

June 12-18, 2009

## PRESCRIPTION FOR CHANGE

Take steps now to protect your private health care records in the digital age

**D**igital records have become part of the American desktop. Electronic banking, e-ticketing, eBay, Amazon and yes, Facebook, are just a few examples of processes and sites we use to upload confidential information to the Internet — trusting blindly that it won't be hacked, disclosed or otherwise held for ransom.

In our data-crammed e-world, however, health care remains the last bastion of 19th-century technology. In a survey last year, the New England Journal of Medicine found that only about 4% of physicians rely upon a fully functional electronic records system, and just 13% have a "basic" system. Sadly, because the specifications of these proprietary systems vary widely, their underlying data structures may not be compatible and, therefore, may not communicate or play well together.

If President Obama achieves his agenda, the days of paper folders with multicolored stickers may end. The American Recovery and Reinvestment Act of 2009 outlines \$19 billion in funding for hospital-technology efforts — enough money, perhaps, to finally push, pull and drag change-resistant hospitals and doctors into the 21st century. The act's stated goal: "Utilization of an electronic health record for each person in the United States by 2014."

The Obama administration is counting on the potential savings associated with this shift to digital to help cut the deficit and stimulate the economy. During his campaign, Obama promised that, by taking steps including "investing in a paperless health care system to reduce administrative costs," the government could save \$120 billion a year, or \$2,500 per family. That's an eye-grabbing number, but some question the factual basis and mathematical accuracy of this prediction because it's based on a study estimating cost savings that won't happen until 2019. Savings or not, it appears our nation's physicians are likely to be "data-entered" into this century.

So what are the privacy implications of this record migration — and what can you,



### EMPLOYMENT LAW

John T. Palter

the health care consumer, do to protect your privacy?

The Health Insurance Portability and Accountability Act of 1996 establishes standards for patient privacy in all 50 states, including the right of patients to access their own records. Although the act provides some protection, it isn't the final answer to medical records privacy. A recent judicial interpretation of the act's regulations, for example, significantly limited its breadth. Moreover, a 2006 article in The Washington Post noted that, while it received more than 19,000 wrongful disclosure complaints under the act, the government has imposed only a single fine to date. Single. As in, one. The takeaway point is don't count on the government to protect your information.

#### Record privacy tips

So how, exactly, can you limit others' access to your medical records? Here are some suggestions.

■ **Establish, review and edit your own medical treatment history.** Obtain copies of your medical records while you can, and verify that the information is accurate. The conversion to e-records will be replete with coding errors. Count on it.

■ **Talk to your doctor.** Start your privacy efforts with your physician. If you want a specific condition to be held in confidence, bring a written request to the doctor's appointment that revokes your consent to release medical information to the insurance company and/or to your employer for that visit. Under the

act, attempts to restrict the sharing of specific records may be denied by the health care provider. Depending upon the circumstances, you should consider paying for some visits out of pocket rather than seek reimbursement from your insurance company.

■ **Redline your releases.** When you're asked to sign a medical release, limit the information released to exactly what you're comfortable sharing. Instead of signing the "blanket waiver," you may decide to limit the information to be shared (e.g., dates of treatment, condition) and with whom it may be shared (e.g. insurer).

■ **Educate your employer.** If your employer is self-insured, it's likely to have access to the health-related claims you file. Talk to the plan's administrator about the company's privacy protection policies. Follow up with a letter stressing — tactfully — your desire for confidentiality, and keep a copy.

■ **Think twice before answering marketing-related questionnaires, surfing health-related Web sites or participating in online discussion groups.** Electronic health sites and communications commonly ask for a great deal of family health information. Before sharing personal information with a health Web site, find out if it participates in a Web seal program such as TRUSTe, [www.truste.org](http://www.truste.org), URAC Health Web Site Accreditation, [www.urac.org/directory/DirectorySearch.aspx](http://www.urac.org/directory/DirectorySearch.aspx), HON (Health on the Net), [www.hon.ch](http://www.hon.ch), and BBBOnline, [www.bbbonline.org](http://www.bbbonline.org). Remember that a few free coupons or a chance to win a contest aren't worth very much when weighed against the value of your medical privacy.

While the shift to electronic medical records may be inevitable, speaking with your physician and remaining vigilant should limit the risk of wrongful disclosure.

**PALTER** is a trial lawyer and managing member of Riney Palter PLLC ([www.rineypalter.com](http://www.rineypalter.com)). Contact him at [jtpalter@rineypalter.com](mailto:jtpalter@rineypalter.com).