



Posted On: **October 5, 2011** by **Patrick A. Malone**

Patient Privacy Is Compromised by Identity Theft

We've all heard tabloid tales of hospital personnel taking unauthorized peeks into celebrity patient files and selling the dishiest contents for personal gain. But there's also reason for the rest of us to guard our medical records like we do our bank accounts.

According to a [survey](#) by PricewaterhouseCoopers, nearly 4 in 10 doctors and hospital staffers have caught one patient trying to use somebody else's identity to obtain health-care services.

As reported on [MedPage Today](#), patients seeking medical care under another name was the second most common privacy or security issue reported by providers. Medical identify theft is the fastest-growing form of identity theft; 1.42 million Americans were victims in 2010 at a cost of \$28 billion.

Security breaches occur most often by the careless treatment of patient files in doctors' offices, hospitals, insurance companies or life science organizations. These problems can be as simple as leaving a document visible to others, posting comments on Facebook or conducting improper elevator

conversation. Other common transmitters of swiped ID are stolen laptops and smartphones. Patient data is used to submit fraudulent claims and to seek medical care in somebody else's name.

This isn't about the high-techery of computer hacking, but the low-techery of clueless, careless or corrupt medical personnel. As summarized by MedPage, the survey concluded that "Digitized health information is becoming increasingly popular, but the majority of health organizations are ill-prepared to protect patient data as the health-care industry moves toward electronic systems."

More than half of the survey respondents said they had experienced at least one issue with information privacy and security over the past two years. One in 4 insurers reported improperly transferring files that contained protected health information.

That's unacceptable, and as a patient, you must ensure the security of your information. Inform your health-care and insurance providers that privacy and security are as important an aspect of your health care as a prompt and proper diagnosis. That you have zero tolerance for compromised files.

James Koenig, director of the Health Information Privacy and Security Practice at PricewaterhouseCoopers, noted that the federal Health Information Technology for Economic and Clinical Health (HITECH) Act requires medical privacy breaches to be disclosed, but only for paper-based health information, not electronic records. That's an unacceptably huge gap in privacy coverage.

*People interested in learning more about our firm's legal services, including **medical malpractice in Washington, D.C., Maryland and Virginia**, may ask questions or send us information about a particular case by phone or email. There is no charge for contacting us regarding your inquiry. A **malpractice attorney** will respond within 24 hours.*

*All contents copyrighted 2010 **Patrick Malone & Associates** except where copyright held by others. Reproduction in any form prohibited except where expressly granted.*

Patrick A. Malone
Patrick Malone & Associates, P.C.
1331 H Street N.W.
Suite 902
Washington, DC 20005

pmalone@patrickmalonelaw.com
www.patrickmalonelaw.com
202-742-1500
202-742-1515 (fax)