



Mitigating a Risk & Protecting Patient Privacy

By David A. Sobel, Ph.D.

July 26, 2004

Jane Doe, a fictitious name for a real person, was treated for depression in an Emergency Room. Jane Doe is thirty-one years of age. She is a single parent of two young children. And, she has breast cancer.

Karen Baker, also a fictitious name for a real person, is employed as a receptionist by a community-based physician office practice.

Two weeks after Jane's visit to the ER, Karen Baker used her access privileges to look up and review Jane Doe's computer-based record. This record includes diagnostic information, laboratory test results, and the results of diagnostic imaging.

Karen Baker printed and altered Jane Doe's medical record and then mailed this altered record to a state agency. This state agency opened an official investigation to determine if Ms. Doe was fit to parent her two children.

As part of the investigative process, Ms. Doe's children were taken out of their elementary classrooms and asked questions about their mother. In addition, Jane missed several days of work in order to defend her suitability as a parent.

The practice where Karen Baker is employed is not involved in the care or treatment of Jane Doe, but it does have access to the hospital's patient care systems. In fact, several members of this practice have access to all patient records in the hospital's data repository.

Believing that her privacy rights were violated, Jane Doe wrote a letter of complaint to hospital administrators. The hospital's response was that it did nothing wrong and that its policies and procedures comply with all applicable federal and state laws. Not satisfied with the hospital's response, Jane sought legal counsel. I served as an expert witness for the plaintiff, Jane Doe.

You won't read about this case in the newspapers. It was recently settled out-of-court and the details are confidential. But I can share with you two points: 1) this is one of the most egregious breaches of confidentiality resulting in patient harm that I have ever been privy to, and 2) I have Jane's permission to discuss this case in forums where it might serve to prevent similar incidents and harm to patients and their families.

Your practice may have access to a hospital's computer-based records in order to access patients' laboratory test results and the results of diagnostic imaging studies. Your access privileges, and those of your staff members, may include the ability to review all patient records.

If you and/or members of your community-based practice have access to all patient records in a hospital or healthcare system's database, you are at risk.

To mitigate your risks, and to prevent harm to patients, consider the following issues:

1. **Does the hospital have a formal policy regarding the establishment and use of computerized links with satellite offices?** Hospitals that provide community-based physicians with access to its systems should have a formal policy that states what information will and will not be provided to a medical practice. This policy should specify the levels of access that will be provided to physicians, nurses, business managers, and other office personnel. And, it should cover how access is to be granted and how it is to be revoked. Additionally, the hospital's policy should comply with all applicable laws and regulations, as well as with generally accepted information security standards.
2. **Does your practice have an Information Security and Privacy Policy?** The Privacy Rule requires that your practice have appropriate policies and procedures regarding the use and disclosure of protected health information. In addition to covering topics such as faxing health information, using e-mail to communicate with patients, and leaving messages in voice mail systems, your policy should include a section on accessing patient information from the hospital's data repository.

3. **Do you have a formal program to educate members of your staff about all matters pertaining to privacy and information security?** One of the best ways to protect patient privacy rights and reduce your risks is to educate members of your staff about their responsibilities to protect patient privacy. As a matter of practice, you should be orienting all new employees to the importance of safeguarding health information. Consider adding to your current educational awareness program the topic of accessing patient information from the hospital's system.

4. **Do you require every physician and staff member in your organization to sign a Confidentiality Agreement?** Every member of your practice should be required to sign a confidentiality agreement as a condition of employment. This agreement should leave no doubt in anyone's mind that those who violate your organization's policies and procedures may be terminated, and that in some cases, legal action may be brought against an individual.

Hospitals and healthcare systems are often eager to provide community-based physicians with access to their IT systems. Such access improves the quality of care physicians provide to their patients. However, in a hospital or healthcare system's eagerness to please and establish close ties with community-based physicians, information security may take a back seat. By establishing appropriate administrative and technical safeguards, you will protect patient confidentiality, reduce your risks, and comply with all applicable laws, including HIPAA's Privacy Rule and Security Standard.

David Sobel is the President of Confidentiality Matters, Inc., a firm that provides information security services to healthcare organizations. He may be reached at dsobel@confmatters.com. For more information on Confidentiality Matters, visit www.confmatters.com.