

Guarding against Data Corruption

Ensuring Data Integrity in IT Systems

HIM professionals know that IT systems enable quality healthcare. However, when the accuracy or completeness of the information contained in those systems has been compromised, there is potential for inefficiency, poor quality, and even harm to patients.

In the Monday presentation “How Technology Influences Data Integrity and Impacts Patient Safety, Privacy, and Security,” Barbara Demster, MS, RHIA, CHCQM, challenged HIM professionals to learn how information is created and

disparity of technology and standards, and varying data conventions and information security practices.

While these issues have the potential to negatively impact care within the organization, data integrity risks have huge implications when information is shared beyond the organization in a health information exchange or regional health information organization. These networks are still relatively new, and the impact of downstream data error may not be fully realized yet.

HIM professionals can take a leadership role in creating data integrity programs within their organizations.

moved between information systems in their organizations and to develop a data integrity program that will minimize the prospect for data corruption and inaccuracies.

IT Systems Can Corrupt, Absolutely

It is not uncommon for IT to corrupt health data, Demster said. Problems can arise when Health Level Seven and other data messages are transmitted among and between the 30 to 60 different systems commonly found in a hospital. When that happens, HIM professionals are frequently the only resource in the organization who understand what the data are and what they should look like.

Because each system's database structure is laid out differently, data transfer is complicated and the potential for corruption is greatly enhanced. For example, Demster said, a simple piece of data such as gender—male or female—can be expressed in different ways among disparate systems: M/F, F/M/Unknown, 1 for male and 2 for female, 2 for female and 1 for male, and more. These issues explode exponentially with increased database size,

“Our current solutions for linking patient information across multiple systems are flawed; for example, producing both false negative and false positive links for an individual's health records,” Demster said. “In the case of the false negative, our technology may not link the record that reports the appendectomy done two years prior to the patient's current presentation in the ER for abdominal pain. The false positive situation links and overlays the medical information of two different individuals and presents them as one individual. Either situation provides poor information for clinical decision making, which directly impacts patient safety.”

The prospect for patient identification errors alone can erode trust by those who must use the information. Demster cited a recent study of 20 million MPI records that found more than 41 percent contained blank, default, or invalid data. Duplicates, overlays, and overlaps are also common. Errors and data integrity issues result in inefficiencies such as redundant services because of a lack of trust in the information needed to care for the patient.

Needed: Data Integrity Programs

Needed to deal with the complex issues surrounding patient identity and data integrity is a comprehensive approach that addresses not just the technical processes but also the business processes. Demster encouraged HIM professionals to take a leadership role within their organizations and take steps to establish data integrity programs. Key program elements include stakeholder involvement, dedicated resources, education of all staff on data standards, and an ongoing monitoring program. Critical components include a dictionary of data definitions, representations, and expressions; identification of data sets; valid value ranges; mappings across vocabularies and systems; and data standards such as HL7 messaging and X12 transactions.

Demster stressed the importance of monitoring and data validation processes.

Checks to ensure that the information sent was actually what was received and that all necessary functions and processes actually occur are critical. Ongoing testing of business and system processes to reduce or eliminate errors is a necessary part of the data integrity program. Findings of monitoring, validation, and testing should be used to constantly re-educate and train staff who collect, create, and use the data.

For HIM professionals, setting up a data integrity program means identifying high-risk areas, educating self and staff, and hiring the right expertise if necessary. It is often also necessary to develop a value proposition and sell the benefits of the program. However, HIM professionals are ideally suited to establish such a program because of their understanding of clinical, administrative, and financial processes; knowledge of how healthcare data structure and use; and expertise in privacy and security.

Attention to detail is a hallmark trait of HIM professionals, Demster noted, and in the matter of data integrity, details can save lives. ▀