Electronic Medical Data – Powerful New Communication Tools Create Privacy Challenges

By Carol A. Umhoefer and Winston J. Maxwell

Telecom companies use the slogan "anytime, anywhere" to describe ubiquitous access to entertainment, e-mail accounts and corporate networks using broadband connections.

In the field of healthcare, "anytime, anywhere" takes on a new meaning, allowing doctors and other healthcare professionals to consult images of a patient who might be located thousands of miles away; to consult, with a simple mouse click, a patient's comprehensive health records, including tests results and images collected in several hospitals located in different cities at different times; to monitor, in real time, patients' vital signs, whether the patient is at work, at home, or in transit.

The advantages of eHealth applications are two-fold: they save money for the national health system, and they save lives. The cost savings come from the ability to avoid unnecessary and duplicative tests, and to permit more health management at home instead of in costly hospital rooms. The life-saving aspects include avoiding medical errors, improving preventive medicine, and getting help to patients quickly.

> "Many eHealth initiatives raise privacy concerns that are serious—but so are the life-saving benefits associated with eHealth."

France and the U.S. are investing heavily in new eHealth initiatives as part of economic-recovery programs. Many eHealth initiatives raise privacy concerns that are serious—but so are the life-saving benefits associated with eHealth. As usual, a careful balance has to be struck between privacy and other important social values before such initiatives can be deployed on a broad scale. Policymakers on both sides of the Atlantic are advancing with caution, knowing that the privacy and security risks will have to be managed so that these new applications can be deployed quickly.

The U.S. is perceived as having weak privacy protection compared to Europe. This is not true for health data. The U.S. has had health-specific privacy rules in place for over a decade, and those rules were recently strengthened by the American Recovery and Reinvestment Act (ARRA) of 2009. France's law on privacy contains special provisions on health data, which are considered "sensitive" and require special protections.

An enlightening case study

Nonetheless, new technologies associated with eHealth applications will raise new privacy challenges for both U.S. and French authorities. These challenges were highlighted in a recent report by the European Network and Information Security Agency (ENISA), which focused on a case study called "Being diabetic in 2011." The case involves a hypothetical patient called Ralph who wears biosensors that transmit information on his glucose level, heart rate and blood pressure to his watch, which in turn transmits the information to a centralized care center. Ralph receives a daily message on his mobile phone reminding him to take his medicine, and must respond to the message—otherwise he is called by someone from the care center. If Ralph needs help, the sensors will trigger an alarm and geolocalization will permit emergency services to reach him quickly. Every evening, Ralph makes entries into his online health journal regarding his diet and exercise that day, as part of a global disease-management program prescribed by his doctor. After validation by a doctor, parts of Ralph's health journal are included in Ralph's electronic health records, which contain all of Ralph's test results and physician notes. Those records are centralized in a secure database. Ralph has access to certain parts of his electronic health records and to the various consents that he has given in connection with using those records.

ENISA used this case study to highlight the enormous benefits associated with Ralph's program, but also the risks of deploying such a program on a broad scale.

How to deal with informed consent?

Most eHealth applications require the informed consent of the patient. Informed consent sounds easy, but it is one of the most thorny issues in data protection. In the hypothetical, Ralph is

able to understand the consequences of his choices, and is sufficiently computer literate to access his online records and review his consent parameters from time to time to make sure they are still valid. New Web 2.0 tools make it easier to put the user in control of his or her privacy profiles, and to manage those profiles over time. But in eHealth, this kind of user-centric approach has its limits because many patients are not in a position to make decisions, let alone access parameters online. Existing practices and regulations in the health field with respect to informed consent may be too elaborate to enable widespread uptake of eHealth applications.

Unauthorized access to Ralph's data?

Electronic health records will contain sensitive information on Ralph, and potentially millions of others. The information will be centralized and accessible to healthcare professionals and national health-insurance schemes for purposes of administering treatment and reimbursing costs. Systems will be designed[1] to mitigate risks of unauthorized access, including identity-management systems that will authenticate individuals and tailor the amount of data that can be viewed by a given professional to only the minimum necessary for that person's function. Nevertheless, as pointed out by ENISA, the data are all in one place, and no system is completely fool-proof. Consequently, there are risks associated with malicious hackers, or even insiders seeking medical information about a famous politician or sports figure. User authentication will be key, but again, this is easier said than done. Sophisticated identity-management systems are emerging to deal with this risk, but the famous New Yorker cartoon stating that "On the Internet nobody knows you're a dog" still raises tricky security problems for network professionals. And beyond electronic-security issues, there is simple human error—as some of Europe's more notorious examples of data loss indicate, massive loss of data may result from nothing more than a notebook computer's being left on a car seat.

Unauthorized use of data?

ENISA also underlines the risk of "mission creep," i.e., that government bureaucrats would find new uses for the data, which may be laudable (in the case of medical research) but nevertheless exceed the scope of the original patient consent. ENISA also points to law-enforcement access to medical data. In Sweden, police obtained access to electronic medical records to help locate a murderer, even though such access was not originally part of the patient's consent. Finally, ENISA mentions the risk that medical data will be used for other kinds of surveillance and profiling, including by insurance companies.

What's "anonymous data"?

Having access to massive patient data can help medical research. One EC-funded project is called @neurIST—Integrated Biomedical Informatics for the Management of Cerebral Aneurysms. This project is based on analyzing large quantities of scanner images of individuals having suffered an accident, and using those data to better predict when an aneurysm presents a health risk requiring intervention: "By uniting currently fragmented clinical data and integrating concepts of the Virtual Physiological Human, @neurIST will have a major impact on the management of cerebral aneurysms." Yet this project faces significant privacy challenges, because it involves the sharing of electronic health records across European countries. One of the key issues for this project and others is what it means to "de-identify" data. Even this relatively simple question has no clear answer. What is anonymous data in one context may be personal data in another, if it is possible to connect data from diverse sources to identify an individual.

System crash

In the case study involving patient Ralph, ENISA points to any number of links in the chain that could fail, in spite of redundancy: the sensors on Ralph's body, the wireless-access network, the telecoms backbone, the call center's patient-management system, the central electronic health-records database itself. Doing away with paper records carries benefits but renders everyone more vulnerable to technical failure, which may be caused by congestion, natural disaster, sabotage, or the proverbial "grain of sand."

After telling the horror story of everything that could go wrong, ENISA lists the benefits of Ralph's eHealth program, which involve rights and interests that are every bit as important as privacy, including better protection of Ralph's life, more efficient use of taxpayer euros, and the ability of Ralph to lead a relatively normal life in spite of his disease.

The path forward will involve IT and telecom companies' implementing security features early in the design stage, at deeper and deeper levels in the network; systematic training of public and private actors, and greater public awareness of privacy rights and obligations. Only by approaching privacy as a continuum involving all actors in the chain (such as with the multi-stakeholder approach in the DMP (*Dossier Médical Personnel*) project recently relaunched by French Health Minister Roselyne Bachelot) will the balance between privacy and eHealth be found.

Carol A. Umhoefer, a Partner at DLA Piper, is Chair of AmCham's Legal Affairs Task Force. (AmCham France Member since 1961) www.dlapiper.com

Winston J. Maxwell, a Partner at Hogan & Hartson, is Co-Chair of AmCham's New Media & IT Task Force. (AmCham France Member since 2004) www.hhlaw.com

1. Using an approach called "privacy by design"