Technological Advances in Medicine: It's Personal

Alf Weaver, University of Virginia
Renée Bryce, University of North Texas

Current technological advances and those still being developed are poised to revolutionize medicine—creating tremendous opportunities for real-time, personalized patient monitoring and treatment, but also posing significant risks for medical data security.

What achievements will we see in medicine over the next 5 to 10 years? Rapid technological advances, driven in part by our growing understanding of the human body and how it works, allow our caregivers—and us as patients—to interact with our bodies in ways previously unimaginable. We stand at the brink of truly personalized medicine that replaces a "one size fits all" approach with individualized attention to the specific characteristics that make a patient unique.

No longer is a breast cancer diagnosis the end of the inquiry; rather, it is merely the beginning. Sequencing a patient's genome enables physicians to determine what kind of breast cancer she has and then tailor effective, evidence-based treatment for the desired outcome. At the same time, low-cost health-monitoring devices and personal health records allow that patient to take a more active role in monitoring and managing her own overall well-being.

> **ACCOMPLISHING A GRAND VISION FOR TRULY PERSONALIZED MEDICINE STARTS WITH PATIENT DATA THAT IT IS RELIABLE, ACCESSIBLE, AND SECURE.**

Accomplishing a grand vision for truly personalized medicine starts with patient data originating from many sources. This data must then be stored so that it is reliable, accessible, and sharable—yet, at the same time, secure. Required, then, are system architectures that guarantee these attributes. While such systems will continue to "live" in medical enterprise environments such as hospitals and clinics, personal wearable devices—whether generic along the lines of smartphones, or customized like Fitbit and its competitors—are making significant inroads into medical data reporting, collection, and storage.

Indeed, mobile devices have matured into intelligent data-gathering machines, able to collect and analyze physiological data and then report results to the wearer as well as to any remote observers or monitors—whether human, software, or some combination of both. Properly designed, such smart systems can be used within hospitals or link to remote locations, augmenting the equipment and personnel that make up current medical infrastructures. At the same time, we see an explosion in inexpensive health monitors and fitness trackers primarily for personal use. All of these trends create an incontrovertible need for new security requirements and privacy controls: given the Internet's infinite memory, once medical data has been promulgated publicly, it can never be effectively purged.

IN THIS ISSUE

Focusing on the need for privacy and security, Jinquan Li's "Ensuring Privacy in a Personal Health Record System" draws an important, but often overlooked, distinction between electronic medical records (EMRs), typically generated and held by health professionals, and the personal health records (PHRs) that individuals can store electronically to manage and share their own health information. Based on how they originate, EMRs as well as PHRs "tethered" to a specific healthcare organization in the US are typically covered by the federal Health Insurance Portability and Accountability Act of 1996 (HIPAA), which governs privacy issues related to EMRs (among other matters). However, Web- and device-based PHRs have no such legal protection, so for them to enjoy widespread acceptance patients must be able to trust those companies and systems that collect, store, and disseminate PHR data. As Li suggests, changing the locus of control from providers to consumers will not be a simple matter. The risks and repercussions inherent in PHR data disclosure, whether intentional or accidental, can be serious; aggregated health information is highly valuable to third parties such as drug manufacturers, insurers, marketers, and employers—who may not always have patients' best interests in mind. System architects, take note!

Mobile devices and their increasingly significant role in health management is the topic of "Intelligent Disease Self-Management with Mobile Technology," by Marina Velikova, Peter J.F. Lucas, and Maarten van der Heijden. Just as today our minds can be connected 24/7 to the Internet, soon our bodies will be continuously reporting personal physiological status to software for recording, analysis, and prediction. Fully exploiting a smartphone's inherent instrumentation, such as using its microphone to measure lung function or its camera to determine blood-oxygen saturation, will open new opportunities for disease self-management. The coming rush of customized, snap-in options will accelerate technological progress—but also exacerbate its perils. New hardware and new Web and mobile apps intended to enable effective, personalized medicine will inevitably create new problems as well.

One such potential problem involves quality of service (QoS). Consider this range of cases:

- a hospital patient on a post-op floor whose heart rate is being monitored;
- a patient in intensive care where multiple physiological quantities are monitored and analyzed;
- home-located patients or remote clinics that send and receive data consistently but on an unscheduled basis;
- doctors and other clinical personnel who oversee all these activities using mobile devices; and
- hospital monitoring stations that must carefully watch overall system performance.

Across such varied instances, can mobile devices adequately collect and display data in real time and maintain QoS? In "Medical-Grade Quality of Service for Real-Time Mobile Healthcare," Kyungtae Kang, Qixin Wang, Junbeom Hur, Kyung-Joon Park, and Lui Sha investigate the parameter space in which systems can supply "a level of [data] transmission speed, reliability, privacy, and security that provides real-time, confidential, and accurate service" for both in-hospital and remote applications.

Given the tremendous amount of medical data that can be generated, where should it all be kept? How should it be shared? Can it be adequately secured? If we solve those problems, what might actually be accomplished with the data? "Healthcare Data Integration and Informatics in the Cloud," by Arshdeep Bahga and Vijay K. Madisetti, proposes a new framework based on their prototype Cloud Health Information Systems Technology Architecture (CHISTAR) middleware to coordinate cloud-based data analytics for collecting, organizing, and securely exchanging healthcare data from a range of stakeholders in a range of formats. Software in the form of a Web and mobile app builder lets users implement multiple functions including epidemiological surveillance, adverse drug event prediction, and medical prognosis.

Even as mobile devices are poised to revolutionize personalized medicine, widespread and affordable whole genome sequencing (WGS) could one day go even further—presenting a novel set of benefits and challenges. In "Whole Genome Sequencing: Revolutionary Medicine or Privacy Nightmare?," Erman Ayday, Emiliano de Cristofaro, Jean-Pierre Hubaux, and Gene Tsudik explain that WGS will usher in a new era of "predictive, preventative, participatory, and personalized (P4) medicine." But like most technology, WGS presents a double-edged sword: on one hand, it can pinpoint and predict disease, allowing early-stage, life-saving treatments; on the other, a genome sequence's detailed biometric specificity offers opportunities to irrevocably compromise privacy.

Personalized medicine, already a reality, will inevitably grow in reach and impact as its diagnostic and predictive power expands. As technologists, our duty is to advance medical hardware and software in any way we can, while simultaneously enforcing data privacy—all with a spirit of passion and innovation.

ABOUT THE EDITORS

ALF WEAVER is a professor of computer science and founding director of the Applied Research Institute at the University of Virginia. His research interests include computer networks, network protocols, telemedicine, electronic commerce, medical data privacy and security, and crowdsourcing. Weaver received a PhD from the University of Illinois. He is an IEEE Fellow and served as an ACM National Lecturer. Contact him at acw@cms.mail.virginia.edu.

RENÉE BRYCE is an associate professor of computer science and engineering and director of the Software Testing Lab at the University of North Texas. Her research interests include software testing, specifically combinatorial testing in relation to Web and mobile applications. Bryce received a PhD from Arizona State University. Contact her at reneebryce@gmail.com.