Limiting the Use of the Social Security Number in Healthcare

Save to myBoK

With its unprecedented funding to support the effective implementation of health IT and health information exchange (HIE), the American Recovery and Reinvestment Act of 2009 has given new urgency to the need for a national health identifier. Because no unique personal identifier has been established, many providers have defaulted to the Social Security number (SSN) as a unique identifier.

This practice brief outlines the importance of accurate patient identification. It also provides guidance on limiting the use of the SSN in patient identification practices and outlines the unique identifier option.

The Importance of Patient Identification

Today, a single patient is likely to have a different identifier for every provider and organization from which he or she has received treatment. These multiple identifiers lead to inefficiencies along the continuum of care, including fragmented health records. In addition, confusion between the terms "personal identifier" and "ID set" can lead to inaccuracies.

A personal identifier is meant to describe a single attribute associated with an individual. In the absence of a personal identifier, a set of multiple attributes can be used to improve the accuracy of identification.

The process of accurately identifying patients is critical, because errors in identification can affect clinical decision making and patient safety, create risk to a patient's privacy and security, and result in duplicate tests and increased costs to patients, providers, and payers. In addition, one organization's patient identification errors will multiply exponentially within a health information exchange network.

Organizations therefore must develop, implement, and maintain practices that support accurate patient identification, including the following:†

- Obtain copies of a government-issued picture identification (such as a driver's license, passport, or official identity card) and insurance card each time a patient registers
- Develop a customer-friendly script for requesting patient identification and verification information
- Define a set of attributes that will be used consistently for patient identification
- Build effective business processes and quality checks with clear standards, policies, and procedures into patient identification activities
- Improve the accuracy of patient matching by collecting additional data elements such as mother's maiden name

HIPAA attempted to streamline patient identification by requiring organizations create a unique health identifier for every patient. However, in 1998 political and privacy concerns caused Congress to include a section in the Omnibus Appropriations Act that prohibits the Department of Health and Human Services from using federal funds to implement the unique health identifier requirement "until legislation is enacted specifically approving the standard."

In the ensuing 13 years, technology has advanced dramatically, and many of the privacy concerns surrounding the unique health identifier now can be addressed with technology and sound business practices underpinned by federal and state regulation.

Patient Identification's Effect on Data Integrity

EHR functionality, links within health systems, data sharing within a regional HIE, and the Nationwide Health Information Network all depend on the integrity of patient ID data. Accurate patient ID data are the basic building blocks of true interoperability. However, as data sharing increases, the integrity of the patient ID data decreases. In fact, systems with local controls often have more reliable ID data. Reliability decreases as a system expands to include multiple entry points, systems, and users. The growth of a system correlates directly with the increased risk to the accuracy of its data.

Impediments to the accuracy of the patient ID set can be attributed to:

- Lack of standardized data dictionaries with uniform conventions for handling data elements such as middle initials, titles (e.g., Reverend, etc.), hyphenated names, and suffixes
- Widespread use of nicknames
- Cultural mores that accept interchangeable names, inconsistent use of a mother's maiden name as a middle name, variation in name order, inconsistent spelling, naming multiple children in an extended family after the same person, and user provincialism (i.e., assuming that any unfamiliar name from a different culture is unique)

The results of compromised accuracy of patient identity can be minor or potentially catastrophic. In the paper record, errors are researched and accuracy verified against a relatively old paper source document. Electronic audit trails of data modification often have a short shelf life, precluding a comprehensive investigation. Data integrity issues include:

- Quality reporting errors if there is intermingling of total records or individual results and inaccurate care decisions based on incorrect information
- Obliteration of an existing patient record if the demographic information is changed to match the proof of ID of the incorrect patient
- Delayed reimbursement resulting from billing the wrong patient's carrier or jeopardizing a patient's credit if coverage is denied or the bill is sent to collection without ever billing the correct patient

Patient identification errors are often accidental, usually occurring at the point of registration. Historically, the HIM department has been responsible for merging potential duplicate numbers or separating records in the event two patients were assigned the same number. Verifying patient identity and correcting the paper record are arduous and not always effective.

In the EHR, correcting patient misidentification is often just as time-consuming and labor intensive for the following reasons:

- Not all downstream systems accept automated correction messages.
- Timing delays could lead to incorrect information in an integrated system overwriting corrections and perpetuating an error thought to have been corrected.
- Manual corrections are more reliable but often cumbersome and may not be timely.
- Electronic systems lack the appropriate functionality to handle deletions, even if the information is wrong or belongs to a different patient. Correction options include:
- A chronological entry stating an earlier entry is incorrect
- Suppression of the error but creation of a link to an earlier version that remains permanently accessible upon request

As a result of these data integrity concerns, there is a substantial need for accurate ID sets.

In December 2009, the Healthcare Information and Management Systems Society developed a white paper on patient identity integrity, available online at http://www.himss.org/patient-identity-integrity-white-paper. The document identifies nine key drivers for accurate identity management and can be used as a guide for implementing ID management activities.

Patient ID Implications for HIE

A remote system depends on the accuracy and controls of the initiating systems. Industry initiatives such as HIEs link patient information from various participating provider systems. As the healthcare industry becomes more computerized and connections are established across multiple disparate systems, challenges increase when matching to a specific and unique person for coordinating that person's healthcare records. The percent of master patient index (MPI) inaccuracies within each entity exponentially increases the number of errors in the HIE environment.

When dealing with patients in a face-to-face environment, incorrect information can be caught and corrected more easily. As additional remote systems are connected, the discovery and resolution of incorrect information becomes more difficult.

A unified record is required to permit true meaningful use of health information. In the absence of a national standard for patient ID, HIEs use a variety of methods to match incoming records to patients.

Common methods for matching patient information include deterministic matching and probabilistic matching or a combination of the two. The formulas used by different vendors vary, and each MPI may use different weights for the same data elements or even different data elements to determine the uniqueness of the patient. In addition, individual organizational electronic MPI configurations and settings may differ.

Since there is neither a standard matching formula nor a standard for the data elements to be used in matching, the results of these methods are not consistent.

The most common elements used in matching and linking patient information are name, date of birth, sex, address, phone number, and SSN (or partial SSN). These commonly are obtained for each patient. Each element has potential problems for accurately and uniquely identifying a person, including:

- Name changes
- Multiple people with the same name born the same day
- Incorrectly identifying sex due to typing errors or sex changes
- Frequent address changes
- Frequent phone number changes
- Use of full SSN is restricted, and multiple people share the last four digits

Providers and organizations should be diligent in their efforts to submit clean patient identification data to HIEs and should have appropriate processes in place for ensuring an accurate MPI. HIEs should also have processes in place to correctly identify patients and duplicates or overlays and correct them within their systems. Processes should be in place for communicating patient duplicates or overlays from the organization to the HIE and vice versa.

SSN as a Patient Identifier

Without a unique health identifier, the most common identifier used to link health information across multiple providers and settings traditionally has been the SSN. SSNs were first issued in the 1930s as a means to track and calculate retirement benefits. Today, however, the SSN has become a de facto national identifier.

The SSN's success as a stable and unique means of identification has led to its use as an identifier in many unanticipated areas such as employee and customer tracking, patient identifier for healthcare providers and health insurance records, banking, and utility service records. For a complete chronological list of SSN legislation, see appendix A.

By 2004, the role of the SSN had changed to the point that it had become universally identified as the single most powerful identifier in use in the United States.[1] Over the years, the healthcare industry has recognized the inherent risks of using the SSN as a patient identifier and has taken some security measures against identify theft.

The most common security measure in use for the healthcare industry has been to allow only those who have a job-related need full access to SSNs (e.g., registration and patient accounting). Some organizations may restrict access to the SSN further, such as limiting use, access, or display to the last four digits.

Although these efforts work relatively well within an organization, when patient information must be correlated across a region or nation, using only the last four digits of the SSN is not adequate to ensure correct patient identification.

The Case against the SSN

The SSN is used as an identifier for many personal financial resources. As such, when it is stolen, it puts a person at great financial risk. Identity thieves seek SSNs to assume identities and commit fraudulent activities such as accessing bank accounts, credit cards, utility records, or medical insurance.

In recent years, it has become increasingly easy to use SSNs for fraudulent purposes, partly because of extensive illegal sales of SSNs. "As long as criminals can buy a list of names and SSNs through an Internet auction, we will continue to be plagued by the consequences," stated Patrick O'Carroll, inspector general of the Social Security Administration.[2]

Exacerbating the problem of using the SSN as a patient identifier is the fact that patient registration staff typically ask for the SSN verbally and, if the staff do request the card, it contains no picture or biometric identifiers. This makes it essentially impossible to ascertain if the person using the card is the one to whom the card was issued.

In an effort to minimize public concerns regarding privacy and identity theft, the federal government and states have enacted laws to restrict the use and disclosure of the SSN. (For a list of federal and state laws, see appendix B and appendix C) Many third-party payers have also replaced SSNs with their own unique identifier, and the Federal Trade Commission has advised minimizing exposure of the SSN and recommends that organizations reduce access and display.

However, despite the federal government's activities to curtail the use of the SSN, Medicare continues to use the SSN as a patient identifier.[3]

The expanded use of the SSN beyond its original intentions supports the contention that a unique individual identifier is a powerful business need. It also provides cautionary lessons on how a national identifier may be used and abused. It highlights the limitations of the SSN for that use.

The Unique Patient ID Option

Another option to accurately identify patients is a unique patient ID number. According to a RAND study, creating a unique patient ID number for every person in the United States would help reduce medical errors, simplify the use of electronic health records, increase overall efficiency, and protect patient privacy.[4]

The healthcare industry and organizations such as the Joint Commission have long recognized the effect unique patient ID numbers will have on continuity of care, patient safety, information integrity, and accuracy. However, there continues to be a struggle between correctly identifying a patient's clinical and financial information and the risks to patient privacy that coincide with easy identification.

"Linking the wrong clinical information to a person can not only cause great personal harm to the patient, but also incur huge costs to the healthcare provider in correcting and mitigating the error," says Howard Anderson, executive editor of HealthcareInfoSecurity.com.[5]

The healthcare industry and organizations can balance these issues by working together and using technology that will assist in accurate patient identification such as biometrics.

The Unique ID's Effect on Patient Safety

A unique patient identifier would assist the healthcare industry in patient safety tracking and trending reports. Current industry reporting is limited to organization-specific data, which include the unique organizational patient ID number.

Standardization would assist in tracking a patient safety incident throughout the continuum of care, as the patient moves from inpatient treatment to possible rehabilitation care to follow-up with primary care or other physicians. This type of tracking and trending would assist the industry in understanding patient outcomes and the development of treatment protocols.

The Privacy and Security Implications of Unique Patient IDs

An ever-increasing number of informed patients are refusing to provide their SSNs for healthcare purposes because of privacy concerns. A unique healthcare identifier appears to be a simple solution to identify patients; however, it is controversial among some privacy advocates.

Failure to identify the correct patient may lead to various privacy concerns. For example, privacy breaches can occur if the wrong patient is billed, the wrong next of kin is notified in an emergency, or the wrong protected health information is sent in response to a request for disclosure. The challenge is to provide an accurate ID set that enables health information to be shared as required for patient care, accurate billing, and collaborative research but is secure from external corruption and access.

Modern universal identifier architectures have solutions that address these concerns. According to Barry Hieb, MD, chief scientist for Global Patient Identifiers, "One of the strongest reasons to adopt a uniform healthcare identifier is its ability to support privacy through the use of anonymous identifiers and anonymized data sets. This promises to enable a new era of patient control of the privacy of their clinical information through the creation of a standardized method to segregate and anonymize information in support of confidentiality and privacy."[6]

Various options to verify selection of a patient by using extended information are:

- Universal identifier
- Health system–specific medical record number
- Third-party payer-specific ID
- Biometric identifier

Best Practices for Limiting SSN Use

Current identity theft concerns, overuse of the SSN, attempts to curtail SSN use, and potential database security risks make a sound argument as to why the SSN is not acceptable as a patient identifier. However, the SSN historically has been collected as an adjunct constant for ID and in some cases actually used as the medical record number.

A RAND study provides additional support in limiting the use of SSNs in healthcare by reporting that "the most likely causes of false-positive errors are data-entry errors and use of an insufficient number of attributes in a statistical search for matches… Larger health record databases, such as those of a national or large regional network, almost certainly require a unique identifier to avoid false-positive errors."[7]

Many facilities already have made major conversions to limit SSN use and even eliminate its collection. Many major health plans have eliminated the need to collect it as systems are converted and patient identifications processes strengthened.

Realistically, it will take decades to cycle the SSN out of healthcare. In the meantime, organizations should take the following recommended steps to manage its use:†

- Organizations that are not currently using the SSN for identification purposes should not begin to do so.
- Organizations that collect the SSN for identity and record-linking purposes should establish a conversion plan to eliminate its collection and use. They should develop and train employees in other matching methods to reduce the organization's dependence on the SSN during the conversion process.
- Organizations that use the SSN for patient identification should limit its display to the minimum number of documents and screens necessary to accomplish its business use. They should further limit its display to the minimum number of digits necessary.

Notes

1. Social Security Administration, Office of the Inspector General. "The Realities We Face: Continuity Amid Change. April 1, 2004 thru September 30, 2004." Semiannual report to Congress. https://oig.ssa.gov/sites/default/files/semiannual/fall-2004sar042004102004.pdf.
2. O'Carroll, Patrick. Testimony before the Subcommittee on Social Security of the House Ways and Means, July 10, 2003.
3. Privacy Rights Clearinghouse. "Fact Sheet 10: My Social Security Number-How Secure Is It?" www.privacyrights.org/fs/fs10-ssn.htm#4.
4. Hildebrand, Richard, James H. Bigelow, Basit Chaudhry, et al. "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.html.
5. Anderson, Howard. "The Problems with Patient Identifiers." January 29, 2010. www.healthcareinfosecurity.com/articles.php?art_id=2071.

6. Hieb, Barry. "A Cost Effective Method to Create a Universal Healthcare Identifier System." *Electronic Journal of Health Informatics* 5, no. 1 (2010). www.ejhi.net/ojs/index.php/ejhi/issue/view/8.
7. Hildebrand, Richard, James H. Bigelow, Basit Chaudhry, et al. "Identity Crisis: An Examination of the Costs and Benefits of a Unique Patient Identifier for the U.S. Health Care System."

References

AHIMA. "Managing the Integrity of Patient Identity in Health Information Exchange." *Journal of AHIMA* 80, no. 7 (July 2009): 62–69. Available in the AHIMA Body of Knowledge at www.ahima.org.

AHIMA. "Reconciling and Managing EMPIs (Updated)." *Journal of AHIMA* 81, no. 4 (Apr. 2010): 52–57. Available in the AHIMA Body of Knowledge at www.ahima.org.

Comcast Finance. "Your Social Security Number May Not Be Unique to You." August 13, 2010.

Dimick, Chris. "Exposing Double Identity at Patient Registration." *Journal of AHIMA* 80, no. 11 (Nov/Dec 2009): Web extra. Available in the AHIMA Body of Knowledge at www.ahima.org.

Dimitropoulos, Linda L. "Privacy and Security Solutions for Interoperable Health Information Exchange: Perspectives on Patient Matching: Approaches, Findings, and Challenges." June 30, 2009. www.rti.org/pubs/fip_execsumm.pdf.

E-HIM Work Group on Patient Identification in RHIOs. "Surveying the RHIO Landscape: A Description of Current RHIO Models, with a Focus on Patient Identification." *Journal of AHIMA* 77, no. 1 (Jan. 2006): 64A–D. Available in the AHIMA Body of Knowledge at www.ahima.org.

Federal Trade Commission. "Security in Numbers ***-**-**** SSNs and ID Theft." December 2008.

Fernandes, Lorraine. "Addressing the Business of the Health Information Exchange." AHIMA's 79th National Convention and Exhibit Proceedings, October 2007. Available in the AHIMA Body of Knowledge at www.ahima.org.

Fernandes, Lorraine. "Patient Identification in Three Acts." *Journal of AHIMA* 79, no. 4 (Apr. 2008): 46–49. Available in the AHIMA Body of Knowledge at www.ahima.org.

Fernandes, Lorraine, and Michele O'Connor. "Future of Patient Identification." *Journal of AHIMA* 77, no. 1 (Jan. 2006): 36–40. Available in the AHIMA Body of Knowledge at www.ahima.org.

Fernandes, Lorraine, and Ron Parker. "Successful Health Data Exchange: Architecture, Practices and Operations Across the 49th Parallel." AHIMA's 78th National Convention and Exhibit Proceedings, October 2006. Available in the AHIMA Body of Knowledge at www.ahima.org.

Healthcare Information and Management Systems Society. "Privacy and Security Toolkit." http://www.himss.org/patient-identity-integrity-white-paper.

Mancilla, Desla, and Jackie Moczygemba. "Medical Identity Theft: An Exploratory Foundational Study." 2009 AHIMA Convention Proceedings, October 2009. Available in the AHIMA Body of Knowledge at www.ahima.org.

Office of the National Coordinator for Health IT. "Perspectives on Patient Matching: Approaches, Findings, and Challenges."

"VA, DOD Agree to Adopt Single Personal Identifier for EHRs." *iHealthBeat*, August 12, 2010. www.ihealthbeat.org/articles/2010/8/12/va-dod-agree-to-adopt-single-personal-identifier-for-ehrs.aspx.

Wheatley, Vicki. "Quality Impact of the Master Patient Index." *Journal of AHIMA* 79, no. 10 (Oct. 2008): 78–79. Available in the AHIMA Body of Knowledge at www.ahima.org.

Appendixes

- Appendix A: Chronological Order of SSN Legislation

- Appendix B: Federal Legislation Restricting SSN Use
- Appendix C: State Legislation Restricting SSN Use

Prepared by

Barbara Demster, MS, RHIA
Julie Dooling, RHIT
Lesley Kadlec, MA, RHIA
Susan Torzewski, RHIA
Ruth Walker, MIS, RHIA, CPHQ
Diana Warner, MS, RHIA, CHPS
Lou Ann Wiedemann, MS, RHIA, FAHIMA, CPEHR

Acknowledgments

Jill S. Clark, MBA, RHIA
Angela Dinh, MHA, RHIA, CHPS
Lynne Henderson, MHA, RHIA
Gwen Jimenez, RHIA
Monna Nabers, MBA, RHIA

The information contained in this practice brief reflects the consensus opinion of the professionals who developed it. It has not been validated through scientific research.

† Indicates an AHIMA best practice. Best practices are available in the AHIMA Compendium, http://compendium.ahima.org.

Article citation:
AHIMA. "Limiting the Use of the Social Security Number in Healthcare" *Journal of AHIMA* 82, no.6 (June 2011): 52-56.