Ethical and Social Issues in Information Systems

During a typical trip to the doctor, you will see shelves full of folders and papers devoted to the storage of medical records. Every time you visit, your records are created or modified, and often duplicate copies are generated throughout the course of a visit to the doctor or a hospital. Take a look at your doctor’s office and chances are you’ll see a bevy of clerks bent over desks filled with

paper forms, mostly insurance claim documents. The majority of medical records are currently paper-based, making effective communication and access to the records difficult: only 8 percent of the nation’s 5,000 hospitals and 17 percent of the nation’s 800,000 doctors use computerized health care records of any kind. Americans made well over a billion visits to doctors and hospitals over the past year, with each American making approximately four visits on average. As a result, there

are millions of paper medical records lining the corridors of thousands of local medical practices, and for the most part, they cannot be systematically examined, and they are difficult to share.

Now for some good news: the administrative waste could be largely eliminated by a massive investment in a nationwide health care record system based on standardized record formats, and the participation of all elements in the health care provider industry. The United States spends about $2 trillion on healthcare, and about $700 billion or one-third is “waste,” loosely defined as costs that could be shed if the healthcare industry followed best practices. This waste is a major reason why the United States has the highest-cost medical system per capita in the world. Among the many

sources of waste are fraud, duplicate tests, unnecessary care, medical mistakes, administrative inefficiency, redundant paperwork, and a paper-based health records system. The outdated administrative procedures and records situation causes an estimated 25 percent of the total “waste,” or about $175 billion a year. There’s more good news about medical records: the new Obama administration in February 2009 set aside $19 billion to fund a Health Information Technology

program as a part of the American Recovery and Reinvestment Act of 2009. The goal: computerize all health records by 2014. And the major technology companies are banding together and offering up solutions, responding to the opportunity of billions of dollars of government contracts. IBM, Google, Microsoft, and a consortium of medical device makers and other companies have formed an alliance to create a software platform that will allow medical data from at-home devices like glucose meters and blood pressure monitors to be sent automatically to Google Health (Google’s online medical record system) or other personal health records systems online. It’s a broad reaching

software platform that will bring data portability and medical records interoperability in direct

conflict with a huge industry entrenched in siloed data. Estimates are that the Health Information Technology initiative will create over 200,000 jobs in MIS and systems, and the 10-year cost is $75–$100 billion. The project should pay for itself with an estimated savings of $175–$200 billion a year. The Health Information Technology initiative is arguably the largest management information systems project in the history of the United States since the computerization of the Social

Security System records in the 1950s. What’s involved is not just dropping PCs on doctors’ desktops and operating tables. Instead, a massive investment in organization and management, cultural change, software, and interface design is required. In short, the skills you learn in this book will be highly valued! The bad news is that the health of your personal privacy will probably decline, significantly. You will most likely lose control over what private medical information about you is distributed, and you will not be able to restrict its distribution. Your medical records will be a very efficient, instantly accessible, “semi public” document accessible by millions of health care

workers whom you will never meet or know about. And you won’t ever really know who has access to your records, or understand how they are or might be used. The health-care industry is notoriously bad at keeping medical records private. Georgia Blue-Cross introduced a change in its medical information system without testing, and sent thousands of patient records to the wrong fax machine in a neighboring state. A former billing clerk at Cedars-Sinai Medical Center in Los Angeles was arrested in November 2008 and charged with stealing patient records and using the identities to steal from insurers. In 2009, the Kaiser Permanente Bellflower Medical Center in Los Angeles was hit with a $187,500 fine for failing to prevent unauthorized access to confidential patient nformation—

employees were improperly accessing the medical records of Nadya Suleman and her eight children. This is the second penalty against the hospital. Even Britney Spears has not been spared: UCLA Medical Center was embarrassed to disclose that employees had sifted through the medical files of more than 30 celebrities, including singer Britney Spears, actress Farah Fawcett, and California First Lady Maria Shriver. There are occasional horror stories like those of Patricia Galvin that reinforce the worries many people have about the privacy of their medical records. Galvin attempted to acquire disability benefits for her chronic back pain but was turned down on the basis of

her psychologist’s notes, which were supposed to be confidential. The number of monthly medical privacy complaints received by the Department of Health and Human Services has been steadily approaching 750 per month over the past several years, up from 150 in 2003. People fear that a switch to electronic medical records could be even more vulnerable to security breaches and privacy violations. Privacy advocacy group Privacyrights.org documented 248 serious personal data record breaches in 2009, and about 24 percent of those involved medical service providers—doctors, hospitals, and insurance companies. In October 2009, the New York Times published a table

illustrating 32 different groups who have “legitimate” access to your medical records, a staggering array of doctors, business associates, government agencies, and data miners (including pharmaceutical companies and their sales staffs). It is conceivable that over a million

people have direct access to medical records throughout the United States. These privacy concerns are far from unfounded. HIPAA—the Health Insurance Portability and Accountability Act of 1996—provides very limited protections for personal medical records. HIPAA basically legitimizes rather than constrains the near unlimited flow of information between healthcare providers, health insurers, and clearinghouses for payment processing. HIPAA makes it all legal and then asks you to sign

off on it as a condition of receiving medical treatment! There are no federal privacy protections for patients who set up personal health records online, say at Google or other Web sites offering medical record services. Even hospitals and practices that currently use electronic storage formats report a high incidence of security breaches, with a quarter of healthcare technology

professionals reporting at least one security breach in the past year. According to a 2006 Federal Trade Commission study, about 249,000 Americans had their personal information misused for the purpose of obtaining medical treatment, supplies, or services. Google has put itself center stage in the health records arena. In March 2008, Google announced an application that it hopes will alleviate the inefficiency of the current medical record storage system: Google Health. Google Health will allow consumers to enter their basic medical data into an online repository and invite doctors to send relevant information to Google electronically. The service is free to users. Features will include a “health profile” for medications, conditions, and allergies; reminder messages for prescription refills or doctor visits; directories for nearby doctors; and personalized health advice. The application will also be able to accept information from many different record keeping

technologies currently in use by hospitals and other institutions. The intent of the system is to make patients’ records easily accessible and more complete and to streamline record keeping.

Google has proven that it is very good at what it does. It is, among other things, one of the largest advertising firms in the world, and the largest Web tracker of individuals in the United States. But what if Google were seeking personal information about you? You might not feel as good about Google’s quest to organize the world’s information when you consider that some of that information is information you’d prefer remain private. Google’s development of its Google Health application

illustrates the conflict between its self-avowed mission and the individual’s right to privacy. Would you trust Google with your health records knowing that a potential employer, or current employer, might be able to access those records? Proponents of electronic health records argue that computer technology, once fully implemented, would enhance security rather than threaten it. They also

believe that it is more important to first get the system up and running than to worry about privacy matters. Congressional Representative Joe Barton of Texas, an advocate of legislation that would speed the development of such records, said that “privacy is an important issue, but more important is that we get a health information system in place.” Lawmakers like Barton feel that the benefits of systems like Google Health outweigh the privacy risks, and that further legislation to impose privacy controls can be added after the fact. Some experts disagree with that stance, saying that unless an electronic system has sufficient privacy controls from the outset, it is less likely to become universally used. Even if the system’s security controls are sufficient, it is important that consumers are aware of those controls and confident that they can use the system without fear of their records being accessed by unauthorized parties. Creating an electronic health system without the proper security controls would not only be an unacceptable privacy risk, but would be doomed to failure because potential users would be unwilling to cooperate with the information requirements of the system. Google is not the only company to set its sights on online medical records. Microsoft and Revolution Health Group LLC, founded by AOL co-founder Steve Case, among others, are also launching similar sites where users can maintain online health profiles. As of yet it is too early to tell whether any of these ventures will be successful in the long term. The federal office in charge

of creating a national network of electronic health records, the Office of the Coordinator of Health

Information Technology, announced in March of 2008 that it plans to integrate its system with both Google and Microsoft’s healthcare databases, among others. One way or another, private industry and government will likely move forward slowly towards a national medical record information system. The ethical and moral dilemma posed by this national system involves an inherent conflict between two closely held values: medical care efficiency and effectiveness versus the privacy of your personal medical information.