Connectivity, Privacy, and Liability: What Medical Professionals Must Consider

by Alan S. Wernick, Esq.

Computing connectivity is usually equated with convenience. However, this convenience can prove to be a liability for healthcare organizations. Any employee can plug a USB memory device into the hospital network and download patient data. This type of transaction is quick, easy, and potentially fraught with legal risks and liabilities for the organization and the patient.

There are a number of ways to get connected to data nowadays, including universal serial bus (USB) devices, Bluetooth devices, infrared devices (also known as IR or IrDA), radio frequency identification (RFID) devices, wireless fidelity (WiFi), and handheld hard drives that can store gigabytes of data. Many of these devices are small enough to put on a key chain or carry in a pocket. Each can enable the user to copy significant amounts of confidential personal data in less time than it took you to read this paragraph.

A Matter of Security

Over the past few years many data thefts or misappropriations have been reported in the news, including data losses involving USB devices. For example, in November 2006 Charter College of Education at California State University in Los Angeles, CA, reported that an employee's personal USB drive was stolen. The drive contained the personal information of 2,534 of the college's credential program applicants, students, program completers, and faculty supervisors.

The drive also included the names and Social Security numbers of faculty supervisors as well as the first and last names, Social Security numbers, campus identification numbers, phone numbers, and e-mail addresses of applicants, students, and program completers. Another theft occurred in September 2006 when Erlanger Hospital in Chattanooga, TN, reported a USB drive lost. The missing device contained the names and personal identifying information of more than 4,100 current and former hospital employees.

Electronic health records (EHRs) are becoming more prevalent, and as more health services are commoditized (for example, health clinics in drug stores), more patient health and billing records will be electronic. There are many benefits to be gained from EHR implementation and use, including the potential for fewer patient treatment and medication errors.

In the future the myriad of electronic connectivity devices will shrink in size while increasing in storage capacity. Small, portable, high-capacity hard drives are already entering the consumer marketplace. Consider the potential risks and liabilities of a physician being able to carry a patient's entire medical history, integrated with various medical and drug interaction reference texts, in his or her hand. And consider the potential risks and liabilities of patients carrying cards containing their entire medical history from birth to the present day in their wallets.

Legal Ramifications

State legislators, Congress, and the courts have given considerable thought and analysis to these potential risks and liabilities. Indeed, many states have passed data breach legislation (see "Data Theft and State Law" in the November–December 2006 *Journal of AHIMA*). These laws include familiar names such as HIPAA, Gramm-Leach-Bliley, and Sarbanes-Oxley.

The courts are weighing in as well. When economic or physical harm results from identity theft, the courts will award damages. In one tragic case in New Hampshire, the careless sale of personal information was followed by the murder of the data subject. In that case the plaintiff was found to have standing to sue, which supports the view that actual harm creates legal standing to sue for data security breaches. The case involved a data broker who provided personal identifiable

information to an individual, a stalker, who subsequently committed suicide after he used that information to locate and murder the data subject.

Whether the entity holding the data is in the business of reselling that data, like the data broker in the New Hampshire case, or the entity holding the data uses the data in the day-to-day operation of the entity's business (a hospital or doctor's office using patient medical or financial data), the courts are likely to hold the entity accountable for the mishandling or misappropriation of the personal identifiable information that results in damages.

However, the courts are not awarding *speculative* damages to alleged identity theft plaintiffs. Recently federal courts in Arkansas, Minnesota, and Ohio, in separate cases (including a potential class-action lawsuit), were confronted with plaintiffs alleging potential identity theft damages due to a data breach.

In each case the respective court agreed with the defendant and found that the plaintiff's damages were speculative. Essentially, the plaintiffs in each of these cases had received notice that their personal identifiable information was included in the data breach alleged in each of the respective cases. However, none of the plaintiffs had actually been the victim of identity theft. The courts in these cases said that speculative damages for identity theft are not to be elevated into actual damages for which the defendant may be held liable. As such, the courts were saying that the plaintiffs lacked standing or the legal right to bring the lawsuit.

As identity theft and data breach cases evolve, plaintiffs with actual economic damages as a direct result of identity theft resulting from a data breach most likely will present the legal basis for standing as a foundation to determine their damage and the defendant's liability. Damages for identity theft may include (by way of example and not limitation) financial losses from the victim's bank account, renewal fees for lost identification cards (such as driver's license), loss of medical benefits, and attorney fees. Damages will depend on the actual facts of each case.

Hospitals, organizations, businesses, and governmental units may also experience liability for damages as a result of failing to act in accordance with all applicable data breach laws. Which data breach law applies may depend on the residence of each of the affected individuals in the compromised database and not the location of the entity that experienced the data breach.

While financial damages to a hospital or other business from a data breach can be significant, they can pale in comparison to a potentially far more deadly damage to an organization-the loss of trust from patients or customers who entrusted the organization to protect their personal identifiable information. This loss of trust can potentially have a far greater negative impact on the institution than any out-of-pocket financial damages award. For example, such loss could jeopardize a hospital's EHR implementation or its programs for improvement of quality care.

Steps to Manage Liability

What can medical professionals and hospitals do to manage the liability risks for data breaches resulting from interconnectivity? Steps for consideration include the following:

- **Have a legal audit done by knowledgeable legal counsel,** preferably one with a technology background and familiarity with data privacy, security, and compliance. A legal audit includes interviewing people in the organization, reviewing practices and procedures (by way of example and not limitation, reviewing vendor contracts for data privacy and related risks), identifying the strengths and weaknesses of compliance with the applicable statutes and laws, and identifying potential risks regarding data privacy and data security.
- **Have a security audit done by a knowledgeable security professional** working with knowledgeable legal counsel.
- **Use encryption** to secure data at all times.
- **Require users to use at least two security elements for interconnectivity access.** This might include a strong password that is changed periodically and something that must be carried (in addition to the interconnectivity device); for example, a security token that generates a unique random number linked to the network's main server.
- **Obtain appropriate insurance** coverage for data breach losses.
- **Educate users** about data security and data quality.

Finding balance between interconnectivity and risk management for data privacy, data security, and data quality will not be easy. Putting together a team of people from the organization and knowledgeable outside advisors is one proactive preventive

approach. Of course, some organizations take the approach of waiting until a problem occurs and dealing with it then. While the first approach will be expensive, suffice it to say that it will be far less expensive than the increased lost management time (i.e., "crisis mode") and increased legal expenses involved in having a court or government agency handle the problem.

Interconnectivity issues will only increase over time as new technologies allow for new ways to access data necessary for medical and other professionals to do their jobs. While the legal risks can be managed, they may not be entirely removed. It is a process and should be treated like one. As the old Chinese saying goes, "if you don't know where you are going, any road can take you there." Which road will you take to connect with your data?

Alan S. Wernick *(alan@wernick.com) is an attorney at Wernick & Associates, Ltd., in Chicago, IL.*

Article citation:
Wernick, Alan S.. "Connectivity, Privacy, and Liability: What Medical Professionals Must Consider" *Journal of AHIMA* 78, no.4 (April 2007): 64-65.