Protecting Patient Information
In an Electronic Age: A Sacred Trust

Peg Kerr

The role of the nurse includes safeguarding the personal health information of patients. Confidentiality and privacy (see Table 1) are fundamental rights guaranteed by law (U.S. Department of Health and Human Services [DHHS], n.d.), and the legal and ethical responsibilities nurses have in this regard should not be taken lightly. However, fulfilling these responsibilities in a technologically complex environment is challenging. Confidential information is necessary when providing health care. Nurses receive and disperse confidential information as part of their job duties. Despite the fact that confidential information is routinely shared, access to this information is a privilege and responsibility. This trust must not be taken for granted.

During his Presidential campaign, Barack Obama addressed members of the Veterans of Foreign Wars using a “sacred trust” theme. In his speech, “sacred trust” was defined as “America will be there for you just as you have been there for America...from the moment you put on that uniform.” Barack Obama further stated that as Commander-in-Chief, his function includes “to safeguard this nation’s security and to keep that sacred trust” (Murray, 2007).

The interpretation of “sacred trust” by President Obama provides an analogy to the bond that occurs between nurses and patients. Specifically, nurses will be there for patients from the moment they seek nursing care, and nurses need to safeguard the security of patients’ health information and keep that sacred trust.

All talk of sanctity aside, there is a need for an occasional refresher on exactly what this means and more importantly, how to accomplish it in an electronic technology environment. This article will provide a brief overview of electronic technologies in the health care workplace; address the challenges that electronic technologies present with respect to security, review laws

Table 1.
Definitions

<table>
<thead>
<tr>
<th>Privacy A Right</th>
<th>Confidentiality An Obligation</th>
</tr>
</thead>
<tbody>
<tr>
<td>The right to keep personal information withheld from others.</td>
<td>The obligation to respect the privacy of patients.</td>
</tr>
<tr>
<td>The right to determine which personal information is to be shared with whom and for what purpose.</td>
<td>A violation occurs when information deemed private, and divulged in confidence, is shared with others.</td>
</tr>
</tbody>
</table>

Source: Erickson & Millar, 2005.
related to privacy; and examine the implications for nurses in maintaining patients’ privacy.

**Technologies and Security in the Workplace**

The implementation of electronic technologies in health care settings, as well as patient privacy and confidentiality consequences, are occurring and changing frequently, making it difficult to grasp their meaning. The transition from paper charts to electronic medical records (EMR) has been one of the biggest changes. Nurses, the professional caregivers who spend the most time with patients, become key stakeholders in documenting and retrieving information from an EMR.

As more health information is maintained using the EMR and shared between providers and institutions, the privacy and confidentiality of this information may be at risk. One challenge associated with the EMR surrounds information storage and access. The electronic format allows large amounts of data to be stored in a very small space. One keyboard stroke has the potential to place page after page of patient data at the computer user’s fingertips, making unauthorized access to the information easier than access to paper records. An EMR cannot be locked in a file cabinet or storage room. Harman (2005) posits that the need to disclose health care information across continuums of care and to obtain third-party approval and reimbursement detracts from the ability to maintain integrity of these data.

According to Christensen and Frank-Stromborg (2001), the most common violations of patient privacy are staff abuse or misuse of the right to access records and unofficial access to patient records. An example of the abuse/misuse of the right to access records is sharing confidential information seen in a record with a neighbor or friend who does not have a right to the information. Unofficial access involves the viewing of a record for which there is no rightful basis for doing so. A well-known example of this is the record breach of famous actor George Clooney following his treatment at a New Jersey hospital for injuries suffered in a motorcycle accident in 2007. Television networks reported that employees not involved in caring for Clooney logged into the computer network and looked at his records. As a result, the hospital issued a statement saying that 27 employees were suspended for unauthorized access to the system (“Background on the Clooney Medical Records Breach,” 2007).

The ability to send a document via facsimile (fax) has been available for some time. Erickson and Millar (2005) claim this is one of the least secure forms of electronic technologies for transmitting confidential patient information. The problem, according to these authors, is that once something is faxed, the sender has no control over the conditions under which it is received. Thus, faxed data with confidential information might be printed in an open, unsecured office area, or received by a person who has no legitimate reason or right to see the information. Cover sheets provide scant protection in these situations.

Patients and family members are becoming more technologically enlightened and use electronic mail (e-mail) as a preferred method of communication with their health care providers. Some experts predict that electronic communication between patients and providers will become the “norm rather than the exception” (Luo, 2008, p. 25). In addition to e-mail, other forms of computer-assisted electronic communication include instant messaging (IM) and voice over Internet protocol (VOIP), which allow for real time questions and responses between patients and providers (Luo, 2008). The Pew Internet Project’s May 2008 survey determined that 73% of adults in the U.S. go online (Fox & Vitak, 2008).

There are many privacy issues associated with electronic communications. These include who has access to these messages, what sorts of transactions are appropriate, and should certain subject matters be prohibited. Do these documents become a part of the permanent health record, and can messages ever be forwarded? One of the most obvious issues is how to keep the content of messages secure, since the confidential information possibly contained in these communications could be exposed to Internet hackers. Encryption programs exist to protect messages from hackers, but the recipient of the message must know how to decrypt and decompress the file (Luo, 2008).

Seventy-eight percent of adults in the U.S. have a cellular telephone (cell phone), making them a ubiquitous means of human interaction (Fox & Vitak, 2008). In addition to their voice communication function, many cell phones provide the ability to take a still or video picture, which can be forwarded. Most phones are also capable of texting messages. Few policies exist that provide standards for using cell phones in a health care setting.

Personal digital assistants (PDAs) represent a technology that is experiencing a great increase in use (Erickson & Millar, 2005). These provide computer and Internet accessibility using a device small enough to fit into a pocket. Most PDAs allow clinicians to store health information and also provide access to health care databases. Nurses can use a PDA to check for drug interactions, calculate accurate dosage amounts, and consult evidence-based practice guidelines or other activities that reduce the probability of dangerous errors (Abrahamsen, 2003;
In the future, nurses may be consulting these online records to obtain information in circumstances where patients or loved ones are unable to provide it. 

Knox & Smith, 2007). 

Emerging advanced technologies also address concerns related to patient safety. Examples of these include image-based sensors and video cameras to detect falls, and mobile safety alarms with drop sensors and positioning devices to monitor falls and wandering (Melander-Wikman, Falthom, & Gard, 2007). Implantable radio frequency identification (RFID) microchips are another option. The technology for an RFID microchip is similar to that of animal tags to identify lost pets. The RFID provides a radio wave signal that is converted into digital signal and transmitted to registries containing links to institutional EMRs, advance directives, organ/tissue donor information, and other applications (Foster & Jaeger, 2008). The development of RFID tags has resulted in concerns about the potential for misuse of this information by criminals, employers, or the government (Westra, 2009). Privacy concerns related to the potential for tracking of individuals exist. There is also the need to balance an individual’s right to privacy with their need for the safety and mobility that these technologies can potentially provide for them.

Finally, another electronic technology that has security implications is the personal health record (PHR) being tested by various corporations, including Google and Microsoft. This is an online software tool that provides health care consumers—patients—total control of their health information (Engstrom, 2008). The Google service, known as Google Health, is free and allows individuals to post electronic copies of information, such as allergies, medications, laboratory and X-ray results, hospital stays, and medical conditions to a secondary health record stored on Google computers. Users may selectively make their records accessible to friends, loved ones, or care providers (Bergen, 2009). In the future, nurses may be consulting these online records to obtain information in circumstances where patients or loved ones are unable to provide it. However, it is not known whether patients clearly appreciate the implications or threat of unauthorized access to the information they are placing on their home computers (Hamn, 2005).

Privacy Protections 

Nurses have always recognized the necessity for confidentiality, beginning with the Nightingale Pledge (McBurney & Filoromo, 1994). The American Nurses Association (ANA) adopted a code of ethics in 1950 in which patient privacy is specifically addressed. The code unequivocally states, “The nurse safeguards the client’s right to privacy” (ANA, 2005).

In addition to ethical obligations, privacy laws also safeguard patients’ rights regarding disclosure and use of personal health information (DHHS, n.d.). In 2002, the U.S. Congress amended the Privacy Rule in the Health Insurance Portability and Accountability Act (HIPAA) of 1996. This Federal law controls the privacy, security, and confidentiality of patient information. The primary concern and focus of this law is “protected health information” (PHI), defined as: 

*Individually identifiable health information relating to an individual’s past, present, or future physical or mental health condition; provision of health care; or payment for the provision of health care. It also includes names, telephone numbers, addresses, medical record numbers, and Social Security numbers (DHHS, 2003).*

Under HIPAA, personal health information cannot be utilized for reasons unrelated to health care or administrative/financial purposes, and only the minimum amount of information may be released when necessary. Patient consent is required before information can be shared for any other non-health care purposes (DHHS, n.d.).

HIPAA education sessions have been mandated, and thus, all nurses working within a clinical setting should have attended an educational forum on this topic. It is required that patients receive information and provide authorization for their personal health information to be disclosed and the reason for the disclosure.

Implications for Nurses 

The implication of electronic patient information for nurses is vast. As caregivers, nurses work with PHI on a daily basis. Therefore, nurses are responsible for adhering to the present privacy laws. It is imperative that nurses are well-informed about HIPAA law. The HIPAA Web site contains a complete and useful summary explanation of the law (DHHS, n.d.).

Nurses must also comply with mandated attendance at HIPAA training seminars, as required by their employer. The
pace of technology change and adoption requires ongoing education to assure appropriate compliance with this law.

Nurses should be aware of and be able to comply with policies and procedures of their employer related to release of patient information. Identification of resource people provides a mechanism to address concerns as they arise. Some employers have developed a “privacy officer” role. These individuals can respond to concerns about disclosure of patient information.

As employees, nurses should be aware of policies regarding fax and cell phone use within a patient care setting, policies related to Internet use, picture taking, hand-held device use, user ID and password use, RFID technologies used in the institution, and any electronic monitoring devices in place. Questions about the acceptable use and appropriate role of these electronic technologies in clinical settings may be used to spur conversations with nurse managers and co-workers about compliance with HIPAA rules (Knox & Smith, 2007). The impact of electronic technologies is largely unknown in terms of patient privacy. Abrahamsen (2003) recommends that every individual makes it his or her business and priority to think about how new electronic tools may cause threats to privacy. Abrahamsen also recommends that nurses question whether existing policies are sufficient to cover privacy concerns posed by new technologies.

The protection of patient information can also be strengthened by mentoring others in the appropriate use of privileged information. Computer screens should be closed out after accessing information, electronic communications should be restricted to just minimally necessary information, printing out large amounts of health information from computers should be avoided, and policy and procedure manuals should be consulted for answers to questions about privacy concerns.

The use of technology in health care settings is expanding and changing on a daily basis. Without question, these result in concerns about patient privacy and confidentiality. Despite the potential peril to privacy posed by electronic health care tools, there is marvelous promise in terms of efficiency, safety, and cost savings. The present challenge for nurses is to continue to advocate patient privacy and confidentiality. The mission is clearly a bigger challenge these days. However, the bond must not be broken – it is up to nurses to keep the “sacred trust.”

References

Urologic Nursing Editorial Board Statements of Disclosure
In accordance with ANCC-COA governing rules Urologic Nursing Editorial Board statements of disclosure are published with each CNE offering. The statements of disclosure for this offer ring are published below.
Kaye K. Gaines, MS, ARNP, CUNP, disclosed that she is on the Speakers’ Bureau for Pfizer, Inc., and Novartis Oncology.
Susanne A. Quallich, ANP-BC, NP-C, CUNP, disclosed that she is on the Consultants’ Bureau for Coloplast.
All other Urologic Nursing Editorial Board members reported no actual or potential conflict of interest in relation to this continuing nursing education article.