Assessing and Improving EHR Data Quality: Model for Implementing an EHR Documentation Improvement Process

Improving data quality in an electronic healthcare environment requires a greater focus on standardized documentation procedures. With an EHR, the need to evaluate and improve healthcare data quality through concurrent assessment, data collection monitoring, and ongoing process improvement requires a shift from the more traditional "retrospective" method of auditing data. EHR quality and integrity depend on front-end acquisition of quality data and subsequent successful transfer of that data throughout the continuum of care. In addition, with an ongoing auditing process, confidence in the data is increased, and decision making, both from the clinical and administrative perspectives, is enhanced. Further advantages to real-time assessing and auditing include the ability to identify and correct errors early in the process, the identification and notification of patterns of errors, and more immediate impact on staff understanding through education and training.

To help move the industry toward assessing and improving healthcare data quality at the front-end, AHIMA's e-HIM® work group developed a model for implementing an EHR documentation improvement process. The model was created based on the 10 data characteristics--accuracy, accessibility, comprehensiveness, consistency, currency, definition, granularity, precision, relevancy, timeliness--outlined in AHIMA's position statement "Quality Healthcare Data and Information" shown down the left side of the table. Across the top, the work group chose six categories to describe documentation components key to front-end acquisition of quality data. These six categories (registration, assessment, treatment, follow-up, information management, and information exchange) were then defined to facilitate consistency in applying the model. In setting up the grid in this manner, a generic replicable model was produced (i.e., it is not data-, setting-, patient type-, disease-, or procedure-based). The model is designed to address measurement, improvement, and validation of data quality.

How to Use the Model

Ensuring data quality is an ongoing process. It is essential to build concurrent data quality checkpoints into all facets of documentation within an EHR. To use the model, first decide the area of focus. Ask yourself what should you be doing at the front-end to ensure data quality in the documentation process. Next, choose the first documentation component (i.e., registration) and determine the critical point in the EHR documentation process where safeguards need to be built to check for data quality. The work group coined the term "data quality checkpoint" for this key step in the process. Keep in mind the types of things that should be done to check for data quality and prevent errors. Identify the checkpoints required to assess and improve healthcare data quality. Once the data quality checkpoint is identified, determine what should be used to measure, improve, or validate data quality to address the 10 characteristics and complete the column for registration. Repeat the process for each documentation component until the table is complete. The finished product provides areas of concentration for implementing your EHR documentation improvement process.

Tips

To ensure data quality within the EHR, keep in mind the following guidelines when using the model:

- Stay at a high level and do not address the details at the data element level.
- Focus on the patient. Run the patient through the process.
- Consider where in the process data are being documented and at what point in the process quality monitoring should occur.
- Focus on front-end data with carefully selected quality checkpoints throughout the process.
- Address the criticality of quality point-of-care data.
- Choose data quality checkpoints that deal with the documentation challenges in your particular facility.

- Checkpoints should be straightforward and adaptable to ensure data quality and meet the increasingly complex data documentation challenges of an EHR.
-

Applying the Model to a Patient Encounter

To further illustrate the use of the model in implementing an EHR documentation improvement process, a completed grid is provided. The work group chose a patient encounter as the area of focus. Next, the data quality checkpoints for each of the documentation components were identified. For example, while it is recognized there are a number of activities which must occur in order to successfully register a patient and each healthcare entity will have its own protocol-specific registration process, patient identification is a core piece for everyone. Therefore the work group chose ID Validation as the checkpoint for the documentation component “Registration.” Moving down the column, the work group determined what should be used to measure, improve, or validate data quality as it pertains to the data characteristic “Accuracy.” For this example the work group decided on photo ID or two other forms of identification. These steps were duplicated until every section of the table contained an item for measuring, improving, or validating data quality.

Data Characteristics	Registration[1] Data Quality Checkpoint: Identification (ID) Validation (identity proofing)	Assessment[2] Data Quality Checkpoint: History and physical (H&P)	Treatment[3] Data Quality Checkpoint: Medication reconciliation	Follow-up[4] Data Quality Checkpoint: Discharge/ Transfer/ Referral (DTR) record with patient instructions	Information Management[5] Data Quality Checkpoint: Audit log of unauthorized access to the patient record	Information Exchange (external)[6] Data Quality Checkpoint: Information from external sources
Accuracy--Ensures data have the correct value, are valid, and attached to the correct patient record.	Photo ID or two other forms of identification used.	Authentication by author licensed by the state. Patient demographics (five core data elements (i.e., name [first, middle initial, last], date of birth, gender, Social Security number, medical record number) against that of the record.	List is current and the source of information is noted.	Policies exist defining the components of the DTR record (e.g., correct patient ID, location for follow-up/ongoing care, patient instructions for self-care, diet, activity, and current medication regimen and allergies).	Periodic system security audits conducted to prevent unauthorized alteration or loss of data.	Incoming records matched against requests for information and validated.
Accessibility--Data items should be easily obtainable and legal to access with strong protections and controls built into the process.	Record of ID validation for each patient encounter exists (i.e., mandatory flag indicating the ID was validated and checked against the master person index).	Available to the right person, in the right place, at right time, for the right purpose as allowed by state and federal law.	Clinical history that pulls the data from previous encounters is available for verification and usage in patient care (e.g., check and verify patient meds with prior record).	Information is made available to patient and patient-authorized organization/individual responsible for ongoing care at conclusion of visit/stay.	End user authentication achieved by system signature, date/time stamp.	Data available in PDF format only and linked to appropriate patient record by note in system.
Comprehensiveness--All required data items are included. Ensure that the entire scope of the data is collected and document intentional limitations.	Source and date of ID validation noted. Flag addressed. Multiple discriminations that would further ID the patient such as mother's maiden name included.	Includes all components required by regulatory/accrediting agencies, medical staff rules, and bylaws.	Data needed for treatment as defined by regulatory/accrediting agencies, medical staff rules, and bylaws is available at the point of service (e.g., for each medication the name, dosage, route, timing, duration are documented).	Record includes all components required by regulatory agencies/accrediting bodies, medical staff rules, and bylaws. Verification of patient/SO understanding of instructions is documented by licensed author	Includes user's login ID and date and time of access and the content accessed.	Policies note external data cannot be certified as comprehensive.
Consistency--The value of the data should be reliable and the same across applications.	Standards exist for ID search criteria (e.g., full name search, partial name search).	Required content is the same and available across the encounter and between applications (e.g., the allergy stated in the H&P should the same throughout the patient stay).	Data values are coordinated across the continuum of care (e.g., the translation of a patient's medication list to a required formulary is verified each time a translation occurs).	Process exists ensuring DTR data is consistent with data in other parts of the medical record.	A plan and schedule exists for audits and follow-up.	Policies address the use of external data because it may not meet internal definitions.

Currency--The data should be up-to-date.	Policies exist ensuring the latest ID data is entered and validated.	Information is updated in real-time or within a certain timeframe (i.e., information is synchronized every 30 minutes). When auto-population of data occurs, author validates and updates as necessary and a notation is captured by the system of this occurrence.	Medications taken by the patient are verified against the previous record and updated as necessary.	Policies exist to ensure the most current dta are entered and verified for each component.	Verify data classes are clearly and appropriately defined and consistent with current business needs and requirements (e.g., public, sensitive, private, confidential).	Policies note data from external source will not be current. Relying on dates within documentation is suspect in electronic form.
Definition--Clear definitions should be provided so that current and future data users will know what the data mean. Each data element should have clear meaning and acceptable values.	A policy and procedure for updating, communicating, disseminating, and implementing the data dictionary exists (e.g., standards exist to ensure the same patient name and ID flows across all modules of the system including use of hyphens, apostrophes, etc.)	Guidelines defining H&P content (e.g., those by an accrediting agency) are available to authors and noted in the application user guide.	Standardized formulary exists.	Standardized data definitions for each required component of DTR are clearly defined.	A storage security assessment and audit procedure integrated with other security practices once the major elements of storage security have been defined appropriately for your organizations.	Policies note any agreements with other providers as to definitions of the data.
Granularity--The attributes and values of data should be defined at the correct level of detail.	A policy and procedure for updating, communicating, disseminating, and implementing the data dictionary exists (e.g., truncation does not occur and values are clearly understood).	Components of the H&P as defined by the chosen standard (e.g., CMS E&M guidelines) are documented.	Attributes for each medication (e.g., dosage, form, route, etc.) are defined.	Content of the DTR is defined so all required information for each component is captured (e.g., for medications: brand/generic name, dosage, route, frequency; for activities allowed description of examples).	A storage security assessment and audit procedure integrated with other security practices once the major elements of storage security have been defined appropriately for your organizations.	Policies note beyond what would be expected from the current standards there is no assurance of the values assigned to data (e.g., laboratory values from another source may not be expressed in the same manner as receiving facility).

Precision--Data values should be just large enough to support the application or process.	Standard policies exist ensuring the same set of rules apply to the ID data values for capture, storage, display, and reporting.	Data obtained by the provider support the degree of patient complexity.	Checks are done to ensure what is ordered is what is given to the patient.	Policies exist to allow prepopulated fields (e.g., discharge medication list, instructions) as well as free text to facilitate data capture (e.g., name/location of organization to provide ongoing care).	Changes are identified and potential security impact assessed.	As directed by HIPAA, the sending organization sends only the minimum necessary information requested.
Relevancy--The data are meaningful to the performance of the process or application for which they are collected	Standard policies exist requiring the capture of all demographic data that reflects the information needed for ID validation. Standard algorithm for pulling up the patient exists.	Data obtained by the provider support the plan of care (e.g., significant positive/negative findings).	Express relationships to established standards meet the patient/client needs, achieve the organizations goals and produce benefits exist.	Policies exist requiring the DTR to contain data relevant and necessary for coordination of ongoing care of the patient.	Compliance with specified controls and procedures verified.	Policies note beyond what would be expected from the current standards there is no assurance of the receipt of meaningful data.
Timeliness--Timeliness is determined by how the data are being used and their context.	Real-time updates of ID are performed.	Documented at the time of encounter by the authorized provider and available for patient care.	Patient's medications are available for patient care.	Record is documented at the conclusion of the patient encounter and made available to the patient and patient-authorized organization/individual responsible for ongoing care.	Conduct audits on a regularly scheduled routine and as needed.	Policies note data from external source will never be timely in the sense of context because the receiver would not be defining the context.

Notes

1. Registration is the process of entering a patient into the system for the purpose of receiving care from a provider.
2. The systematic collection and review of information pertaining to an individual who wants to receive healthcare services or enter a healthcare setting.
3. Treatment is intervening in a collaborative manner; providing appropriate preventive care, providing supportive care, treating a disease or condition, or symptoms using accepted professional standards of practice.
4. Follow-up is the recommended care, treatment, or services to be continued to ensure continuity of care once a patient is discharged or transferred.
5. The acquisition, organization, analysis, storage, retrieval, and dissemination of information to support decision-making activities.
6. Information exchange is the transfer or dissemination of information that is gathered or computed about a patient as part of a healthcare encounter.

References

AHIMA. "Quality Healthcare Data and Information."

Article citation:
AHIMA e-HIM Work Group on Assessing and Improving Healthcare Data Quality in the EHR. "Assessing and Improving EHR Data Quality: Model for Implementing an EHR Documentation Improvement Process" *Journal of AHIMA* 78, no.3 (March 2007): 69-72.