuals with a variety of functions including healthcare scheduling, appointment reminders, goal tracking, assessment, and social networking.

Next, Sarah Lord, director of the Dissemination & Implementation Core at the Center for Technology and Behavioral Health (CTBH), demonstrated mHealth's potential along a continuum of care by presenting an array of CTBH mHealth tools. She discussed a smartphone-based self-management tool for schizophrenia, a mobile psychosocial intervention for substance abuse care, Web-based education and skill-building programs to promote sexual health and HIV testing, wearable and mobile sensors to track smoking behavior and cravings, and finally, a new center grant to enhance the integration of healthcare technology for evidence-based supported employment.

Timothy Bickmore, associate professor at Northeastern University, presented his work in the development of mHealth tools featuring relational agents, or health provider "avatars," which can be built into a number of platforms including portable kiosks and mobile devices. Bickmore discussed the potential of relational agents to assist in healthcare delivery by modeling therapeutic alliance and improving health literacy, patient satisfaction, and medication adherence.

The final panelist, Niels Rosenquist, faculty member at Massachusetts General Hospital, discussed the importance of connections between mHealth and mental health and presented his approach involving social media analysis and mobile mood monitoring. He also provided strategies for rallying interest and investment in mHealth, including making an economic argument for its importance by citing specific data highlighting the economic benefits and conducting cost-effectiveness studies.

Audience questions included the following:

- With patients increasingly habituated to privacy warnings, how do we prevent patients from ignoring them?

- What types of devices, for either intervention or assessment, do you anticipate in the near future?
- How do we, as providers, determine if smartphone tools are safe, reliable, and the most effective approach?
- Looking forward five years, where will big breakthroughs occur in mobile development and behavioral health research? Is it in assessment or interventions?
- What role can employers play in mHealth?
- With the wide gap between research and practice, how do we rapidly move knowledge into the field and implement effectively?

Panel 2: Evolving Business Models in mHealth

The second panel focused on mHealth's business aspects and how healthcare is likely to change in the coming years. Johnson began the session by putting mHealth in the larger context of the Internet of Things. He pointed out that there are now more Internet-connected devices than there are human beings on the planet, and that when things are connected, they become smart. This combination creates an enormous opportunity to influence the trillions of dollars spent annually on healthcare.

Although the opportunity is large, several panelists commented that making money in mHealth is very difficult. One reason, cited by Chuck Parker, executive director of Continua Health Alliance, is a lack of standards. Due to limited interoperability, it's difficult for data to seamlessly flow between mHealth devices and EHR systems. Paul Gorup, chief of innovation at Cerner, suggested that start-ups and established companies alike have failed in mHealth, often due to a lack of focus on healthcare. He cited IBM's repeated entry and exit from this market as well as non-core efforts by Google and Microsoft that have failed to gain market traction.

Several panelists pointed out that the current healthcare system is broken. Cameron McKennitt, president and COO of start-up PolyRemedy, noted that the historical focus has been on episodic care, in which the patient is treated after becoming ill. Preventing health trouble from occurring in the first place and getting patients back home quickly if it does occur are key. The panelists thought mHealth, although still in its early development stages, is already starting to drive a shift toward this preventive model. Clearly, we have a long way to go.

Surprisingly, the panelists felt that some non-healthcare organizations might be well-positioned to thrive in a prevention-centered business model. Specifically, they listed telecommunications companies for their role in facilitating data flow and organizations like Walmart for wide-ranging customer reach. Joseph Ternullo, associate director of Partners HealthCare's Center for Connected Health, generated a lively discussion by pointing out that some existing healthcare organizations have large, fixed costs that limit their ability to adapt quickly to changing conditions. Newcomers to healthcare might not have these conditions and might be well positioned for the prevention-centered model.

Participants felt that mHealth was important for the future of healthcare and that the ultimate winners from the changing business environment will be the patients. Parker pointed out that many more people in the US will be covered under new legislation and the system will need to adapt to handle the influx. mHealth offers a possible way to achieve this.

Panel 3: Opportunities for mHealth in the Developing World

Moderator Kotz opened the panel with an overview of mHealth opportunities in the developing world. He noted the many potential benefits of mobile technologies to monitor and provide healthcare, especially in remote villages of the developing world, where healthcare would be otherwise inaccessible to a large fraction of the population. Applications include improving access and lowering costs, disseminating health information, distributed data collection, personal health management, behavior change communication, telemedicine and rural clinics, and remote patient monitoring.

David Aylward, senior advisor, Global Health and Technology at Ashoka, presented a vision to change healthcare to focus on not only caring for the sick but also promoting wellness and vitality (especially nutrition) and encouraging people to monitor and manage diseases at earlier stages. Information and communication technologies (ICTs) are suited to support this change, empowering and guiding less-skilled staff. Mobile sensors can collect and manage data from the field, with minimal human error. Aylward envisions that ICTs can provide the breakthrough healthcare needs with wellness systems that are more distributed and less hospital centric; provide effective interventions and public empowerment through portable devices; and demonstrate effectiveness through evidence-based protocols, remote diagnostics, and improved health and vitality outcomes.

Hamish Fraser, director of informatics and telemedicine at Partners in Health, talked about OpenMRS, a modular and open source electronic medical records platform that uses a concept dictionary for data storage. The open development approach lets groups share code, modules, and the concept dictionary. OpenMRS does not fall under the HIPAA umbrella and can be used for sharing de-identified data to analyze system performance. As one evaluation of OpenMRS, Fraser reported on a new study published by Martin Were, who tested the effectiveness of OpenMRS in a pediatric care study in Kenya. In this study, OpenMRS was con-

figured to give pediatricians printed reminders of tests and other activities to be conducted during that child's visit. The study, which lasted for five months with 1,611 random patients and 30 providers, showed a significant improvement in task completion (68 percent for intervention and 18 percent for control with $p < 0.01$).[9] OpenMRS 2.0 will be released soon, with a better user interface. (For more information, see openmrs.org.)

Ashutosh Sabharwal, professor of electrical and computer engineering at Rice University, noted that the core of healthcare is reliable and accurate data. Medical devices currently rely on well-trained, sincere, and incentivized staff. But because human operators could be inefficient, devices should have the ability to detect and adapt to errors. Sabharwal recently visited a town in India with a population of 2.5 million people that had access to only one spirometer; this inspired him to build capable mobile medical sensors with built-in intelligence. He developed two devices—a spirometer and a retinal imager—which can connect to mobile phones, be operated with minimal or no training, and detect errors during data collection. He highlighted the difficulty of working with medical devices available in the market, most of which have a closed interface, whereas others that are nonproprietary or open are not calibrated; this experience highlighted the need for a business model to encourage open devices.

Lakshmi Subramanian, associate professor of computer science at New York University, pointed out that people are willing to invest money in health, especially when they are sick. He talked about his experience working with Aravind Eye Hospitals, setting up communication networks to provide live conferencing with remote patients. He also talked about three projects that he was involved in, the broad goal of which was to detect, track, and determine the health effects of fake drugs: Paperspeckle is a technology that can uniquely fingerprint pharmaceutical drugs, Epothecary is a system for printing unique bar codes on medications, and an mHealth project at Korlebu Hospital collects patient feedback about drugs to monitor side effects. He recently launched an intelligent disease surveillance system that could predict (at the block level) the outbreak of dengue in a city in the Punjab. He pointed out that the major roadblock he encountered was the lack of a sustainable business model and a clear incentive structure for hospitals and clinical systems in developing regions to adopt mHealth solutions.

During the Q&A session, Subramanian emphasized the need for incentives for both patients and providers in mHealth systems. Aylward encouraged the audience to think about services in the middle—what he referred to as a *virtual enterprise* that could connect the different stakeholders. Fraser pointed out that the industry is moving very fast, so when designing solutions, developers must assume that the technology to make the solution feasible will be available in the future. One audience member wondered why mHealth deployments were not happening in developed countries; Subramanian pointed out that long clinical trials might be a barrier to such deployments. Another audience member wondered what incentive poor people might have to pay for health, when they don't have spare money; Aylward pointed out how Ashoka emphasized the benefits its program had on babies (healthier babies lead to smarter children and a brighter future), so mothers wanted to spend money on health and nutrition programs. Fraser explained how, ultimately, the government should create incentives to promote wellness programs. Another audience member noted that, in the case of healthcare, it might be hard to show incentive because results might not be immediate. Aylward replied that some aspects of wellness have short-term return; for instance, some depression and malnutrition patients show signs of improvement immediately after treatment.

Panel 4: Challenges in Securing mHealth Infrastructure

Andrés Molina-Markham introduced the fourth panel's topic by highlighting mHealth's potential in healthcare and identifying some challenges of securing mHealth devices and infrastructure.

According to Yih-Chun Hu, associate professor in the University of Illinois at Urbana-Champaign's Department of Electrical and Computer Engineering, there are two types of adversaries in mHealth: "honest but curious," that is, someone who provides a service to users and has access to the data generated by the users, and "less honest, but equally curious," that is, someone who attempts to access data in transit or attacks service provider systems to access data at rest. Hu emphasized the need to solve the access-control and authorization problem in healthcare—for example, how do we decide who should have access to which device or what data? His group is working on the problem of securing a body-area network (BAN) by sharing a secret among the devices on the body. Their approach is to use the body as a communication channel.

Jaeyeon Jung from Microsoft Research presented privacy-related challenges that mobile phone users and mobile app developers face. According to Jung, the burden of protecting user privacy is on the user. In a recent project, called Privacy Leaks, her group developed an app that helps users better understand what their mobile apps are sharing—with or without their knowledge. According to Jung, we need to reduce the gap between users' expectations and applications' actual data collection behavior. Her other project, PriScreen, attempts to do that by providing app developers with better privacy analysis tools.

Jacob Sorber, assistant professor in Clemson University's School of Computing, pointed out that the consequences of a security or privacy leak in mHealth can be severe, and often the resources available for mHealth devices are limited. His mHealth research focus is on making safe, privacy-preserving, and efficient computing ecosystems. In his prior project, Plug-n-Trust, he developed a method to compute and communicate securely on an untrusted mobile phone. Currently, he is involved in designing and building a wearable device that manages BAN security, provides the user a trusted means to access mHealth information and control mHealth devices, and acts as a glue for all the devices in a user's BAN.

An audience member asked about data ownership and who gets to decide who can see the data, suggesting that maybe patients should control access to their data, for instance, allowing access only to their doctors. Hu said it isn't clear whether patients should control the data because, in some cases, patients don't have a choice about which doctor will treat them (for example, in emergency units), and in some cases, we don't want patients to read their records (for example, their psychiatrist notes). Another audience member asked what we could do to help users choose better privacy settings. Jung said that the one approach usability researchers take is to avoid having users make decisions for every setting, but instead let them choose good defaults based on other similar users' settings. Hu agreed that we need good default settings because many users are considered functionally illiterate.

One audience member expressed the difficulty of quantifying privacy leaks. Jung said there are two ways to look at it: First, app stores have specific rules regarding privacy while handling user data, and when an app violates those rules, we say it leaked private information. Second, the meaning of privacy from the user's point of view is hard to define because different people have different expectations and different levels of understanding of the system or apps. Hu said we can go to an extreme and define any information theoretic leakage as a privacy leak—for example, expressing an interest in medication reveals something about you. However, this definition is too strict, and typical users don't think like this. Sorber added that users' privacy preferences change over time, so any system we design should be flexible enough to handle changing preferences and evolve accordingly. Hu agreed with an audience member's comment that people are concerned about privacy only when it's violated, and he added that this is why we need privacy laws and regulations. Jung said that typical users don't understand inference attacks, and moreover, we cannot enumerate all possible inference attacks—these attacks will get better with time. So the question for researchers is how to arm users to make better decisions.

In response to a question about how we can enforce the privacy policies on mobile apps, Jung said that her group has explored the possibility of extending their previous work on identifying leaks to achieve this. However, one challenge is that, when programmers are not aware of user privacy settings, apps break or usability suffers. She said a better solution is to add support in mobile platforms that offers users granular control and the flexibility to change access permissions for apps. However, she was skeptical that mobile platforms would do so because it would put a burden on app developers.

SITH3 Summary

The most recent workshop focused on mobile technology and its potential uses in healthcare. Behavioral health is one of the most promising directions for mHealth, whether for interventions encouraging change toward healthier behaviors or for researchers studying human health–related behaviors with unprecedented detail and scope. However, although mHealth technology appears to have great potential to improve health and wellness while reducing costs, the business models remain unclear. An important challenge is to identify a range of models to cover device and deployment costs, consistent with the incentive structures that patients, employers, health providers, and payers face.

The developing world offers an entirely different range of challenges and opportunities; promising early results from numerous pilot studies now face the need to scale and reach financial and logistical sustainability.

Finally, in all settings, many security concerns remain with mobile technologies, particularly those that collect and manipulate highly personal information about physiology and behavioral activity. An important challenge is to provide users with usable control over their privacy.

Because of the positive response from workshop participants regarding the workshop's value—and the resulting potential for future collaboration—ISTS might host another similarly focused workshop in 2014. ■

Acknowledgments

The Institute for Security, Technology, and Society hosted all three SITH conferences. SITH1 received support from the Department of Homeland Security's National Cyber Security Division and the National Science Foundation (NSF). SITH2 received generous support from the Center for Digital Strategies at Dartmouth's Tuck School of Business and funding from the NSF and the Dartmouth Conferences. SITH3 also received generous support from the Center for Digital Strategies and was conducted in cooperation with the Center for

Technology and Behavioral Health in the Geisel School of Medicine. Funding for SITH3 came from the NSF and the Dartmouth Conferences. The Dartmouth Conferences were created by a gift from Fannie and Alan Leslie.

References

1. D.A. Squires, "Explaining High Healthcare Spending in the United States: An International Comparison of Supply, Utilization, Prices, and Quality," *The Commonwealth Fund*, vol. 10, 3 Mar. 2012.
2. G.F. Anderson et al., "Healthcare Spending and Use of Information Technology in OECD Countries," *Health Affairs*, vol. 25, no. 3, 2006, pp. 819–831.
3. R. Rozenblum, "A Qualitative Study of Canada's Experience with the Implementation of Electronic Health Information Technology," *Canadian Medical Assoc. J.*, vol. 183, no. 5, 2011, pp. E281–288.
4. C. Schoen et al., "A Survey of Primary Care Doctors in Ten Countries Shows Progress in Use of Health Information Technology, Less in Other Areas," *Health Affairs*, vol. 31, no. 12, 2012, pp. 2805–2816.
5. D. Blumenthal and M. Tavenner, "The Meaningful Use Regulation for Electronic Health Records," *New England J. Medicine*, vol. 363, no. 6, 2010, pp. 501–504.
6. *Risky Business: Sharing Health Data while Protecting Privacy*, K. El Emam, ed., Trafford Publishing, 2013.
7. S. Avancha, A. Baxi, and D. Kotz, "Privacy in Mobile Technology for Personal Healthcare," *ACM Computing Surveys*, vol. 45, no. 1, 2012; doi:10.1145/2379776.2379779.
8. *Patient Privacy in a Mobile World: A Framework to Address Privacy Law Issues in Mobile Health*, mHealth Alliance, 2013; www.mhealthalliance.org/images/content/trustlaw_connect_report.pdf.
9. M.C. Were et al., "Computer-Generated Reminders and Quality of Pediatric HIV Care in a Resource-Limited Setting," *Pediatrics*, vol. 131, no. 3, 2013, pp. 789–769.

Denise Anthony is an associate professor in Dartmouth College's Department of Sociology, adjunct associate professor in Dartmouth's Department of Community and Family Medicine, and a faculty affiliate at the Dartmouth Institute for Health Policy and Clinical Practice's Center for Health Policy Research. Contact her at denise.l.anthony@dartmouth.edu.

Andrew T. Campbell is a professor of computer science at Dartmouth College, where he leads the smartphone sensing group. Contact him at campbell@cs.dartmouth.edu.

Thomas Candon is the associate director of Dartmouth College's ISTS. Contact him at thomas.k.candon@dartmouth.edu.

Andrew Gettinger is professor of anesthesiology and associate dean for clinical informatics at Dartmouth College's Geisel School of Medicine. Contact him at andrew.gettinger@dartmouth.edu.

David Kotz is the Champion International Professor in Dartmouth College's Department of Computer Science and Associate Dean of the Faculty for the Sciences. Contact him at kotz@cs.dartmouth.edu.

Lisa A. Marsch is director of Dartmouth College's Center for Technology and Behavioral Health and associate professor in the Department of Psychiatry at the Geisel School of Medicine. Contact her at lisa.a.marsch@dartmouth.edu.

Andrés Molina-Markham is a postdoctoral researcher at Dartmouth College's ISTS. Contact him at amolina@cs.dartmouth.edu.

Karen Page is the program administrator for Dartmouth College's ISTS. Contact her at karen.m.page@dartmouth.edu.

Sean W. Smith is a professor of computer science at Dartmouth College and research director of Dartmouth's ISTS, and he works in trustworthy systems in the real world. Contact him at sws@cs.dartmouth.edu.

Carl A. Gunter is a professor of computer science at the University of Illinois, where he serves as director of the Illinois Security Lab. Contact him at cgunter@illinois.edu.

M. Eric Johnson is dean of Vanderbilt University's Owen Graduate School of Management and the Bruce D. Henderson Professor of Strategy. Contact him at eric.johnson@owen.vanderbilt.edu.