

Issues up close

No peeking allowed

By Susan Trossman, RN



The benefits of electronic health records still outweigh the risk of unauthorized use.

WHETHER IT WAS AN ISOLATED INCIDENT or just the tip of the iceberg, a breach in patients' electronic health records at a California hospital may serve as a wake-up call to all healthcare professionals, who are ethically and legally bound to ensure patient privacy and confidentiality.

"There's no ambiguity in our code of ethics," says Barbara Ott, PhD, RN, nurse ethicist and Pennsylvania State Nurses Association member. "I would not expect a nursing student, a new nurse, or an experienced nurse to think there is any wiggle room when it comes to maintaining patient privacy and confidentiality."

Yet RNs and physicians were among those who reportedly peered into the electronic hospital records of some high-profile patients, allegedly including Britney Spears, Farrah Fawcett, and Maria Shriver, within the UCLA Health System. California public health department officials stated that the records of about 1,040 patients have been breached over the past few years and 165 employees have been disciplined, according to an October 30, 2008 article in the *Los Angeles Times*.

Around the same time, the U.S. Department of Health and Human Services (HHS) Office of Inspector General was issuing a nationally focused report stating that the Centers for Medicare and Medicaid Services had taken "limited actions to ensure that covered entities adequately implemented the Health Insurance Portability and Accountability Act of 1996 Security Rule." The rule requires health providers who transmit electronic health information to ensure the integrity and confidentiality of the information, protect against anticipated threats or risks, and guard against unauthorized uses or disclosures.

ANA's Center for Ethics and Human Rights Director Laurie Badzek, MSN, JD, RN, LLM, NAP, added that HHS recently launched a project ultimately designed for most Americans to have access to "secure and interoperable" electronic health records by 2014.

"Strict adherence to the ethical standards of confidentiality and need-to-know access will be crucial if you think about a system being available nationally to any healthcare provider with a keyboard," says Badzek, a West Virginia University School of Nursing professor.

Documents of the profession

From the first days in nursing school, students learn about key documents in nursing—among them ANA's *Code of Ethics for Nurses*. Within it are principles outlining nurses' responsibilities to safeguard patient privacy and maintain confidentiality of all patient information.

Specifically, the code states: "The patient's well-being could be jeopardized and the fundamental trust between patient and nurse destroyed by unnecessary access to data or by the inappropriate disclosure of identifiable patient information."

The code also addresses nurses' need to pay special attention to maintaining data security when using electronic communications. Perhaps that's why it was so troubling to nurse experts in informatics and ethics to think that any healthcare professional intentionally would delve into patient records without having a legitimate reason.

"I believe nurses do take patient privacy and confidentiality seriously," says Pauline Robitaille, MSN, RN, CNOR, director of perioperative services at a Colorado hospital and member of ANA's Congress on Nursing Practice and Economics Work Group on Electronic Health Records. "It's something that's drilled into nurses as part of our ethics, and it's discussed at my work site quite often. I even receive routine notices from our IT (information technology) department reminding staff to not leave their work stations unattended if they are still signed on to a computer."

Although the position statement on electronic health records developed by Robitaille's work group hasn't been finalized, it emphasizes that the "principles of privacy, confidentiality, and security cannot be compromised" when healthcare IT is created, implemented, and integrated within wider systems. It also addresses the public's right to expect that their healthcare data will be correctly stored and used. (ANA's other position statements on privacy and confidentiality, nursing informatics, and principles of documentation are available at www.nursingworld.org.)

Besides talking about the importance of nurses' involvement in selecting electronic health record systems, Robitaille recalls a fair amount of discussion among work group members about the importance of ensuring the security of data.

"At the time, there certainly were enough stories in the news about significant breaches in the confidentiali-

ty of people's electronic data," she says. "Two of the major benefits of having electronic records are that they provide nurses and other healthcare professionals with immediate access to information and they improve the flow of that information. But accessibility is also a risk, because it means a lot of people can get into those records."

Carol Bickford, PhD, RN-BC, a senior policy fellow in ANA's Department of Practice and Policy and liaison to the work group, adds that the same principles that govern documentation in the "paper world" also apply to electronic health records. "Nurses should only be looking at the (electronic) charts of patients to whom they are assigned," Bickford says. "If security is in place, those who don't need to know information on patients should not be able to access that information."

However, restricting access can pose problems at times. For example, when an RN covers for another staff nurse who's on break or dealing with an emergency, the covering RN can be locked out of the extra patients' records. Nurse faculty also have been stymied in their ability to review patient charts when making student assignments during clinical rotations, according to Bickford.

Nurse informaticist Sharon Sweeney Fee, PhD, RN, and other interviewed nurses believe the benefits of electronic records still far outweigh the risks. Throughout the Montana healthcare system where Sweeney Fee works, emergency physicians, for example, can access a patient's records from two off-site clinics and nurses can review a patient's medications, vital signs, and progress notes—which can give them a more accurate and faster picture of the patient's overall health and needs.

"This access also saves the patient from having to answer the same question over and over again," says Sweeney Fee, a member of ANA's Center for Ethics and Human Rights Advisory Board. "And it means healthcare professionals can spend more time listening to their patients."

The Montana Nurses Association member also believes that all staff who work with IT know the importance of security. "But when these systems are designed, the No. 1 priority is to satisfy provider needs," Sweeney Fee says. "There is software that can monitor who's accessing what, but not all facilities have the funding for implementing that capability."

However, many safeguards are in place, including password-protected access to certain patients or departments. And Sweeney Fee and other nurses believe electronic systems are much safer than paper documentation. "We're not always copying and faxing paper all the time in plain view," Sweeney Fee says.

Robitaille concurs, recalling how staff used to use

addressographs that imprinted multiple copies of lab requests and other documentation; it wasn't unusual to see forms waiting to be filed in charts around the nursing station.

Adds Sweeney Fee, "There's a real dichotomy in this country. The public wants electronic health records, yet they're always concerned about its security—even if they have no problem with online banking or shopping."

She further believes that when breaches do occur in electronic systems but don't result in harm, those outcomes—and the protections that were in place—also should be publicized. That action will help build the public's confidence.

Keeping data safe

Robitaille has been involved in implementing four different electronic health systems since 1992 at various healthcare facilities. Each generation has brought improvements in accessibility, ease of use, and security. At her current workplace, the system has several layers of security. For example, with her password, she can check a lab result for one of her patients, but the Colorado Nurses Association member cannot access the entire lab module. "And when I look at patient records to check billing accuracy, I know my access is being recorded and IT staff can see which fields I have gone to," she says.

Nurses suggest several strategies to protect patient data, including:

- educating staff about the ethics and laws guarding patient health records
- ensuring nurses help craft facility policies and guide the development and implementation of electronic health record systems
- promoting increased funding to IT departments to implement more secure software that includes user-traceability
- utilizing filters on computer screens to prevent them from being easily read.

Badzek adds that the multistakeholder Ethical Force Oversight Body, which ANA is a part of, developed a privacy and confidentiality information toolkit to help organizations assess their ethical climate on those vital principles (available at www.ama-assn.org/ama/pub/category/9103.html).

Ott believes that nursing programs need to do a better job educating students about the "covenantal relationship" between nurse and patient. "It can sometimes be a hard concept to get across, but understanding it is important," says Ott, associate professor at Villanova University College of Nursing. "And grooming good character is equally important." ★

Susan Trossman is Senior Reporter in ANA's Communications Department.