Educating Employees on Risk

Jagbir Kaur

Grand Canyon University

04-3-2020

Educating Employees on Risk

**Introduction**

The health sector is faced with numerous risk issues with patient injury while receiving treatment being one of the most avoidable risks. Many patient falls and injuries in hospitals result from adverse drug effects, surgical complications, and patient falls. Healthcare organizations have patient safety as the topmost priority in the delivery of care. As such, there is a need to have an adequate plan for ensuring patient safety while providing care.

**Rationale**

According to the World Health Organization (2014), the United States has a high rate of patient injuries that take place in hospital stays. About one in ten patients around the world are injured while receiving treatment. Medical errors are also a leading cause of injuries to patients. According to Cagliano et al (2011), the highest percentage of injuries recorded by patients occur within the healthcare setting. The states require the adoption of safety culture as a mechanism of improving patient safety (Weinberg et al., 2005). As such, through patient education, the organization is enabling a safety-focused culture for dealing with patients.

**Support**

Much of the responsibility of maintaining patient safety lies with employees. As such, there is a need to equip employees with the attitude, skills, and knowledge to deal with potential cyber threats. The National Quality Forum is a non-profit organization that develops nation-wide strategies for dealing with patient safety (Lee & Namburi, 2019). One of the appropriate ways for improving patient safety is through education and training of employees to ensure that they are aware of the necessary safety procedures.

**Implementation**

The strategy that will be utilized is a targeted training program. For optimum effectiveness, there is a need to begin by the identification of the competencies that users require to complete their tasks. Through this step, there is the possibility of identifying the know-how gaps and the strategies for closing the gaps (Beyer & Brummel, 2015). Additionally, attitude and behavior change required can easily be identified. The training is further aligned with the policies and strategies for the organization in the long-term. This will allow for the end-user strengths and developmental needs to enhancing patient safety be aligned to the mission and vision of the organization.

**Challenges**

Some of the challenges that may be faced include resistance to change. This is a challenge that can be handled by prior education on the program and the benefit of the program to the employees and organization. Another challenge is engaging the employees actively in the learning process. There is a need to have innovative and interactive strategies for the education and teaching sessions which include analogies and demonstrations. Also, there is a need to create flexibility in training programs to allow for online programs (Andriotis, 2018). This can favor hectic employee schedules that creating more engagement. Finally, conflict may arise among various departments during the implementation due to the interdisciplinary nature of the education drive. There is a need to have adequate conflict management strategies that allow for open communication.

**Evaluation**

There is a need to find out the extent to which the learning process inspired users to change. As such, the number and type of security breaches will be monitored and compared to previous stages. Employee feedback is another tool where the employee will answer a questionnaire before and after the education to determine their understanding. Finally, the attendance of the employees and consistency throughout the education drive will indicate the efficiency of the implementation.

**Opportunities**

The education drive looks at maintaining the integrity of the organization's patient safety systems by focusing on the human aspect. There is a need to look at other ways that patient safety can be put at risk such as through data breaches which may occur such as through improper disposal of old hardware. The hardware still contains valuable data that can be retrieved. As such, there is a need to develop appropriate strategies for ensuring old hardware – hard-drives and computers – are safely disposed of by considering the environmental needs and the safety needs of the organization's data.

References

Andriotis, N. (2018). *Training and Development Challenges and Solutions in the Workplace*. Retrieved from <https://www.talentlms.com/blog/training-challenges-solutions-workplace/>

Beyer, R. E., Brummel, B. J. (2015). *Implementing Effective Cyber Security Training for End Users of Computer Networks*. Society for Human Resource Management and Society for Industrial and Organizational Psychology. Retrieved from https://www.shrm.org/hr-today/trends-and-forecasting/special-reports-and-expert-views/Documents/SHRM-SIOP%20Role%20of%20Human%20Resources%20in%20Cyber%20Security.pdf

Cagliano, A. C., Grimaldi, S., & Rafele, C. (2011). A systemic methodology for risk management in the healthcare sector. *Safety Science, 49*(5), 695-708

Lee, L., Namburi, N. (2019). *National Quality Forum (NQF).* Retrieved from https://www.ncbi.nlm.nih.gov/books/NBK549854/

Weinberg, J., Hilborne, L. H., Nguyen, Q-T. (2005). *Regulation of Health Policy: Patient Safety and the States*. Retrieved from https://www.ncbi.nlm.nih.gov/books/NBK20479/

World Health Organization (WHO). (2014). *10 facts on patient safety*. Retrieved from https://www.who.int/features/factfiles/patient\_safety/en/