Keys to Help Solve Patient Data Matching

By Michael L. Nelson, DPM

Accurate patient data matching is a critical patient safety issue. Overlays that comingle the medical information of two or more people may lead to disastrous adverse medical events and duplicate medical records, which may be fragmented and incomplete and can limit the effectiveness of treatment plans, resulting in less than optimal outcomes.

Patient data matching is also a fundamental core building block for interoperability and health information exchange. After all, what good is it to have disparate electronic medical records speak the same language if they don't know who they are talking about?

Overlays, mismatches, false positive matches, and false negative matches have plagued the healthcare industry for decades. In spite of the widespread deployment of master patient indexes (MPIs) with sophisticated matching algorithms, a 2008 RAND report noted that, on average, an eight percent duplicate record rate existed in the MPI databases studied.[1] The average duplicate record rate increased to 9.4 percent in MPI databases with more than one million records. Additionally, the report identified that the duplicate record rates of the enterprise master patient/person index (EMPI) databases studied were as high as 39.1 percent. According to a 2012 College of Healthcare Information Management Executives (CHIME) survey of healthcare CIOs, error rates due to patient mismatching averaged eight percent and ranged up to 20 percent.[2]

There are a number of reasons that may lead to high duplicate medical record rates, such as: multiple information systems and databases, merger and acquisition data consolidation, health information technology/electronic health record (EHR) upgrades or replacements, and poor or no system integration.

The biggest culprit, however, is poor data integrity, including:

- Non-standardized data
- Missing or inaccurate data
- Old data
- Name, address, or phone number discrepancies
- Aliases
- Data entry errors

Healthcare organizations may not have the ability or resources required to manage changes to patient demographics, and the effectiveness of MPIs is limited due to unreliable data.

Take, for example, a case in which a female patient returns for care at a single healthcare system after a five-year hiatus. During that time away she has gotten divorced and reverted to her maiden name, moved to her own apartment, and changed employers. This presents a challenge to the organization, which must match her medical record to the original record created five years earlier.

Another example at the macro level could be that of a "snowbird," an individual who lives and receives medical treatment in their northern home state during the spring and summer and lives and receives medical treatment in a southern state where they reside during the winter. The difference in residential addresses may be a challenge for matching records across the different states.

Organizations including the Office of the National Coordinator for Health IT (ONC), CHIME, AHIMA, and the American Hospital Association have all called for a better way to solve the patient data matching dilemma.

A compelling patient matching strategy would include implementation of a four-pronged, comprehensive approach that:

1. Cleans up the MPI
2. Improves ongoing data integrity
3. Authenticates patient identities
4. Verifies that an authenticated identity belongs to the patient

Cleaning Up the Master Patient Index—'It's All About the Data'

MPI cleanups can be quite costly for records that cannot be automatically merged. Time-consuming manual processes are needed to help resolve many questionable medical record matches that require human intervention due to inaccurate, missing, out of date, and/or conflicting demographic data. A practical solution to this data integrity problem is to leverage third party Big Data referential databases and keying technology.

There are a handful of organizations that maintain national databases of individuals that generally include current and historic name, address, and phone number information. These Big Data companies monitor and maintain this information as a business-critical process. When considering such a Big Data company, one should investigate the sources they rely upon for their information. A Big Data company that receives information from financial institutions, the utility industry, and the telecommunications industry generally has more current name, address, and phone information because these sources are consistently conducting financial transactions with their customers. Even though an individual may be "underbanked" with little or no credit history, this person may still pay a utility or cell phone bill.

Maintaining a national database of consumers requires assigning a unique key to the consumer that can be matched to a patient and/or member database so as to facilitate matching patient/member data for providers and payers at both the micro and macro levels. Deterministic matching to third party Big Data, which contains current and historical information about addresses, aliases, and name changes, can be leveraged to assist in dramatically increasing match rates and decreasing the number of questionable matches, resulting in potential lower cleanup costs. This solution does not suggest completely replacing the traditional MPIs in which healthcare organizations have invested a great deal of time and money. Rather, the organization can submit its patient record files to a third party Big Data company for matching and keying against that company's database. The potential output would be a more accurate list of unique patients along with a unique "key" that can be consumed by the MPI and utilized as a weighted additional matching attribute to help enable auto-merging of a much greater number of duplicate records. This could significantly lower the potential cost of an MPI cleanup.

There has been much debate over the subject of a national patient identifier. Although the concept was conceived and written into the original HIPAA law, privacy and consumer groups have asked the federal government not to fund such an endeavor. There is now a movement in Congress to stop using Social Security numbers on Medicare cards and institute a new Medicare enumerating system for improved privacy and accuracy. Although the federal government has not pursued a national patient identifier, there is no reason that the private sector cannot pursue alternatives to address the issue. For example, a Big Data company's unique "key" for each unique person in its national consumer database, when matched to a patient's medical record at disparate health systems, can facilitate patient data matching across those systems.

Improving Ongoing Data Integrity

Once the MPI is cleansed, it is vital that it be kept clean moving forward by capturing accurate data at registration. Optical character recognition of identifying documents such as driver's licenses can help eliminate transcribing errors. Instituting policies that require capturing specific data elements in specific formats will also assist to keep the MPI clean and help prevent the creation of duplicate medical records. For missing or questionable demographic data, the third party Big Data companies can offer one-stop shop web service lookups of current and historical demographic data. Such a web service can be valuable when there are language barriers or to help prevent the creation of duplicate medical records in the emergency department when patient registration may be secondary to patient care.

Authenticating Patient Identities

Fraud in healthcare is growing—particularly identity-based fraud. At registration, patients must confirm that their identity is real. Synthetic identities can come in multiple guises. For instance, it is possible to fabricate a completely new false identity with phony demographics and identifiers. Another identity thief might use real demographic and identity information from

multiple real people to create a new false identity. A web service call from registration to a credit bureau can often help authenticate whether or not the identity is real.

Verifying That an Authenticated Identity Belongs to the Patient

Once the registrar authenticates the identity, the next step is to verify that the identity belongs to the person who is registering for services. There are various options to do so—in face-to-face registration usually the patient is asked for a government-issued photo ID. In most cases this is a driver's license that then is scanned into the electronic medical record. However, care should be taken to ensure that the ID itself is not fraudulent. Suppose the patient does not have a government-issued photo ID, or there is something questionable about the ID the patient presents. An effective alternative identity-proofing solution is to ask knowledge-based authentication (KBA) challenge questions that the patient must answer correctly to prove their identity. KBA questions should be based on information that may not be publicly available, making it more difficult for a fraudulent patient to answer correctly.

Biometrics, smart cards, and unique patient identifiers can help prevent the creation of overlays and duplicate medical records from the day they are implemented. However, the healthcare organization should attempt to validate a patient's proof of identity prior to issuing him or her a biometric, smart card, or unique patient identifier. There should also be a linkage to historical medical records at the facility. Do not underestimate the importance of medical history. One must know where one comes from before determining which path to take.

Bringing it All Together

Accurate patient data matching is a core element in building a foundation for interoperability and health information exchange, and is a critical component of patient safety. A comprehensive patient data matching solution should include third party Big Data referential databases and technologies to drive processes that link historical medical records, biometrics, smart cards, and unique identifiers to the patient wherever the patient seeks treatment.

Notes

[1] RAND Corporation. "Identity Crisis: An Examination of the Costs and Benefits of a Unique Patient Identifier for the U.S. Health Care System." 2008. www.rand.org/pubs/monographs/MG753.

[2] College of Healthcare Information Management Executives. "Summary of CHIME Survey on Patient Data-Matching." May 16, 2012. http://chimecentral.org/wp-content/uploads/2014/11/Summary_of_CHIME_Survey_on_Patient_Data.pdf.

Michael L. Nelson (michael.nelson@equifax.com) is the vice president of healthcare and business development, identity, and fraud solutions at Equifax, Inc.

Article citation:
Nelson, Michael L. "Keys to Help Solve Patient Data Matching" *Journal of AHIMA* 86, no.8 (August 2015): 28-30.