Opportunities for HIM Involvement in the HIE Landscape

Save to myBoK

By AHIMA Staff

Accurate patient identification and successful linking of electronic records is highly dependent on the accuracy of key demographic data. There are three different events that must occur in order to maintain patient identity data integrity.

- The data must be collected correctly.
- The data must be entered correctly.
- The data must be queried correctly.

Errors during any of these three events create opportunities for inaccurate patient identity. The HIM challenge is managing multitudes of detailed data on thousands of records and millions of transactions each and every year. A strong data quality and control program must be maintained or the data will get out of control quickly in a health information exchange environment.

Data Ownership, Data Governance, Stewardship

The term data governance signifies "the exercise of decision-making and authority for data-related matters."[1] It refers to the overall management of the availability, usability, integrity, and security of the data employed in an organization or enterprise. It is about getting the right information to the right people at the right time. The goals of an organization's data governance include enabling better decision-making, reducing operational friction, protecting the needs of data stakeholders, training management and staff to adopt common approaches to data issues, building standards and repeatable processes, reducing costs, and increasing effectiveness through coordination of efforts and ensuring the transparency of processes. Data governance is needed to guide stakeholders on decisions and activities to ensure an agreed-upon process is followed and enforced.

Data governance principles include:[2]

- **Integrity:** Demonstrate integrity in dealings with others; be truthful and forthcoming when discussing drivers, constraints, options, and impacts for data-related decisions
- **Transparency:** Clarify to all participants and auditors on how and when the introduction of data-related decisions and controls occurred
- **Standardization:** Introduce and support standardization of enterprise data
- **Checks and Balances:** Provide checks and balances between business and technology teams, as well as between (a) creators and collectors of information; (b) managers of the information; (c) users of the information; and (d) those who introduce standards and compliance requirements
- **Stewardship:** Define accountabilities for individual contributor responsibilities and groups of data stewards
- **Accountability:** Define accountabilities for cross-functional data-related decisions, processes, and controls
- **Audit-ability:** Ensure all data-related decisions, processes, and controls are auditable and meet compliance-based and operational auditing requirements
- **Change Management:** Support proactive and reactive change management activities for reference data values and the structure or use of master data and metadata

A key principle of data governance is data stewardship, which refers to managing the enterprise's data assets in order to improve their reusability, accessibility, and quality. It is the science, art, and skill of responsible and accountable management of resources. Data ownership and data stewardship must be clearly defined and must be reflected in organization policies for data access, use, and control. An HIE must determine the gold standard of each data source and agree on who owns the data —including duplicate record tables and data transaction logs. HIEs must define the data they "own" and their information stewardship responsibilities.

Management of the data governance and stewardship activities are often led by a data administrator. This role manages all data resources for the organization, working collaboratively with all departments to support the organization's business needs by transforming data into information, and information into knowledge. It is often an executive level position and HIM professionals are well suited for this role.

Breaches

Breaches are defined under the HIPAA privacy rule as an impermissible use or disclosure that compromises the security or privacy of protected health information, such that the use or disclosure poses a significant risk of financial, reputational, or other harm to the affected individual. The HITECH Act revised the HIPAA provisions (effective September 2009) to require business associates—including HIEs—to comply with breach notification requirements.

AHIEs and participating organizations or providers should have an appropriate business associate agreement in place that clearly outlines breach notification requirements. The agreement should designate the HIE as the business associate, and the participating organizations or providers as covered entities.

The HITECH breach notification regulations require covered entities and business associates to promptly notify affected individuals of a breach. Covered entities and business associates must also report breaches to the Department of Health and Human Services and notify the media of breaches involving more than 500 individuals. Business associates must notify covered entities of any breach involving the business associate. In addition, the HHS secretary is authorized to conduct compliance audits and use civil enforcement provisions, provided no criminal conviction is associated with the breach. However, if willful neglect is proven then the secretary is required to impose civil penalties.

HIEs must include appropriate safeguards against potential breaches, such as:

- Releasing protected health information in accordance with privacy rule requirements
- Protecting electronic information per the security rule requirements
- Ensuring staff are properly trained on privacy and security rules
- Abiding by minimum necessary requirements
- Securing computers through appropriate access policies and procedures

HIEs also must be prepared to investigate and report if a breach does occur. An HIM professional can assist the HIE in development of policies and procedures that outline responsibilities for breach notification. These policies should address the notification process, who shall make such notifications and by what means, the role of the HIE versus the individual participating partners, and the penalties related to breaches.

Corrections

In an HIE environment there are three major correction challenges:

1. Information in provider records
2. Matching errors
3. Consolidation errors

All three of these errors can result in information being consumed in an electronic health record system erroneously.

The first challenge relates to information entered into a provider's electronic health record system, which is later deemed incorrect either by the provider or by the patient. This results in two challenges—how to get the information corrected and what to do with the information that others may have used when obtaining information through the EHR. Information that is deemed incorrect at the provider level should be changed at the provider level.

The second challenge relates to matching of patients using a record locator service, master patient index or another approach. For example, Provider A may identify a patient as Robert Doe and Provider B may identify the patient as Bob Doe. Consequently, it becomes a challenge to determine if the individuals are the same. Combining the patients when they are not the same person can result in information being provided for a patient that is incorrect. Not combining the patient when they

are the same person can result in an incomplete picture of the patient's health. Therefore, it is very important the providers use the complete and accurate information when entering information into an EHR. Further information can be found in the "Patient Identification Management Challenge" section above.

The third challenge relates to information that is consolidated by an HIE that results in an inaccurate or confusing consolidated record. For example, you may have lab results that are reported differently from one lab to the next. This type of consolidation can happen today with paper records.

Correcting electronic health information can be a struggle for any organization. System limitations and functionality often dictate who, when, and how corrections can be made. However, HIPAA states that individuals should be provided with a timely means to dispute the accuracy or integrity of their individually identifiable health information and have erroneous information corrected or have a dispute documented if their request is denied. Covered entities have 60 days to correct the record or notify the individual the request was denied.

Covered entities must ensure that corrected information is provided to business associates and anyone who may have received the erroneous information, including HIEs. Challenges occur when corrected information is not sent to others, source systems are not identified at an organizational level, or the HIE agrees to a correction that an organization may have previously denied.

As the HIE will most likely not be the source system for the health information, corrections in this environment can be risky. Organizations should understand how corrections will be made by the HIE when the healthcare organization has agreed to make corrections in the patient's health record. The change has to be made to all copies of the health record across the continuum of care. HIM professionals can provide leadership and guidance regarding HIPAA privacy rule amendment requirements for the organization and HIE.

Clear and concise policies and procedures are required at both the organizational and HIE levels to ensure that corrections are handled in an appropriate manner. Corrections will depend on HIEs and their agreement with the hospital or provider. At a minimum the policy should clearly state who can initiate a correction and who is required to notify whom and within what time frame.

Notes

1. Data Governance Institute. "Data Governance: The Basic Information." http://www.datagovernance.com/adg_data_governance_basics.html.
2. Ibid.

Original source:
AHIMA Staff. "Opportunities for HIM Involvement in the HIE Landscape" (Journal of AHIMA website), January 01, 2013.

Driving the Power of Knowledge

Copyright 2022 by The American Health Information Management Association. All Rights Reserved.