Anticipating Error: Identifying Weak Links in the Electronic Healthcare Environment

by Madhavan Nayar and Sharon Miller

In HIM, technology is only as good as the data it delivers. Information integrity offers a systematic way to identify where and how error can enter the electronic health record.

The electronic health record (EHR) offers crucial improvements to healthcare, including reduced medical errors, better-informed decision making, and reduced cost. But HIM professionals know that what the EHR really offers is the potential for improvement. Delivering more patient information at the point of care, for example, improves care only when the information is accurate and complete. Ultimately, an EHR is only as good as its data.

Ensuring the integrity of data has always been a key tenet of HIM practice. Now, as health information goes digital and workflows move across networked electronic systems, HIM professionals are playing an important role in identifying where patient information can be compromised in these new systems. One way to do this is through the discipline of information integrity.

Where Do Errors Come From?

Information integrity is the dependability or trustworthiness of information. It concerns more than data quality or data accuracy—it encompasses the entire framework in which information is recorded, processed, and used.[1]

Accuracy, consistency, and reliability define the value of information. Content, process, and system describe the universe in which the information operates. In EHR systems, integrity is the accuracy, consistency, and reliability of the information content, process, and system. Examples are shown in "Seeing the Forest and the Trees" below.

Risk to the integrity of information comes from intrinsic and extrinsic factors. Intrinsic risks are anticipated sources of errors, those within the control of the information producer or user. Extrinsic risk is unanticipated, coming from sources outside the system and beyond the control of data producers and users.

The Errors Within

The Errors Within

Intrinsic risk factors are anticipated sources of errors, which are within the control of the information producer or user:

- Design
- Data
- Deployment
- Development
- Detection

Data is vulnerable to compromise at five points in internal processes. These can be described as errors in design, development, deployment, data, and detection.

Design. The design process defines user needs, system functionality, and system workflow. Poor design specifications can result in a flawed product and loss of information integrity; for example, the failure to capture an important patient statistic.

Design errors can be minimized by thoroughly defining system requirements at the start of the design process and then through subsequent design walkthroughs. Because the EHR system will cut across the entire organization, the design phase should involve a team that includes physicians and clinical staff, information technology staff, business staff, and HIM professionals, according to Lindy Alves, RHIA, manager of practice management applications and technical development at Harvard Vanguard Medical Associates in Newton, MA.

The design process should also include a workflow walkthrough, Alves notes. A walkthrough can be accomplished by creating a detailed flowchart that follows the work through its complete cycle. This should be done for all departments, both clinical and business. The walkthrough should assign responsibility for each step in the process, check for redundancies and inefficiencies, establish which data will be presented and how data will be shown, set security policies, and confirm the ability to audit the system. In particular, HIM professionals must be actively involved in planning every aspect of new systems and be particularly watchful to make sure all records meet legal requirements, says Terri Bunsen, RHIA, director of health information records services at Evanston Northwestern Healthcare in Evanston, IL.

Development. The development phase involves construction of the verified design.

Development errors can be minimized through the use of proven development methods and effective software and system testing. Effort spent on good development minimizes threats to data integrity at later stages, such as conversion from old systems to the new system.

A great deal of thought needs to be given to EHR screens and formats during design and development because a “user friendly system is key to success,” says Hazel Kimmel, RN, CCS, CPC, audit specialist at Wellmont Health Services in Kingsport, TN. Kimmel suggests that two teams design screens and formats: an “input” team for those who will be inputting data and an “output” team for those who will be accessing data on an as-needed basis at the point of service and for those using the data in the archive or for required reporting.

Deployment. In the deployment phase, users first try out the new system. This is the stage of implementation and training, when flaws in design and development surface. Unanticipated gaps in security and control, for example, may become apparent at this point.

Lancaster General Hospital in Pennsylvania uses a security checklist that evaluates vendor capabilities for unique user IDs, password security, auto log off, inactivation of lapsed user IDs, and generation of audit and activity logs that track users’ activities, says Andrea Thomas, MBA, RHIA, director of clinical information management at the hospital.

Data. A typical hospital system interfaces between lab, pharmacy, clinical, and HIM departments, with the possibility that data may be altered when moving among systems. A common data error, for example, is the rounding of dosages or the truncating of numbers at system interfaces where data fields are not standardized. Data errors can be minimized through appropriate audit and validation of input data. Thomas notes that testing data at every interface is a vital step in rolling out a new or evolved system.

Detection. The failure to detect error is another point in internal processes where data integrity may be compromised. Detection errors can be minimized through effective verification and reconciliation. Audits for common errors regarding level of service, medical necessity documentation, and multiple physician visits (segregating services by specialty) should be undertaken randomly and then followed with more detailed examinations when problems are identified, says Cathy Zimmer, RHIT, manager of compliance and EHR at ChoiceCare Physicians in Pittsburgh, PA.

When Hazel Kimmel sees a billing error, she drills down to see why it happened. For example, Kimmel may see a lab test has been billed but no order for the test is on record. This could be the result of too many, too few, or the absence of correct choices on the nurses’ order screen, she says. Or it may be the result of a choice having been incorrectly cross-walked between systems.

The Errors Without

The Errors Without

Extrinsic risk factors are unanticipated errors caused by factors outside of the system and beyond the control of the information producer or user:

- Change
- Communication
- Complexity
- Corruption
- Conversion

Five factors external to the EHR can also threaten its integrity. These can be described as change, complexity, communication, conversion, and corruption.

Change. If external influences change, the system may fail to adapt with complete accuracy. New legislation, such as HIPAA, can require significant changes to system and process that create the possibility of error. Organizational restructuring and mergers can have the same result, as can simpler changes to personnel. Hardware upgrades can cause change that results in errors being introduced to the EHR. Adoption of new software designed for multiple users in the lab, pharmacy, and clinic may result in errors caused by a lack of interoperability.

Change also has a very human dimension. Buy-in to a new system is important throughout the organization, even in a medium-sized office, says Cathy Zimmer. The risk of error is higher during this time. Harvard Vanguard negotiated the same transition period, according to Lindy Alves. After some initial resistance, she says, most clinicians now feel the EHR system has immeasurable value.

Complexity. The large number and variety of components and interfaces in an EHR system, coupled with high volume and speed of information processing, create opportunities for error. The proliferation of new hospital systems and the resulting multiple interfaces introduce new complexities because electronic interfaces for many departments and facilities must communicate without losing integrity of information. Additional complexities include rules and alarms that may be built into the EHR: allergy warnings, drug interactions, and rules-based checks and balances.

The longitudinal nature of the EHR introduces challenges of its own and, while making tasks easier for clinical staff, may add complexity to HIM responsibilities. This increased difficulty can occur when documentation for a procedure is located in the physician office record and not entered in the hospital record, says Terri Bunsen. Many physicians will not make duplicate entries when they know the records are electronically linked. This requires HIM staff to cut and paste documentation.

Communication. Errors due to communication include partial, duplicate, or missed transmission or receipt of information. For example, a physician may need access to the EHR from a remote location, but the office records are not updated with hospital admitting and discharge information. The Harvard Vanguard EHR system allows physicians secure access to office records when they are at the hospital, as does the Evanston Northwestern Healthcare system, but these may be in the minority. Similarly, hospital records are often not electronically available to office locations.

Conversion. Error can be introduced when information is merged, split, or transformed from one format or medium to another. Conversion of records from paper to electronic provides opportunity for loss of integrity of information because historical information may be discarded or disconnected from the new electronic record. Duplication of information may result from a patchwork of systems based on combining programs from several vendors or programmers. The risk of conversion errors can also be managed by rolling out a new system in phases—documentation first and order entry second, says Terri Bunsen.

Corruption. Both accidental failure and deliberate fraud can be considered errors due to corruption. Fraud can occur when a patient uses another person's name or Social Security number when seeking treatment. A master patient record, as part of a complete EHR system, can avoid confusion among patients. Another form of corruption in the EHR results from misdirected results to the wrong patient record—potentially causing an error of patient care (e.g., additional consultations, transfer to another level of care, and inappropriate follow-up tests). Finally, accidental system failure is also considered a form of corruption. Down time on a system can be disastrous to patient care and should be considered a patient safety concern, says Andrea Thomas.

HIM's Role in Information Integrity

HIM professionals should be involved in all decisions that affect EHR accuracy, consistency, and reliability as well as content, process, and system. This involvement should include being represented or leading all design and deployment projects involving EHRs and, in many cases, facilitating communication among the various design team members representing clinical, business, information technology, support staff, and other functions.

Regular contact with physicians, other health professionals, and support staff will help improve consistency, as will rules that require modification or amendment rather than alteration of an entry. Drop-down menus, predefined paragraphs, or templates for documentation of common procedures and checklists can add additional consistency to the EHR, but they may also introduce errors based on wrong choices in automated features. These errors may then proliferate in the electronic environment. HIM involvement in the design of such features is important.

HIM professionals also prove themselves good resources for designing or leading training on new systems. Staff training is crucial to ensuring accuracy and reliability. Evanston Northwestern Healthcare requires 16 hours of classroom training for all physicians and others who will access the EHR before receiving passwords. Training is an ongoing process as new staff is added and system upgrades add new features and sophistication. Training on similar systems at other institutions should not be permitted to fulfill training requirements because it is important to clarify policies and procedures for use of the system in your own organization. If new users have experience with a similar or identical system at another institution, it may be sufficient to explain differences in expected and permitted use in your institution.

It is now more important than ever that the HIM professional reach out to all parts of the organization and take a leadership role in ensuring information integrity in the electronic environment. Terri Bunsen sums this up clearly: "We need to be actively involved in planning new systems and be prepared for the new challenges of complexity, training, access, and new types of mistakes possible in the electronic environment."

Viewing the development and management of electronic medical records in the context of information integrity will help HIM professionals anticipate the intrinsic and extrinsic risk factors and prevent problems before they occur. The information integrity concept, while still in an early stage of development, can provide many insights that make the adoption of EHR easier and more effective. In the long term, this emerging discipline may evolve into more rigorous principles to help ensure the dependability of the EHR.

Seeing the Forest and the Trees

HIM professionals ensure the accuracy, consistency, and reliability of health information records. They must also evaluate the larger context in which the records are created and maintained: the content, process, and system through which the information flows. Assessing information integrity in the EHR includes evaluating data for each of these criteria.

Accuracy
Is the recorded health data accurate, or has it been impaired by improper entry, coding, missing information, organization of information, or damage brought about by lack of system interoperability?

Consistency
Do all healthcare professionals and support staff with access to the EHR enter and manage patient data in the same manner, and do systems prohibit alteration after an entry has been saved?

Reliability
Does the required health information find its way to the EHR in a timely fashion, or does it become waylaid or lost?

Content
Is the content of the health record adequate for making correct clinical decisions and ensuring appropriate billing?

Process
Are the steps of capturing, translating, storing, and accessing health information accurate, consistent, and reliable over time and across the entire organization?

System
How does the EHR fit into the overall system of the practice group or hospital, and what systemic factors assist or impede the integrity of the EHR?

Note

1. Nayar, Madhavan. "The Information Integrity Imperative." Available online at www.informationintegrity.org/php/content/readsubsection.php?catid=19.

Madhavan Nayar *(m.nayar@informationintegrity.org) is company leader of Unitech Systems and cofounder of the Information Integrity Coalition. Sharon Miller (smiller@iicoalition.org) is president of Health Care Innovations and an active member of the Information Integrity Coalition, representing the healthcare industry.*

Article citation:
Nayar, Madhavan, and Sharon Miller. "Anticipating Error: Identifying Weak Links in the Electronic Healthcare Environment." *Journal of AHIMA* 75, no.8 (September 2004): 46-50.