Ethics in Nursing Practice- Case Study Paper

Name

Institution

Ethics in Nursing Practice- Case Study Paper

The role of technology in the healthcare industry has expanded exponentially in the past few years. The ability to store, exchange, and analyze health data is directly connected to improved technology integrated into most facilities (McGonigle & Mastrian, 2018). Most adult patients are computer literate, and they are advantaged to seek healthcare knowledge. As such, nurses must be alert on available resources to alleviate patent literacy but must do so with caution. The purpose of this paper is to analyze two case studies and respond to the questions.

Similarity and Differences of cases

Both cases are similar in that they involve a breach of confidentiality, and they address issues regarding the use of technology in the healthcare context. Also, patients involved in these cases are not available. In other words, an information breach affects patients who are not immediate to the scene. In the first case, Matts S, a nurse in the coronary care unit, attends to an alarm, leaving data of another patient who is not described in the case. In the second case, Jill P allows her daughter to use the computer, and the information of a patient is breached.

The two cases are different in that; the first scenario was due to an emergency issue. Matt S. hears an alarm about cardiac arrhythmia and rushes to check the patient. The caregiver is not aware of Mr. Joe, a cleaner who is in the hallway. In the first case, the use of computers and information about a patient was accessed without the knowledge of Matt S. As such, the healthcare provider did not consent to the use of healthcare equipment. However, in the second case, the nurse jill consented to her daughter and allowed her to use a workplace computer to complete school homework. She gave permission deliberately without being aware that the daughter might access a confidential patient record.

Ethical Principle to the Cases

The ethical principles that apply to each case are veracity and fidelity. Veracity is defined as being true and remaining honest to patients (Heiskell, 2010). The principle relates to that of autonomy, and it is the basis of establishing a relationship with trust between patients and health service providers. Autonomy is an underlying value of confidentiality, and even though it is not intrinsic, it is instrumental (Heiskell, 2010). Veracity binds patients and professionals as they establish treatment goals. Patients are expected to be truthful about providing their personal information while caregivers must remain honest about clinical practices, including diagnoses, treatment options, and patient data maintenance. In the first case, Matt S. logged on to the computer to update patients' medical history before leaving in a rush and left the system open for access by an authorized individual. In that way, he violated the trust that the patient had established. The same happens in the second case where Jill P is trusted by a patient student with personal data but lets her daughter access the computer with private data.

Additionally, the principle of fidelity applies in two cases. Fidelity is an obligation to remain faithful to commitments (Heiskell, 2010). A professional code of standards requires caregivers to be authentic and commit delivering safe care to promote welfare. On the contrary, the two cases do not present an act of committed patient safety in terms of the psychological harm that patients may experience once they learn about the breach of personal information.

The autonomy principle is applicable in the two scenarios, where patients have the right to decide what to do with their medical information. Mr. Joe accesses a piece of data belonging to the patient who is his neighbor. The patient has the right to decide whether to notify anyone about the health conditions and decided to keep is personal. Mr. Sneaks to a computer and accesses information which he shares with other people, but the blame is to the care provider for

negligence. Both case scenarios involve using medical records that were accessed and viewed by unauthorized personnel, leading to a compromise in ethical confidentiality. Tied to privacy, confidentiality is when patient medical history should be kept private unless the owner agrees or consent for sharing. In the two cases, patients were not aware of the breach. Instead, they trusted that information in good hands of healthcare professionals, hence, confided with professionals who betrayed trust.

Aspects of the Code of Ethics

The nurses' professional code of ethics applies to these cases and specifically, provision three. The code's provision requires to promote, advocate, and protect patients' rights, health, and safety ("American Nurses Association," 2015). Regarding the two cases, protecting patient's information and maintaining a level of confidentiality is essential for using technology in clinical settings. Another person's health data should not be accessed or shared with a third party without the information owner's consent. The code of ethics affects both cases where nurses were responsible for promoting, advocating, and protecting patients' health data ("Health Education & Training," 2010). Another aspect of the code is ensuring the safety and health of patients.

In the first case scenario, Matt S forgot to log out of the healthcare system and left patients' information open for unauthorized people to sneak into. As such, it implies that the patients' rights to confidentiality were not protected. Provision three of the nurses' code of ethics requires professionals to protect people's rights, and in these cases, patients' rights are maintenance of privacy to their healthcare data ("U.S. Department of Health & Human Services," 2020). In the second case, nurse Jill permitted her daughter to use the professional system, again allowing unauthorized persons to sneak into patient details. The nurse did not protect patients' rights to privacy and safety. The patient in the second case whose information

was accessed might end up suffering psychological conditions like trauma or depression after other students learn that her health information is widely known at school.

Institution Accountability

In the first case, the employing institution, the Coronary Care Unit, facility is accountable for a breach of patient private information to an unauthorized person. The institution can be held responsible for not placing strict policies that govern the protection of patient records. In the second case, the employing institution is a suburban school district. Again, this organization can be held accountable for the information breach and lack of effective policies to guide data management professionals. Nurse Jill allows her daughter to use a computer, pointing a laxity in regulation measures, which leads to unauthorized data access. Employing institutions and care providers are liable for penalties according to civil rights regulations. The penalty could be up to $250,000 if the act were done knowingly or purposely to share confidential information. For the first time offenders, the penalty usually is lower than that, and if the situation occurred due to negligence. In both cases, care professionals can be considered negligent in adhering to the right protocols and failure to observe professional standards. In the first case, it was not the will of Matt S to have patient information accessed, but the person neglected a fact that a computer system needs to be logged off when in use. In the second case, while Jill P did not allow access to patient information by her daughter, she willingly let the student use professionals' system.

Disciplinary Actions

Disciplinary actions should be taken in both cases. Where the breach of information is determined as inadvertent, member of the care team is subjected to disciplinary actions like verbal warnings for the first violation, written notice for the second violation, and termination of

employment when an offense is committed the third time. Corrective actions in these two cases are required because it occurred due to negligence, and patients are affected.

HIPAA Violations

There was a violation of HIPAA regulations regarding the cases, which require patients to be protected from inappropriate disclosure of personal health information (PHI). PHI is individual and identifiable health data created by an organization, including demographic details that identify a person. Typically, there are a number of ways that HIPAA regulation can be violated, but the most common is the access of PHI by unauthorized personnel. In both cases, patient's information was accessed by third parties, who are unauthorized persons. In the two cases, HIPAA was a violation because patients did not consent to information access. Penalties for HIPAA violation can be severe where a state's attorney general may issue a fine up to a maximum of $25,000 as per violation category ("Overview of HIPAA," 2012). Potential penalties and criminal penalties for people who violate HIPAA rules might be appropriate as well. For example, the jail term is possible, with some violations which can lead to being jailed for two years.

In conclusion, this paper has looked at ethical issues in healthcare by analyzing two cases. The use of technology is vital to increase providers' capabilities and patient healthcare services, but it comes with significant responsibilities. When professionals like nurses are empowered to integrate technology in enhancing patient care, they should abide by HIPAA rules and professional standards.

References

American Nurses Association. (2016). *Code of Ethics for Nurses, Provision 3*. Retrieved 23 September 2020, from https://anacalif.memberclicks.net/assets/Events/RNDay/2016%20code%20of%20ethics%20for%20nurses%20-%209%20provisions.pdf.

Health Education & Training. (2010). *Ethical Issues in Nursing: Introduction: Concepts, Values, and Decision Making*. YouTube. Retrieved 23 September 2020, from https://www.youtube.com/watch?v=9VRPMJUyE7Y.

Heiskell, H. (Feb, 2010) Ethical decision-making for the utilization of technology-based patient/family education. Online Journal of Nursing Informatics (OJNI), 14 (1) Retrieved from http: ojni.org/14 1/hHeiskell.pdf.

McGonigle & Mastrian, K., (2018). Nursing Informatics and The Foundation of Knowledge: *Chapters 5 and 8*. 4th ed. Burlington, MA: Jones and Barlet Learning, pp.77-166.

Overview of HIPAA. (2012). *HIPAA*. YouTube. Retrieved 23 September 2020, from https://www.youtube.com/watch?v=d2Cw0ARJVDM.

U.S. Department of Health & Human Services. (2020). *Health Information Privacy*. HHS.gov. Retrieved 23 September 2020, from https://www.hhs.gov/hipaa/index.html.