Compliance Today – October 2019
Maintaining data integrity

By Nicole S. Huff, DHA, MBA, CHC, CHSP

Nicole S. Huff (nicole.huff@sluhn.org) is Chief Compliance & Privacy Officer at St. Luke's University Health Network in Bethlehem, PA.

- linkedin.com/in/nicole-huff-dha-mba-chc-6359499/

Everyone in the healthcare industry depends on data to do their jobs. The integrity of that data is the backbone of any healthcare organization.

Most employees create, collect, maintain, or use data whether it is during patient registration, providing a service/treatment, recording financial transactions, or submitting claims for payment. Imagine for a second the chaos that would occur if the paper or electronic data we used daily was wrong or altered. Maintaining and relying on incorrect data carries a variety of risks and liability, including patient harm and submission of inaccurate claims for payment. To avoid these risks, data integrity is essential and considered a priority for any organization. Data integrity is defined as "a dimension of data contributing to trustworthiness and pertaining to the systems and processes for data capture, correction, maintenance, transmission and retention."[1]

Initial registration is key

Let's review how data is important for various departments within a health system. Most hospitals treat and care for thousands of patients each year. The accuracy of patients' demographics and insurance information at the initial registration is key to ensuring clinical teams treat the correct patients based on accurate and complete data noted on paper and/or electronically, and that claims are submitted based on the proper treatment of the correct patient. When employees select the incorrect patient or input the incorrect demographic information, this error affects multiple departments, including:

- Business office (e.g., correct billing and patient registration)

- Clinicians (e.g., documenting on incorrect chart because wrong patient was registered)

- Finance (e.g., correct statistical data)

- Health information management (e.g., correct medical records for the incorrect and correct patients)

- IT (e.g., correct the EPIC demographics and assist with correcting electronic data)

- Network compliance (e.g., report of possible identity theft or someone accessing medical records without authorization)

- Risk management (e.g., resolve patient complaint about billing error)

This document is only available to members. Please log in or become a member.