But all I did was share a photo of my patient's wound with one friend... you couldn't even see his face!

What Nurses Need to Know about Informatics, Social Media, and Security!

Denise Hirst, RN, MSN

Purpose:

Advances in technology, telehealth, and an increasing global focus have had major impacts on the health care workforce. The purpose of this article is to provide information about current trends related to electronic information use and social networking as related to nursing practice.

Outcome:

Recognize healthcare information security advantages and risks. Identify appropriate and inappropriate use of social media.

Advances in technology have changed the way in which healthcare is delivered. These advances have made significant impacts on how nurses deliver and document patient care and communicate nursing issues (National Council of State Boards of Nursing Regulator Staff, 2015). The Pew Research Center reports that 88% of people in the United States use some form of internet-based social media (Pew Center, 2017). Ninety-four percent of respondents between the ages of 18 to 64 years, use social media. Further, respondents age 65 years or older reported a lower, yet significant utilization of social media at 64% (Pew Center, 2017). These data provide clear evidence that the information we place on the internet may be seen by roughly nine out of ten adults.

As technology continues to evolve and advance, it is critical that nurses understand technology's impact on healthcare delivery. With the wide variety of entertainment, educational, and information-technology advances, it is essential that we keep in mind ethical, legal, and security issues when considering use of these technologies. The opportunity to use a wide variety of web-based programs, including social media, to provide education and resources to the public and healthcare professionals is an impactful use of technology advances. However, as we use these tools, it is important to recognize the regulatory and legal implications.

Healthcare and Informatics Historical Perspective

Informatics is an enigma to some and a way of life to others. The term informatics is simply defined as "the collection, classification, storage, retrieval and dissemination of recorded knowledge" (Merriam-Webster, 2017) and can be broadly described as the practice of creating, storing, finding, manipulating, and sharing information. From as early as 1937 with the introduction of the first computer, a Model K Adder, to 1971, with the implementation of personal computing (Computer History Museum, 2017); society has integrated the use of technology for information management into almost all aspects of life. In healthcare, informatics provides advantages and poses risks.

Advantages

- Wellness and fitness information is readily available.
- Disease and illness information can be found through a simple web search.
- Electronic health records provide a method for documentation of care and treatment.
- Electronic health information is available across health care systems and individual healthcare providers.
- Patients have easy access to personal health information (PHI) and direct communication to their healthcare providers.

Risks

- Internet information may be misleading or inaccurate.
- Disease and illness information retrieved from the internet may be misunderstood, misinterpreted, or put to erroneous use.
- PHI can be compromised due to unauthorized access.
- Healthcare system data breaches pose a threat to health and personal data of all system participants.

J. Weaver (2017) reported that 80 percent of Americans who use the internet have searched for health-related topics. Nurses, aware of this evidence

should develop and implement strategies that will have a positive impact. In addition to directly providing healthcare education and information via electronic means, nurses can provide much-needed education and guidance with regards to the public's use of healthcare information retrieved from the internet. Nurses can implement strategies to provide safe evidence-based care and reduce risk of PHI compromise, by:

1. identifying and anticipating risks,
2. develop policies and procedures which provide for consistent electronic patient education practices
3. close monitoring and assessment for existing and emerging risks.

Protection and security of healthcare information in the electronic environment requires ongoing assessment, continuous monitoring and improvement of safeguards and security practices. The model shown in FIGURE A, developed by the Department of Health and Human Services (n.d.) demonstrates a cycle of monitoring to promote security and reduction of risks for breach of confidentiality, integrity and availability of private information.

Patient Trust and Confidentiality

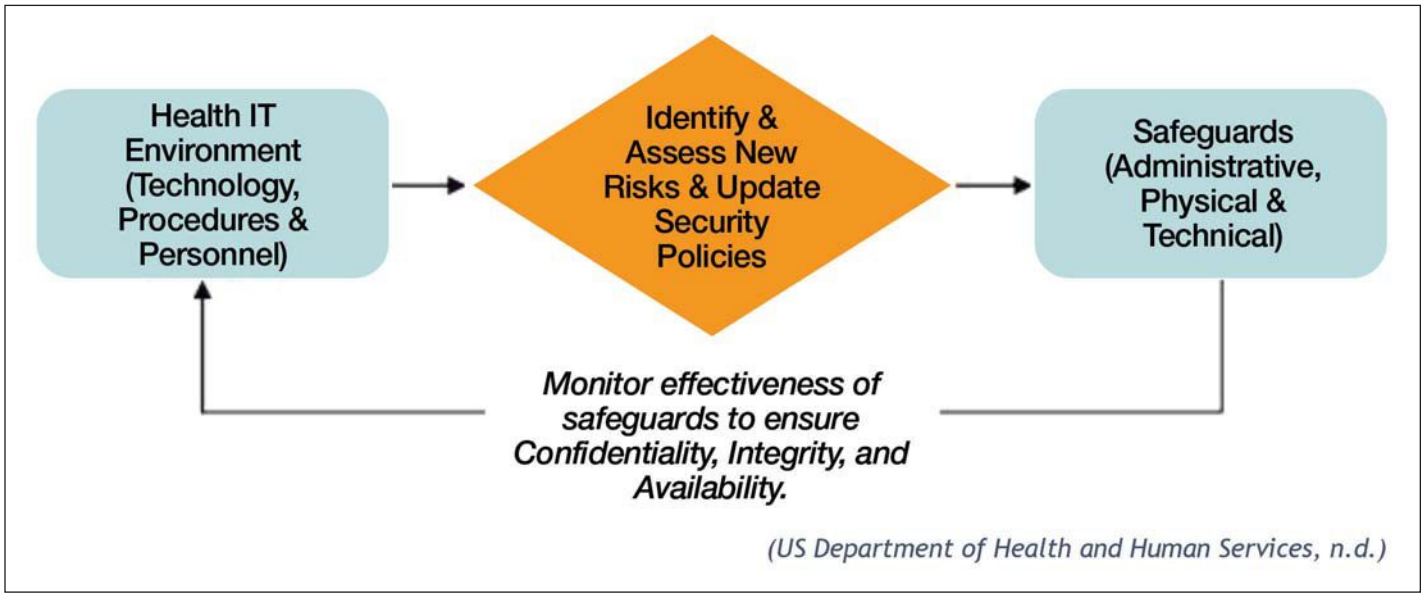
According to the January 2017 Gallup poll, nursing continues to be ranked the most trusted profession in the United States (The Advisory Board Company, 2017). Protecting those who entrust us with their healthcare and safety is not only a nurse's professional responsibility, it is a required by the North Carolina (NC) law and rules which regulate nursing practice. Ensuring that today's nurses remain competent in this responsibility in our modern era requires knowledge and understanding and correct application of evolving technologies used in healthcare.

As the information age continues to evolve, a multitude of electronic devices and software applications are available. Preserving our patient's trust and confidentiality can sometimes be a challenge. The "Health Insurance Portability and Accountability Act (HIPAA) and the privacy and security rules outline how individuals, including nurses, at covered entities should collect, use and handle protected health information" (Borten, 2017). This federal law and rules have prompted those covered healthcare agencies and services to develop and utilize policies and procedures to protect PHI. Nurses and other healthcare providers should follow these policies and procedures as they plan and implement patient education, sharing of information, and networking.

Social Media

American adults have increased their use of social media from 5% in 2005 to 69% in 2016 (Pew Research, 2017, January). One might assume that the information posted online is private because most sites require a personal login and password. Unfortunately, personal privacy settings on social media provide a false sense of security. Anything posted online on social media accounts has the potential to be viewed by the public. For example, posts shared with a friend may end up being viewed. As nurses, we have an ethical responsibility to self-regulate that which we post on social media accounts. These accounts have unlimited potential as a communications tool to help us educate our clients and share reliable healthcare information resources. However, caution should be the rule, whenever posting anything work related to social media or elsewhere on the internet.

Figure A



(US Department of Health and Human Services, n.d.)

The National Council of State Boards of Nursing (NCSBN) and the American Nurses Association (ANA) developed guidelines for upholding professional boundaries with regards to social media. The NCSBN provides several resources for download free of charge at https://www.ncsbn.org/3739.htm. These resources provide information to guide nurses in the use of social media. They provide tips for using social media appropriately while avoiding disclosure of confidential information. Although there are cases of intentional abuse and malicious intent with social media, most often the exposure of private and/or confidential information is unintentional. Nurses must remember that there is an opportunity for confusion between a patient's right to disclose personal information about themselves and the need for healthcare providers not to reveal or share client information without a care-related need for the disclosure.

The NCSBN has summarized the following list of common myths and misunderstandings of Social Media to heighten awareness of risk related to false beliefs (NCSBN, 2011).

MYTH: Communication or post is private and accessible only to the intended recipient.
FACT: The nurse may fail to recognize that content once posted or sent can be disseminated to others.

MYTH: Content deleted from a site is no longer accessible.
FACT: The moment something is posted, it lives on a server that can always be discoverable by others, including in a court of law.

MYTH: It is harmless if private information about patients is disclosed if the communication is accessed only by the intended recipient.
FACT: This is still a breach of confidentiality.

MYTH: It is acceptable to discuss or refer to patients if they are not identified by name, but referred to by a nickname, room number, diagnosis or condition.
FACT: This, too, is a breach of confidentiality and demonstrates disrespect for patient privacy.

Minimize Risk when using Social Networking

The American Nurses Association (ANA) has developed guidelines for using social media and a social networking principles toolkit (American Nurses Association, 2017). The ANA's principles for social networking are:

Nurses

- must not transmit or place online individually identifiable patient information;
- must observe ethically prescribed professional patient-nurse boundaries;
- should understand that patients, colleagues, institutions, and employers may view postings;
- should take advantage of privacy settings and seek to separate personal and professional information online;
- should bring content that could harm a patient's privacy, rights, or welfare to the attention of appropriate authorities; and,
- should participate in developing institutional policies governing online conduct.

(American Nurses Association, 2017)

Consequences for Nurses

Whether intentional or unintentional, the potential consequences for the nurse's inappropriate use of electronic social media and networking can be severe. The consequences are variable and dependent on the specific details of each incident or event. NCSBN (Spector, Kappel, 2012) reports that a Board of Nursing (BON) may investigate the nurse if a reported event or incident includes:

- Unprofessional conduct;
- Unethical conduct;
- Moral turpitude (a malicious way of behaving);
- Management of patient records;
- Revealing a privileged communication; and,
- Breach of confidentiality.

If the NCBON finds the allegations to be true, the nurse may receive disciplinary action. Disciplinary actions by the BON can range from a letter of concern, to a reprimand, or up to sanctions that result in loss of licensure privileges. Additionally, if employment policy and/or regulations are not followed, the employer may take disciplinary action or termination. In March 2012, the NCSBN conducted a survey of executive officers and of the 30 respondents, 63% reported that they had received complaints against nurses for inappropriate use of social media. Of the 63% who reported complaints, 64% reported that they had disciplined the nurses (Spector, Kappel, 2012). In addition to violation of the Nurse Practice Act for failing to maintain patient confidentiality and safety, the nurse who discloses confidential or personal health information may be subject to prosecution by state and/or federal law enforcement.

Illustrative Stories:

The following illustrative stories (based on actual cases) are intended to highlight risky situations that could be avoided.

Public Debriefing

A nurse takes a picture of a patient room and posts it on a popular social media site along with a detailed account of his workday experiences caring for a challenging patient. The hospital room includes soiled linens with the hospital logo clearly visible, several personal patient items, and papers with printed type on a bedside table. The nurse's account of the day is posted under the photo and includes the patient's diagnosis and prognosis along with descriptions of an incontinence event and subsequent bathing. The photo was noticed by a friend of the patient due to the personal items on the bedside table. They were able to enlarge the photo and identify the patient's name on the papers on the bedside table. A complaint was made to the healthcare agency regarding the breach of confidentiality and disclosure of personal health information. In addition, the comments regarding the incontinence event were considered humiliating and demeaning. The nurse was identified by the healthcare agency and terminated immediately. Further, the nurse's actions were reported to the Board of Nursing. After an investigation by the Board of Nursing, the Board found that the nurse had violated the confidentiality requirements of the Nursing Practice Act. The nurse received a disciplinary action that will be permanently noted on their nurse license records.

Photographic Disclosure

Two nurses working in an emergency room used their cell phones to take a picture of an x-ray from a patient with a foreign body lodged in the rectum. One of the nurses then posted the picture on her personal social media page with comments. An anonymous call reported the incident to hospital administration. The nurses admitted that they had indeed taken photos of the x-ray but denied that it was posted to social media. The nurses' employment was terminated by the hospital. The nurse accused of posting the photo removed her account from the internet site. Police were not able to acquire enough evidence to prove a violation of state law. However, the case has been referred to federal authority to investigate for federal law violations; specifically, HIPAA and patient rights violation (WISN-TV, ABC Milwaukee, 2009).

Intentional or unintentional breaches of patient confidentiality and private health information is a violation of Federal HIPAA regulations. If the information provides enough detail or could be used to identify an individual, HIPAA rule is violated. HIPAA rules outline how protected information should be collected, used, and provides detailed guidance regarding handling of any information that relates to past, present or future physical or mental health information (Thacker, 2003).

Conclusion

As technology evolves and expands, nurses and the public will need to remain diligent in accessing and using information retrieved and communicated via the internet. Educating patients about the reliability and use of healthcare information located on the internet will contribute to limiting opportunity for misinterpretation. It is essential that nurses follow policy and procedure when interacting with and contributing to personal health information records. Always remember, if you post images or comments in an online media site, they can be viewed by the public.

References

1. American Nurses Association. (2017). Socal Networking Principles Toolkit. Retrieved August 2017 , from ANA: http://nursingworld.org/FunctionalMenuCategories/AboutANA/Social-Media/Social-Networking-Principles-Toolkit
2. Borten, K. (2016, August). The Role of Nurses in HIPAA Compliance, Healthcare Security. Health IT Security Newsletter. Retrieved August 2017, from https://healthitsecurity.com/
3. Computer History Museum. (2017). Timeline of Computer History. Retrieved from Computer History: http://www.computerhistory.org/timeline/computers/
4. Merriam-Webster. (2017). Medical Dictionary. Retrieved from Merriam-Webster: https://www.merriam-webster.com/dictionary/informatics
5. National Council of State Boards of Nursing. (2011). A Nurse's Guide to the Use of Social Media. Retrieved August 2017, from NCSBN: https://www.ncsbn.org/3739.htm
6. National Council of State Boards of Nursing. (2011, December). A Nurse's Guide to Use of Social Media. Retrieved May 2017, from NCSBN: https://www.ncsbn.org/NCSBN_SocialMedia.pdf
7. NCSBN. (2011, November). A Nurse's Guide to the Use of Social Media. Retrieved August 2017 , from https://www.ncsbn.org/NCSBN_SocialMedia.pdf
8. Pew Research Center. (2017). Internet/Broadband Fact Sheet. Retrieved August 2017, from Pew Research Center Internet and Technology: http://www.pewinternet.org/fact-sheet/internet-broadband/
9. Pew Research Center. (2017, January). Social Media Fact Sheet. Retrieved August 2017, from Pew Research Center Internet and Technology: http://www.pewinternet.org/fact-sheet/social-media/
10. Spector, N., Kappel, D. (2012, September). Guidelines for Using Electronic and Social Media: The Regulatory Perspective. Retrieved August 2017, from The Online Journal of Issues in Nursing: http://www.nursingworld.org/MainMenuCategories/ANAMarketplace/ANAPeriodicals/OJIN/TableofContents/Vol-17-2012/No3-Sept-2012/Guidelines-for-Electronic-and-Social-Media.html
11. Thacker, S. (2003, April). HIPAA Privacy Rule and Public Health: Guidance from CDC and US Department of Health and Human Servies. Retrieved August 2017, from CDC MMWR Epidemiology Program Office: https://www.cdc.gov/mmwr/preview/mmwrhtml/m2e411a1.htm
12. The Advisory Board Company. (2017, January). Nursing is America's most trusted profession yet again, Gallup finds. Retrieved August 2017, from The Advisory Board Daily Briefing: https://www.advisory.com/daily-briefing/2017/01/03/nurse-trusted-profession
13. US Department of Health and Human Services. (n.d.). Reassessing Your Security Practices in a Health IT Environment. Retrieved August 2017, from US Department of Health and Human Services: https://www.hhs.gov/sites/default/files/small-practice-security-guide-1.pdf
14. Weaver, J. (2017, July). More people search for health online. Retrieved August 2017, from Telemedicine on NBC News: http://www.nbcnews.com/id/3077086/t/more-people-search-health-online#.Wbp35rpFxaQ
15. WISN-TV, ABC Milwaukee. (2009, February 26). Nurses Fired Over Cell Phone Photos of Patient. Retrieved September 2017, from http://www.wisn.com/article/nurses-fired-over-cell-phone-photos-of-patient/6291966

Additional Resources

16. American College of Healthcare Executives. (2016, November). Health Information Confidentiality. Retrieved 2017, from ACHE: https://www.ache.org/policy/hiconf.cfm
17. Barry, M. (2017, September). Social Media: Proceed with caution. (A. N. Association, Ed.) Retrieved September 2017, from The American Nurse: http://www.theamericannurse.org/2014/01/02/social-media-proceed-with-caution/
18. Health Information Technology. (2014, October). Health Information Privacy Law and Policy. Retrieved August 2017, from Patient Consent for eHIE: https://www.healthit.gov/providers-professionals/patient-consent-electronic-health-information-exchange/health-information-privacy-law-policy
19. Independence Hall Association. (2017). 60 d. Living in the Information Age. Retrieved 2017, from US History: Pre-Columbian to the New Millenium: http://www.ushistory.org/us/60d.asp
20. National Council of State Boards of Nursing Regulator Staff. (2015, January). The 2015 Regulatory Environment: Executive Summary. Journal of Nursing Regulation, 5(4), 39-48. doi:http://dx.doi.org/10.1016/S2155-8256(15)30039-9
21. North Carolina Office of Administrative Hearings. (2017, June). 21 NCAC 36.0217 Investigations; Disciplinary Hearings. Retrieved August 2017 , from NCAC Rules: http://reports.oah.state.nc.us/ncac/title%2021%20-%20occupational%20licensing%20boards%20and

%20commissions/chapter%2036%20-%20nursing/21%20ncac%2036%20.0217.pdf
22. Office for Civil Rights. (2013, July). HHS.gov: Summary of the HIPAA Security Rule. Retrieved August 2017, from Health Information Privacy: https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html
23. Tillman, C. (2013, Fall). Social Networking and Nurses, Archived Nursing Bulletins. Retrieved May 2017, from NC Board of Nursing: http://www.ncbon.com/dcp/i/news-resources-publications-archived-nursing-bulletins
24. US Department of Health and Human Services. (2013, July). Breach Notification Rule. Retrieved August 2017, from Health Information Privacy: https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html
25. US Department of Health and Human Services. (2017, June). HIPAA for Professionals. Retrieved 2017 August, from Health Information Privacy: https://www.hhs.gov/hipaa/for-professionals/index.html

EARN CE CREDIT

"But all I did was share a photo of my patient's wound with one friend—you couldn't even see his face! … What Nurses Need to Know about Informatics, Social Media, and Security!" (1.9 CHs)

Read the article and the Chapter 36 (consolidated) Administrative Code Rules which guide the work of the NCBON and reflect on the following situations for reflection. Chapter 36 (consolidated) is located at http://reports.oah.state.nc.us/ncac/title%2021%20-%20occupational%20licensing%20boards%20and%20commissions/chapter%2036%20-%20nursing/chapter%2036%20rules.html.

SITUATIONS FOR REFLECTION

1. The mother of a pediatric patient has asked the nurse to snap a photo and post it to the internet so that she can download it when she gets home. What is the best response or action for the nurse in this situation? If the nurse complies with the request, what are the potential consequences with regard to NC law and rules?
2. The nurse keeps an online personal journal/blog. After one especially rough shift, the nurse decides to debrief in the blog. As long as there is no mention of patient name or identification, is it ok to write about the challenges of the day that one experienced at work? If the information is posted to the internet, are there potential consequences with regard to NC law and rules?
3. A patient and nurse have developed a close relationship during a long recovery period. The patient asks the nurse to be a "friend" on a social media site. This would make it possible for them to talk when the nurse is not on duty and share photos. What is the best response or action for the nurse in this situation? What are the implications for the nurse should they choose to engage in an off-duty internet relationship?

There is not a test requirement, although reading for comprehension and self-assessment of knowledge is encouraged.

RECEIVE CONTACT HOUR CERTIFICATE

Go to www.ncbon.com and scroll over "Education;" under "Continuing Education" select "Board Sponsored Bulletin Offerings," scroll down to the link, "What Nurses Need to Know about Informatics, Social Media, and Security!"

Register, be sure to write down your confirmation number, complete and submit the evaluation, and print your certificate immediately.

If you experience issues with printing your CE certificate, please email practice@ncbon.com. In the email, please provide your full name and the name of the CE offering (What Nurses Need to Know about Informatics, Social Media, and Security!).

Registration deadline is 7-01-2018.

PROVIDER ACCREDITATION

The North Carolina Board of Nursing will award 1.9 contact hours for this continuing nursing education activity.

The North Carolina Board of Nursing is an approved provider of continuing nursing education by the North Carolina Nurses Association, an accredited approver by the American Nurses Credentialing Center's Commission on Accreditation.

NCBON CNE CONTACT HOUR ACTIVITY DISCLOSURE STATEMENT

The following disclosure applies to the NCBON continuing nursing education article entitled "What Nurses Need to Know about Informatics, Social Media, and Security!"

Participants must read the CE article and additional reading(s) listed (if applicable) in order to be awarded CNE contact hours. Verification of participation will be noted by online registration. No financial relationships or commercial support have been disclosed by planners or writers which would influence the planning of learning outcomes and content of the article. There is no endorsement of any product by NCNA or ANCC associated with the article. No article information relates to products governed by the Food and Drug Administration.