Learning outcome, instructions for completing the evaluation, and statements of disclosure can be found on page 61.

Data Breaches Are Not Just Information Technology Worries!

Donna M. De Simone

De Simone, D.M. (2019). Data breaches are not just information technology worries! *Pediatric Nursing, 45*(2), 59-62.

A data breach of protected health information can be a costly problem, not only for a healthcare corporation, but also for the healthcare provider, including the pediatric nurse. A data breach of protected patient information involves the Health Insurance Portability and Accountability Act (HIPAA), which is not just the once-a-year online educational activity. HIPAA's most serious breach ramifications are huge and not frequently stressed. A HIPAA breach can incur monetary penalties, loss of a nursing license, employment termination, prison time, and now, the exposure of a new cause of action – a lawsuit.

Key Words: Data breach, protected health information, Health Insurance Portability and Accountability Act (HIPAA).

Data breaches are problematic. One needs to look no further than the nightly news about the explosion of "Big Data" breaches with healthcare companies becoming prime targets. Over the last few years, the number of monetary violations imposed over those data breaches has markedly increased, with many breaches of a patient's protected health information (PHI) being made by a healthcare professional (U.S. Department of Health and Human Service [DHHS] Office for Civil Rights, 2018). This has implications for all nurses, especially pediatric nurses, because pediatric nurses tend to have greater familiarity with the family of the patient than nurses who provide health care for adults. This familiarity then becomes a social familiarity, which can result in a greater ease of becoming social media friends with patients and/or their family.

What seems to be so innocent can have dire consequences for the pediatric nurse. An innocent posting on any social media site can reveal a child's PHI. This release of a patient's personal data or PHI not only has ramifications and implications for the nurse's employer, but also individual ramifications for the nurse. The release of unauthorized information is a breach. A data breach of patient information involves the Health Insurance Portability and Accountability Act of 1996, commonly known as HIPAA. HIPAA and its costly breach ramifications are huge and not frequently stressed in most educational activities. A breach can occur just by means of communication, including a social media posting. Most nurses not only communicate by email but also have social media accounts, such as Facebook, Twitter, and Instagram; however, few nurses know that a breach of a patient's PHI can cost nurses their license and employment, and expose them to future litigation.

Donna M. De Simone, JD, MS, APRN-CNP, APRN-CNS, FNP-C, CPN, *is an Attorney, De Simone Law, PLLC, Tulsa, OK.*

A Brief Review of HIPAA

HIPAA provides federal protection for patient health information and gives patients an array of rights with respect to that information (HIPAA Pub. L. 104-191, 110 Stat. 1936, 1996). Most nurses are familiar with some components of HIPAA, such as the Privacy Rule, which addresses the privacy of "individually identifiable health information;" the Security Rule, which sets national standards for the security of electronic protected health information (ePHI); and the Breach Notification Rule, which provides notification process following a breach of unsecured PHI. Implications and violations of the Privacy Rule will be discussed in this article.

First, an important part of understanding of any legal rule or regulation is to be familiar with the definitions set forth in that regulation. The most important part of the Privacy Rule is the definition of what is protected.

What exactly is PHI? Pursuant to HIPAA regulations (45 CFR § 160.103), PHI is defined as individually identifiable health information that is transmitted or maintained in electronic media or transmitted or maintained in any other form or medium (45 CFR § 160.103). Individually identifiable health information is defined as "Information that is collected from an individual…that relates to the past, present, or future physical *or* mental health or condition of an individual… that identifies the individual or with respect to which there is a reasonable basis to believe that information can be used to identify the individual" (45 C.F.R. §160.103).

This definition of PHI is why displaying a photo of a patient can be deemed a HIPAA breach.

What constitutes a breach? A breach is "the acquisition, access, use or disclosure of PHI in a manner that is not permitted…which compromises the security or privacy of the PHI" (45

CFR § 164.402). Unpermitted use is a breach. Unauthorized use is a breach. Access to PHI is a breach if it is unauthorized. Thus, reviewing the medical record of a patient you are not caring for in the hospital is a HIPAA breach; in most electronic medical records systems, it is blocked and the user is unable to access.

HIPAA Breaches

As mentioned above, the consequences of a HIPAA breach can result in monetary penalties, such as a fine, but penalties may also include prison time, loss of a nursing license, and exposure of litigation. Monetary consequences of a HIPAA violation can be steep. A HIPAA violation due to willful neglect and not corrected within a specified time amounts to $50,000 per violation, with an annual maximum of $1.5 million (45 CFR § 164.404; 42 USC § 1320d-5). These figures are staggering and would be overwhelming for any healthcare professional.

Additionally, a HIPAA breach can have criminal penalties. The U.S. Department of Justice (2005) explained who can be criminally liable under HIPAA:

> Covered entities and specified individuals, whom "knowingly" obtain or disclose individually identifiable health information in violation of the Administrative Simplification Regulations, face a fine of up to $50,000, as well as imprisonment up to (1) one year. Offenses committed under false pretenses allow penalties to be increased to a $100,000 fine, with up to (5) five years in prison. Finally, offenses committed with the intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain or malicious harm permit fines of $250,000 or imprisonment for up to ten (10) years, or both (42 USC § 1320d-6).

As if the monetary and criminal consequences of a HIPAA violation were not steep enough, there are additional penalties that seem to be neglected or missed in most educational yearly discussions. When a breach occurs, and a penalty is imposed, there is a "Notice to the Public" provision in the HIPAA regulation (45 CFR 160.426), which is, in essence, a notice to the world, including the healthcare provider's current or future employer. Further, if the employee is an "at will employee" (the status of most nurses, where the nurse is essentially working at the pleasure of his or her employer without a contract), the nurse can be terminated for any reason. If the nurse has been involved in a HIPAA breach, the employer may terminate the nurse, and the potential future employer may know the nurse has been involved in a breach because breaches greater than 500 individuals are publicly available on the U.S. DHHS Office of Civil Rights (2018) Breach Portal.

If a nurse is responsible for the HIPAA breach, the "Notice to the Public" includes a provision that the Secretary of the U.S. DHHS may notify the State Board of Nursing of the nurse involved in the breach. According to most state statutes, state Boards of Nursing can take disciplinary action against any violation of the Nurse Practice Act. The language used to describe types of actions available to Boards of Nursing varies according to state law. Although terminology may differ, Board action affects the nurse's licensure status and ability to practice nursing in the state taking the action. Board actions may include the following:

- Fine or civil penalty.
- Public reprimand or censure for minor violation of the Nurse Practice Act, often with no restrictions on license.
- Imposition of requirements for monitoring, remediation, education, or other provision tailored to the particular situation.
- Limitation or restriction of one or more aspects of practice (e.g., probation with certain restrictions, limiting role, setting, activities, hours worked).
- Separation from practice for a period of time (suspension) or loss of license (revocation or voluntary surrender).
- Other state-specific remedies (National Council of State Boards of Nursing [NCSBN], 2018).

The NCSBN (2011) survey from all state Boards of Nursing revealed that 72% of Boards of Nursing received complaints of nurses violating patient privacy that resulted in a reprimand, sanction, fine, and/or loss of license. This can easily happen to any pediatric nurse. For example, when a nurse posts photos or information about patients on social networking sites, such as Twitter and Facebook. Fund-raising sites (such as Go Fund Me) can be especially risky professional behavior. Nurses' postings are often seen on Facebook when pediatric nurses "friend" a child or the child's family, and then discuss the child's condition or treatment, or describes the activities of the healthcare day.

According to the NCSBN (2011), with regard to violation of a patient's privacy, the Boards of Nursing took disciplinary action based on complaints in 79% of those cases. The action taken ranged from a letter of concern to conditions on license, and in some cases, suspension of license related to the state's Nurse Practice Act under "unprofessional conduct," "unethical conduct," "moral turpitude," "mismanagement of patient records," "revealing a privileged communication," and "breach of confidentiality."

These findings implicate the important need to take time to review the Nurse Practice Act for the state of employment; most are available online. Patient privacy and trust are paramount to good patient care. A breach can not only erode that trust, but it can also compromise the nurse's career (NCSBN, 2011). Recently, a New York nurse practitioner's license was suspended after she took, without permission, personally identifiable information of about 3,000 patients from her former employer to her new employer with the intention of ensuring continuity of care (Spitzer, 2018). Additionally, her former employer was fined because the HIPAA breach of the release of information to the new employer was without the patient's permission. This incident most certainly can compromise future employment.

Professional Position Statements on Privacy

Most professional nurses' associations have privacy guidelines or position statements and knowledge of those statements is a worthwhile endeavor. For instance, the American Nurses Association (ANA) (2011) advises the following in its Principles for Social Networking:

- Nurses must not transmit or place online individually identifiable patient information.
- Nurses must observe ethically prescribed professional patient-nurse boundaries.

Instructions For Continuing Nursing Education Contact Hours

Data Breaches Are Not Just Information Technology Worries!

Deadline for Submission: **April 30, 2021** **PED 1902**

To Obtain CNE Contact Hours

1. To obtain CNE contact hours, you must read the article and complete the evaluation through the ***Pediatric Nursing*** **website** at **www.pediatricnursing.net/ce**
2. Evaluations must be completed **online** by April 30, 2021. Upon completion of the evaluation, your CNE certificate for **1.3** contact hour(s) will be mailed to you.

Learning Outcome

After completing this learning activity, the learner will be able to define a data breach of protected health information and explain the consequences of violating standards of care established by the Health Insurance Portability and Accountability Act (HIPAA).

Learning Engagement Activity

1. This article states that pediatric nurses tend to have greater familiarity with the family of the patient than nurses who provide health care for adults. This familiarity then becomes a social familiarity that can result in a great ease of becoming social media friends with patients and/or their family. See pages 60-61 for examples of privacy violations via social media.
2. To view reported breaches in the last 24 months, visit:
   U.S. Department of Health & Human Services Office for Civil Rights. (2018). *Breach portal.* Retrieved from https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

Fees — *Subscriber:* FREE *Regular:* $20

The author(s), editor, editorial board, content reviewers, and education director reported no actual or potential conflict of interest in relation to this continuing nursing education article.

This educational activity is provided by Anthony J. Jannetti, Inc.

Anthony J. Jannetti, Inc. is accredited as a provider of continuing nursing education by the American Nurses Credentialing Center's Commission on Accreditation.

Anthony J. Jannetti, Inc. is a provider approved by the California Board of Registered Nursing, provider number CEP 5387. Licensees in the state of California must retain this certificate for four years after the CNE activity is completed.

This article was reviewed and formatted for CNE contact hours by Michele Boyd, MSN, RN-BC, Anthony J. Jannetti, Inc. Education Director.

- Nurses should understand that patients, colleagues, organizations, and employers may view postings.
- Nurses should take advantage of privacy settings and seek to separate personal and professional information online.
- Nurses should bring content that could harm a patient's privacy, rights, or welfare to the attention of appropriate authorities.
- Nurses should participate in developing organizational policies governing online conduct. (pp. 6-7).

New Cause of Action, New Type of Lawsuit

Lastly, and perhaps more worrisome, is the new cause of action that has arisen in the last few years, a new tort in negligence, which means a new type of lawsuit. Medical malpractice is essentially a tort of negligence with the required elements of duty, breach, causation, and damages that must be satisfied. In a negligence case, such as a medical negligence or medical malpractice case, the duty element is usually satisfied with the standard of care or national guidelines. Once that duty, or standard of care, has been breached, there must be a causal connection with the damages claimed.

Recently, in a number of court cases, HIPAA regulations have been held to be the standard of care for patient privacy. In *Acosta v. Byrum* (2006), the plaintiff, Heather Acosta, sued under the privacy and security provisions of HIPAA to establish the standard of care owed by her physician, with regard to her medical records. The North Carolina Court of Appeals adopted HIPAA as the standard of care healthcare professionals must meet to avoid a claim of negligence in failing to prevent the unauthorized disclosure of patient treatment information. Likewise, in *Hinchy v. Walgreen* (2015), the Indiana Court of Appeals upheld a $1.4 million jury verdict holding Walgreen Co., the owner of Walgreen's pharmacies ("Walgreen's"), liable after one of the company's pharmacists shared a customer's confidential medical record in violation of HIPAA. The Walgreen's lawsuit was one of the first cases resulting in a substantial jury verdict in which a plaintiff relied on HIPAA to establish the standard of care to prove a healthcare provider's negligence.

Finally, in *Byrne v. Avery Center for Obstetrics & Gynecology* (2018), the Connecticut Supreme Court unilaterally created a new state law cause of action for violation of a patient's healthcare privacy, which is lack of compliance with HIPAA. In other words, a healthcare provider's violation of HIPAA can lead to a state law claim in Connecticut. That court held that "a duty of confidentiality" arises from the physician-patient relationship, and unauthorized disclosure of confidential information obtained in the course of that relationship for the purpose of treatment gives rise to a cause of action sounding in tort against the healthcare provider, unless the disclosure is otherwise allowed by law.

The reason these cases are so important is that current HIPAA regulations do not allow individual patients to sue when healthcare providers violate it, which means HIPAA does not provide a private right of action, leaving enforcement up to federal and state governments. However, with the Acosta, Hinchy, and Byrne cases, and others to follow, HIPAA can be used by plaintiff attorneys and patients to establish the standard of care in con-

nection with negligence and other tort claims. This creates a new type of lawsuit. Additionally, the cost of defense of a HIPPA lawsuit may not be covered under most medical malpractice insurance policies.

Conclusion

In summary, a breach of patients' PHI can result in violations of privacy under 42 USC § 1320d-5; civil penalties of $100 to $50,000 imposed by U.S. Office of Civil Rights; criminal penalties, such as prison time imposed by the U.S. Department of Justice; employment penalties, such as termination; loss of professional licensure; and now, a new cause of action in a lawsuit.

Patient privacy and trust is paramount to good patient care. A HIPAA breach can erode that trust and can compromise the nurse's career and erode one's bank account.

References

42 USC § 1320d-6. (2009). Retrieved from https://www.gpo.gov/fdsys/granule/USCODE-2008-title42/USCODE-2008-title42-chap7-subchapXI-partC-sec1320d-6

42 USC § 1320d-5. (2010). Retrieved from https://www.govinfo.gov/app/details/USCODE-2010-title42/USCODE-2010-title42-chap7-subchapXI-partC-sec1320d-5

45 CFR § 160.103. (2013). Retrieved from https://www.gpo.gov/fdsys/pkg/CFR-2007-title45-vol1/pdf/CFR-2007-title45-vol1-sec160-103.pdf

45 CFR § 164.402. (2013). Retrieved from https://www.gpo.gov/fdsys/granule/CFR-2011-title45-vol1/CFR-2011-title45-vol1-sec164-402

45 CFR §160.426. (2013). Retrieved from https://www.govinfo.gov/app/details/CFR-2018-title45-vol1/CFR-2018-title45-vol1-sec160-426

45 CFR § 164.404. (2013). Retrieved from https://www.gpo.gov/fdsys/granule/CFR-2011-title45-vol1/CFR-2011-title45-vol1-sec164-404

Acosta v. Byrum, 638 S.E. 2d 246 (N.C. Ct. App. (2006).

American Nurses Association (ANA). (2011). *ANA's principles for social networking and the nurse*. Retrieved from https://www.nursingworld.org/~4af4f2/globalassets/docs/ana/ethics/social-networking.pdf_

Byrne v. Avery Center for Obstetrics & Gynecology, 327 Conn. 540. (2018).

Health Insurance Portability and Accountability Act of 1996. HIPAA Pub. L. 104-191, 110 Stat. 1936. (1996). Retrieved from https://www.gpo.gov/fdsys/pkg/PLAW-104publ191/pdf/PLAW-104publ191.pdf

Hinchy v. Walgreen, 25 N.E.3d 748 (2015).

National Council of State Boards of Nursing (NCSBN). (2011). *White paper: A nurse's guide to the use of social media.* Retrieved from https://www.ncsbn.org/3874.htm

National Council of State Boards of Nursing (NCSBN). (2018). *Board action.* Retrieved from https://www.ncsbn.org/673.htm

Spitzer, J. (2018). *New York suspends former U of Rochester Medical Center nurse for sharing patient data with new employer.* Retrieved from https://www.beckershospitalreview.com/cybersecurity/new-york-suspends-former-u-of-rochester-medical-center-nurse-for-sharing-patient-data-with-new-employer.html

U.S. Department of Health & Human Services Office for Civil Rights. (2018). *Breach portal.* Retrieved from https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

U.S. Department of Justice. (2005). *Scope of criminal enforcement under 42 U.S.C. § 1320d-6.* Retrieved from https://www.justice.gov/sites/default/files/olc/opinions/attachments/2014/11/17/hipaa_final.htm