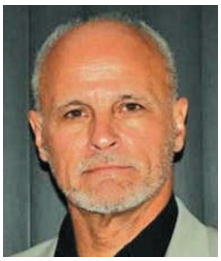
VIEWPOINT



JOE CARVALKO

Who Should Own In-the-Body Medical Data in the Age of eHealth?

Within the next decade, reactive medical practices will evolve into what has been popularly coined "P4" medicine – predictive, preventive, personalized, and participatory – where examinations will take place at home, where devices connected to the body, externally and internally, will send medical data into the cloud, where expert systems will analyze and determine wellness and disease, as well as tweak, in real time, personalized electronic prescriptions for medical treatment and anatomical enhancement. Patients should own this data, and here is why.

Expert systems will have the facility to acquire physiological data from sensors (e.g., temperature, electrical activity, oxygen levels), which will be supplied to processors to draw inferences about medical conditions using decision trees, neural networks, and statistical inference engines, to provide for diagnoses and prognoses. This information will be sent to a physician, and depending on the diagnosis, it may be used to alert health officials, such as the National Center for Disease Control, of impending pandemics, or the potential transmission of "private" diseases, such as AIDS, at the level of the individual.

JOE CARVALKO

These systems will have the capability to track our instantaneous physiological condition, update parameters if necessary, and identify location. Clearly, if the channels between the expert system and our devices are left wide open to government, commercial, and nefarious interests – as some might conclude is the case with our connection to the Internet – we might find our cherished autonomy in jeopardy. Prospective "electronic medicine" will raise privacy and security issues that will make present day concerns for medical records privacy seem benign by comparison.

What price will we pay in individual liberty and privacy for this level of social utility? And, importantly who should own the data? This question leads to the question of who should have access and control over the data: government, private enterprise, or the individual?

Before we answer these questions, let us distinguish between medical data and medical information. Medical data consists of electronic data representations directly related to a patient (e.g., heartbeats) as

Digital Object Identifier 10.1109/MTS.2014.2320136
Date of publication: 4 June 2014

acquired through a sensing device (e.g., pacemaker). The data is useful when it exists in a permissible medical context, such as in a feedback loop to control and maintain stasis (e.g., glucose levels), or to diagnose when a medical event occurs (e.g., fibrillation). Medical data at the patient level also includes transmission protocols, such as device addresses, packet control data, hash codes, and encryption keys. Medical data will be accumulated in knowledge bases and used by inference engines to form the basis of medical information, which is typically embodied in a patient record. The data and information may be parsed, so it exists in various places, usually as paper-based or electronic charts, so that doctors can have access. Charts authored by doctors are considered medico-legal records, and in the U.S., through convention and law, are typically "owned" by the doctor. The difference between medical data and medical information is more than semantic. Although valid arguments might be made as to the right of a patient to own his or her medical record, our attention is drawn to medical data, because it further differentiates itself on the basis of 1) the potential for non-medical uses, 2) the seriousness of harm that may occur in its misuse, and 3) the lack of present day protection for its privacy and security.

> "Electronic medicine" will raise privacy and security issues that will make present day concerns for medical records privacy seem benign by comparison.

Two primary concepts in medical ethics relate to autonomy and non-maleficence. Autonomy deals with the natural rights of individuals to self-determination and by extension the ability to make informed decisions. The concept of non-maleficence is rooted in the dictum, "first, do no harm." These principles serve in part as the predicate for the jurisprudential right to privacy and to one's liberty interest (i.e., to be free from harm, to be let alone.) Personal ownership, which is complete interest and title to medical data and *the power to enforce those rights*, better assures that the data will be used for its intended purpose.

Common experience has shown that sharing personal data over networks, for instance when we search a website, apply for credit, or make purchases, often leads to commercial and government intrusion. Government listens in, ostensibly for security reasons, and businesses find ways to commoditize our information for advertising and product solicitation. In other cases, personal identity information is hacked for amassing non-publically available information, creating fake IDs, passports, and fraudulently accessing bank accounts.

The Medical Device Security Center, a partnership among several highly respected institutions, has as its mission the balancing of security, privacy, safety, and effectiveness for next-generation medical healthcare devices. In one study they easily purchased a used transmit/receiver online, and gained access to a heart defibrillator/pacemaker, following which they accessed medical telemetry data: patient name, diagnosis, and successfully reprogramed, shut down, depleted its battery, and delivered potentially fatal jolts of electricity. In 2011 a researcher told a Black Hat 2011 audience that vulnerabilities with implanted insulin pumps worn by diabetics allowed hackers to remotely control dosage rates. As in-the-body devices proliferate matters can only worsen. Unlike hacking financial or medical records, where the losses are ultimately economic or privacy, these crimes constitute an assault, not merely affecting a specific victim, but an entire class within a population.

Little doubt exists that the future practice of medicine for cure, palliation and human enhancement will be moved by computers integrally connected to the body. The only way to protect our well-being is absolute, patient owned medical data.

Author Information

Joe Carvalko is Adjunct Professor of Law at Quinnipiac University, School of Law, Hamden, CT. Email: carvalko@sbcglobal.net.

Previous Page | Contents | Zoom in | Zoom out | Front Cover | Search Issue | Next Page