Protecting Your Privacy

(NAPSA)—Some people are taking an unhealthy interest in your medical information—but they can be stopped.

The Problem

With data breaches occurring across many industries, even sensitive data pertaining to patient health care records is at risk. A recent University of Phoenix study of 504 registered nurses and administrative staff found that only a quarter of registered nurses have seen changes in the way their companies handle data security and patient privacy over the past year despite increased data breaches across all industries. The survey also found that 20 percent of registered nurses and 19 percent of administrative staff admitted their facilities have experienced a breach of private patient data.

Furthermore, the Identity Theft Resource Center notes that, as of November 2017, there had been nearly 5 million data breaches in the health care industry. These breaches can be detrimental to organizations: According to IBM's 2017 Cost of Data Breach Study, health care is the most costly industry for data breaches, with the average cost per affected record at $380.

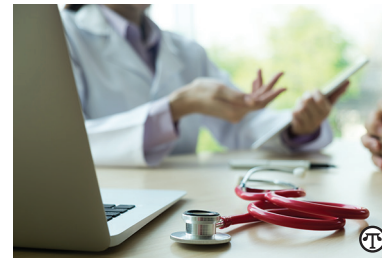
The issue is further compounded by a lack of trained cybersecurity professionals to combat hackers, especially in health care, where professionals make less and are responsible for not only protecting systems, but lives. Without trained experts, the onus falls on RNs and administrators, who may be unaware of how to identify or prevent breaches.

Expert Advice

"Patient safety transcends physical, emotional and electronic bounds and, in our increasingly digital world, it is important for health care professionals to be prepared for the possibility of data breaches," said Doris Savron, executive dean for the College of Health Professions, College of Education and College of Humanities & Sciences at University of Phoenix. "Everyone in the health care industry must work together to establish protocols and implement training to secure and protect all patient data to reduce the risk of being compromised."

Nurses and administrative staff agree, with 23 percent of RNs and 34 percent of administrative staff stating that additional support and training is needed for health care privacy and security.

"Health care organizations are extremely susceptible to human error. If one employee accidentally invites malicious malware into a system, the impact can be catastrophic. To limit the amount of breaches, cybersecurity governance must improve," said Dennis Bonilla, executive dean for the College of Information Systems and Technology at University of Phoenix. "Without improved training and robust cybersecurity response plans incorporated into information technology strategies, the health care industry will continue to bear the brunt of these attacks."



Health care facilities these days take several steps to ensure patient privacy—and you can learn how to help.

What's Being Done

Current steps being taken to ensure the protection of patient data include:

- Updated privacy and access policies, according to more than two-thirds of RNs and administrative staff;
- Role-based access, according to 59 percent of RNs and 60 percent of administrative staff; and
- Data surveillance, according to most RNs and administrative staff.

"Understanding what we do well now to protect patient data can help us create an increasingly sophisticated framework to safeguard this sensitive information," added Savron. "University of Phoenix offers degree and certificate programs that help prepare health care professionals to provide the best possible care to their patients while taking steps to protect their personal information." The school helps working adults move efficiently from education to careers in a rapidly changing world.

Learn More

For information about programs offered through the College of Health Professions and College of Information Systems and Technology, visit phoenix.edu. For full survey information and an infographic, visit www.phoenix.edu/about_us/media-center/news/uopx-survey-finds-one-in-five-healthcare-professionals-have-experienced-patient-data-breaches.html.