Maintaining Data Integrity

CPT Jeffry Thomas Negard

Uniformed Services University of the Health Sciences

Maintaining Data Integrity

In 2013, the American Health Information Management Association (AHIMA) released the practice brief "Integrity of the Healthcare record: Best Practices for EHR documentation". Due to the numerous features electronic documentation tools offer, the sheer number and complexity may create integrity concerns and misuse, both accidental and intentional. To combat these issues, the AHIMA sought to provide its suggestions for how to maintain integrity, quality, and the utility of clinical documentation (Arrowood et al., 2013). The steps taken to clarify how data is input into an Electronic Health Record (EHR) are to determine who will be allowed to make changes to the system, how to identify them once they are logged onto the system, how to tracks changes, and then how to properly train them to use the software correctly (Arrowood et al., 2013).

Most employees in a health care facility will need access to patient EHRs, but not everyone will need the same level of access. For example, the technician responsible for making appointments will need to see basic information about the patient, but he or she will not need to view diagnosis history, medications, or have access to screens to input orders. It is up to the institution to determine what level of access each person needs based on his or her job description and create limited access profiles for those users. Doing so keeps those without need-to-know from obtaining unauthorized access (Win, Susilo, & Mu, 2006).

All users responsible for making changes to an EHR must be identified by a unique login, and they are responsible for protecting it from unauthorized access. It is not to be shared, and desktops, laptops, and other input devices must be secured whenever the use is away (Arrowood et al., 2013). To track any changes made by a user, electronic logs must be kept with the user's login data coupled with a time stamp. Any changes made will be kept as a part of the record and

no data will ever be allowed to be permanently erased (Arrowood et al., 2013). Every time a user views a chart, makes an entry or change, writes an order, or exports personal health information (PIH), a record of the login and a timestamp will be created (Arrowood et al., 2013).

All users should not only receive initial training, but also annual education and retraining. This training should focus on updating users on software changes and can include case studies to ensure users are document information correctly and in the proper areas. One suggestion is to make the training part of the yearly HIPPA certification (Arrowood et al., 2013). Additionally, the training should be documented in the employee's human resource record so that the institution can show due diligence in the future should a question arise regarding false or fraudulent errors (Arrowood et al., 2013).

I agree with the American Health Information Management Association's guidelines as they ensure that the personal health information is kept as secure as possible, especially in this day and age of identity theft and systems hacking. A person's data is not confined to just one entity, as one of the primary purposes of an EHR is the ability to share the data with other facilities. Because of this, a large number of people have access to sensitive and private information, and not all of those who look at it have good intentions.

Kaiser Health published a report in 2012 regarding the theft by a medical technician of patient information, including Medicare numbers, to be sold for healthcare fraud (KHN, 2012). Even something as simple as losing a laptop can be devastating. In the same year, a contractor downloaded the files of 34,000 patients at Howard University Hospital, and that laptop was subsequently stolen from his car (KHN, 2012). With all of this information floating around and how often it changes hands, it is imperative that all necessary safeguards are employed to protect such sensitive data.

References

Arrowood, D., Choate, E., Curtis, E., DeCathelineau, S., Drury, B., Fenton, S., … Williams, M. (2013). Integrity of the healthcare record: Best practices for EHR documentation. *Journal of AHIMA 84*(8), 58-62. Retrieved from http://www.ncbi.nlm.nih.gov/pubmed/23984510

KHN. (2012, June 3). As patients' records go digital, theft and hacking problems grow. Retrieved from http://kaiserhealthnews.org/news/electronic-health-records-theft-hacking/

Win, K. T., Susilo, W., & Mu, Y. (2006). Personal health record systems and their security protection. *Journal of Medical Systems, 30*(4), 309-315. Retrieved from http://link.springer.com/article/10.1007/s10916-006-9019-y#page-1