A majority of medical professionals improperly share log-in credentials to EMRs

September 26 2017

Strict regulations for keeping confidential data secure often make it difficult for caregivers to get the information they need. As a result, a majority of medical staff surveyed have accessed an electronic medical record (EMR) system using a password improperly supplied by a fellow medical staffer.

Published in *Healthcare Informatics Research*, the "Prevalence of Sharing Access Credentials in Electronic Medical Records" is the first study to examine EMR access among medical providers. EMRs store extensive, highly sensitive information about patients, including personal, demographic and financial data. Healthcare organizations also use EMRs for billing, appointment-scheduling and managing critical life-supporting devices.

In the study, researchers gathered survey responses from 299 medical professionals, including residents, medical students, interns, and nurses. The research team included researchers from Ben-Gurion University of the Negev (BGU), Harvard Medical School, Duke University, Hadassah-Hebrew University Medical Center, and the Interdisciplinary Center in Herzliya, Israel.

Nearly three-quarters (73 percent) of the 299 participants claimed to have used another medical staff member's password to access an EMR at work. More than 57 percent of participants (171 out of 299) estimated they have used someone else's password an average of 4.75 times.

Of the medical residents, all (100 percent) say they had at one time obtained another medical staff member's password with their consent. Within the student and intern groups, 77 percent and 83 percent (respectively) used someone else's access credentials because they said they "were not given a user account."

Similarly, 56 percent of students and almost 70 percent of interns cited that their user access had inadequate permissions " to fulfill my duties" so they had to ask for someone else's access credentials. Only half of the nurses surveyed (57.5 percent) reported using someone else's password.

"The strength of an information security system is determined by the strength of its weakest link," says researcher Dr. Florina Uzefovsky, an associate professor of developmental psychology at BGU and member of its Zlotowski Center for Neuroscience. "Even a single breach may render an information system ineffective."

Breaching patient privacy—which is protected under the strict Health Insurance Portability and Accountability Act (HIPAA) rules in the United States and International Standards Organization (ISO) criteria in Israel and other countries—can result in large fines if reported. In addition, an EMR system attack could seriously disrupt healthcare operations and cause direct injury to patients, such as with the manipulation of a prescription or medical device.

Consequently, HIPAA requires healthcare organizations to establish and enforce comprehensive security policies, which include clear definitions of each worker's role and access privileges. Organizations must also supply a way to authenticate the identity of each worker, control his or her access to relevant data and audit editing.

"Medical staff must provide timely and efficient care while maintaining patient confidentiality," says the primary investigator, Dr. Ayal

Hassidim, at Hadassah-Hebrew University Medical Center. "This may sometimes cause conflict between their duty and their obligation to meet security regulations."

The researchers offer a number of recommendations. First, attaining access credentials needs to be less difficult and time-consuming. For example, in Israel—where junior staff turnover clinical rotations weekly—medical school students, interns, and other new employees often resort to using another employee's credentials to fulfill their duties while going through the strict, lengthy registration process.

The researchers recommend that understaffed hospitals, especially during on-call hours, may need to delegate administrative tasks and extend EMR system access to para-medical, junior staff, interns, and students. Nurses, who generally carry out more precisely defined duties, are more likely to have the EMR privileges they need. An understanding of the requirements of the medical staff and extending broader access privileges can actually lead to less password sharing and better medical data protection.

Lastly, the researchers recommend adding an option for each EMR role that grants maximum privileges for one-time use only. When this option is invoked, the senior physician and a protected health information (PHI) security officer would be informed. This would allow junior staff to make urgent, lifesaving decisions under formal retrospective supervision without having to sneak onto the EMR.

Provided by American Associates, Ben-Gurion University of the Negev