Adopting A Unique Health Safety Identifier (UHSI)

Eliminating Medical Identity Theft, Duplicate Records, and Payment Fraud

Health IT for Value-Based Care

Interoperability. ConnectCare. Intelligent Care. MACRA. ACO. Value-Based Care. The Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009 has driven an unprecedented transformation in care settings—the federal government alone investing nearly $30 billion. In 2015, 96 percent of all non-federal acute care hospitals possessed certified health IT. Small rural and small urban hospitals had the lowest rates at 94 percent. Ninety-six percent of Critical Access Hospitals had certified health IT, while 98 percent of large hospitals had certified health IT—the highest rate among these hospital types.[1]

Tom Foley, Director of Global Health Solutions Strategy

With the overall market seemingly embracing the use of health IT to electronically store, retrieve, and analyze clinical information, it is once again poised to transform itself from an encounter-based delivery of care to a "value-based care" model—a risk-based model with reimbursements increasingly linked to patient outcomes.

To best achieve patient outcomes, it's critical that there be a focus on improving the quality of data at the point of care. To achieve this objective, it is believed the market needs to give specific focus on addressing the following to maximize its ability to mitigate financial risk and achievement of patient outcomes:

1. Medical Identity Theft: $84 billion a year problem
2. Duplicate Records: 10% of electronic medical records in an electronic health record (EHR) system are impacted
3. Payment Fraud: $28 billion annual financial impact to health delivery organizations

Medical Identity

Who are you? In 2014, nearly 9 million patient health records were breached in 164 reported incidents. By March 2015, some 90 million patients were affected. In one incident, the Social Security number (SSN) of 79 million individuals was compromised. While driver's licenses, SSNs, birth certificates, and other forms of information which represents an individual were not intended to be identity credentials, they have become just that.

As a result of these breaches, the acquired information is making its way into the mainstream as synthetic identities. Therefore, it's challenging to confirm that the presenter of credential(s) is the individual he or she is claiming to be, hence the importance of enhancing the health services registration process with an identity proofing process coupled with collecting and validating the representation of the person with a biometric.

The black market value of protected health information (PHI) data is at an all-time high, tempting more cybercriminals to breach health IT systems. This is because PHI data lends itself to pharmaceutical fraud, insurance fraud, and access to more channels like Medicare and Medicaid. The International Data Corporation (IDC) Health Insights report predicts that one in three health records will be compromised in 2016.[2]

A dramatic set of statistics published by Harris County Health District in Houston on April 5, 2011, illustrates just how easy it is to misidentify a patient based just on name and birthday. In a database of more than 3.4 million patients, two patients sharing the same first and last name occurred 249,213 times. Five or more patients sharing the same first and

Health

Lenovo

last name occurred 76,354 times. Of the 249,213 pairs of shared names, 69,807 of those pairs had the same birthday. In one woman's case, 2,488 patients shared her first and last name, and 231 of those also shared her birthday.[3]

The coincidences and questions add up quickly: Are those 231 records the same person? How many could be duplicates? There needs to be a unique way to decipher each of those 231 patients with the same name and birthday. If not, this challenges an accountable care organization's ability to accurately account for the true number of lives it manages, which increases the probability for misdiagnoses, ineffective treatment plans, and patient identity theft.

Historically, the issue of identity disambiguation was addressed through the use of Enterprise Master Patient Index (EMPI) technology, but it has a theoretical limit of just 98 percent accuracy, and that occurs only when the patient demographic record has a complete set of details with strong data governance policies.[4]

Duplicate Records

An alarming statistic is that health IT systems contain an average of 10% of duplicate medical records.[5] The American Health Information Management Association (AHIMA) emphasizes that misidentification and duplicate information entered into EHRs cause misdiagnoses, unnecessary tests, and inappropriate treatments, all of which hinders the ability to improve patient care and drives up medical costs.[6] According to the Office of the National Coordinator for Health Information Technology (ONC), accurate patient identification is the single largest roadblock to true interoperability.[7] Hence, it calls for all organizations that match electronic health information have an internal duplicate record rate of no more than 2% at the end of 2017.[8]

The average Medicare/Medicaid patient has multiple chronic conditions and sees nine different providers in a given year. To dramatize a point, let's assume all providers are using a different EHR. They also will have a different patient ID in each system, and many aspects of his or her demographic information are recorded differently or in error. When this information is shared, oftentimes it cannot be automatically reconciled, creating duplicate records, hence the earlier reference indicating patient identification is the single largest roadblock to true interoperability.

It is further suggested that the practice of manually reconciling data in the backend, given that medical identity theft is such a pervasive problem, raises the question of how does an IT person or analytics program know the data is associated with the same person?

Payment Fraud

Payment fraud is a byproduct of identity theft—a misrepresentation of whom one is and/or a case of having proper identity yet providing unauthorized forms of payment. With consumers bearing a greater burden of the cost of care, last year alone consumers spent $824 billion for healthcare services, including out-of-pocket and deductible payments. This spending trend is expected to reach $2 trillion by 2020. Sixty-two percent of finance professionals report that their organizations were targets of payment fraud in 2014.[9] This has translated to nearly $28 billion in overall costs (out-of-pocket expense plus the cost of overall services). Payment for services should not be looked at separately from medical identity theft and duplicate records as the same solution—assignment of a Unique Health Safety Identifier (UHSI), coupled with the use of biometric or other equally strong second factor, has demonstrated to eliminate each of these barriers.

Conclusion

Medical identity theft, duplicate records, and payment fraud have been longstanding problems in the care delivery model. Many organizations have implemented data reconciliation processes that merge records without awareness nor detection of medical identity theft, potentially causing harm to innocent patients. Others collect biometrics from patients without identity proofing them, employing recommended National Institute of Standards and Technology (NIST) Level of Assurance 3 (LOA3) criteria while also using processes and trained resources from an accredited EHNAC (Electronic Healthcare Network Accreditation Commission) Registration Authority. As well, most only identity proof a consumer patient within the silo of a specific delivery of care facility and still have different identities across the multiple care settings.

The solution cannot be solved by one EHR vendor; however, it does require a single approach recognized by all. Implementing one UHSI coupled with multifactor authentication while validated under the guides of an EHNAC accredited Registration Authority is known to eliminate medical identity theft, duplicate records, and payment fraud. Moreover, eliminating these longstanding challenges will lead to improved data quality at the point of care, as well as provide value-based care delivery providing the true data set necessary to manage the lives within their care.

Leverage the following steps to improve data quality, and minimize your financial risk in a value-based care delivery model:

1. Employ an EHNAC accredited Registration Authority to employ the appropriate processes and protocol to effectively identity proof a patient prior to receiving services which establishes a high confidence in the asserted identity's validity. The ONC recommends that NIST LOA3 criteria for in-person proofing. Note: Admittedly doing this in an EMS or emergency room setting may not be possible.
2. Provide associated training to registrars to perform this critical function—the National Association of Healthcare Access Management (NAHAM) should be solicited for this effort.
3. Assign a UHSI, once patient has been identity proofed.
4. Assign the UHSI to a patient record.
5. Capture a second factor authentication to establish a token to be used across any supporting system. Multiple tokens (based on the approach of a given facility) can be linked to a single UHSI.

If each of these five steps are employed, and most importantly one has the authoritative UHSI recognized across all care settings in a community, it will allow the necessary interoperability to securely and safely exchange patient health records while also eliminating medical identity theft, duplicate records, and payment fraud. Therefore, let's not rush to a value-based care model without employing this critical service.

If you would like to further discuss this model, please send me a tweet **@FoleyTom** or **@LenovoHealth.**

1. ONC/American Hospital Association (AHA), AHA Annual Survey Information Technology Supplement. 2015.
2. Healthcare Fraud: A Five-Step Plan for Diagnoses and Treatment. Information Age. April 20, 2016.
3. Thoughts and Recommendations on a National Health Safety Identifier. Healthcare Infomatics. February 22, 2016.
4. AHIMA Work Group. Managing the Integrity of Patient Identity in Health Information Exchange (2014 update). Journal of AHIMA. May 2014.
5. AHIMA Foundation, Perspectives in Health Information Management, Why Patient Matching Is a Challenge: Research on Master Patient Index (MPI) Data Discrepancies in Key Identifying Fields. Spring 2016.
6. Petition Calls for Unique Patient Identifier Solution. Journal of AHIMA. March 21, 2016.
7. Patient Matching and Identification Report. The Office of the National Coordinator for Health Information Technology. February 7, 2014.
8. Connecting Health and Care for the Nation: A Shared Nationwide Interoperability Roadmap Final, Version 1.0, Office of National Coordinator. October 6, 2015.
9. 2015 AFP Payments Fraud and Control Survey, Underwritten by J.P. Morgan, March 2015.