Unique Patient Identifiers -- What Are the Options?

Save to myBoK

by Soloman I. Appavu

HIPAA has brought patient identifiers into the spotlight. But what's the best option? The author of a national study offers an overview.

Envision all of the players in the healthcare system—patients, providers, health plans, and payers. Now, envision all of the day-to-day processes these players need to perform using information about patients—operations such as delivery of care, support services, follow- up, preventive care, record keeping, and administrative processes such as verification of eligibility, coordination of benefits, billing, and reimbursement. To perform all of these operations, organizations need to be able to keep track of—and identify—patients.

This task isn't a simple one. Patients, for one thing, are mobile and are treated by multiple organizations. Different types of care—acute, long term, ambulatory, and so on—are available to patients in a system that includes numerous players, from doctors and hospitals to integrated delivery systems, managed care organizations, and pharmacies. And with the evolution of technology, patient information is commonly processed by computers at some point in the system.

In this increasingly complex and fast-changing environment, it is necessary to uniquely identify patients across multiple providers and to access information from multiple locations. Moreover, identifiers establish a comprehensive framework across the national healthcare system to facilitate information exchange, continuity of care, evaluation of quality improvement, outcome measurements, and population-based healthcare research.

Though the use of identifiers has been under discussion for many years, the issue was brought into the national spotlight with the passage of the Health Information Portability and Accountability Act of 1996 (HIPAA). This legislation, which generally seeks to establish a process to achieve national health data standards, specifically mandates the adoption of standards for patient identifiers.

Unique Patient Identifiers (UPIs)

Most healthcare providers already use some method of patient identification. Generally this consists of the use of a medical record number issued and maintained by a practitioner or a provider organization. This number is based on an institutional master patient index (MPI), and the numbering system is specific to the issuing organization.

Different provider organizations use different numbering systems. Patients may receive multiple medical record numbers, each issued by the organization that provided them care. These numbers provide unique identification only within an issuing organization. In addition to a medical record number, some organizations use a patient account number for billing and reimbursement purposes. Patient account numbers are unique to each patient encounter or visit to the provider. VA hospitals, Medicare, and the Department of Defense use Social Security numbers (SSNs) to identify patients.

These kinds of patient identifiers, which are unique only within a provider organization or a single enterprise, are inadequate to support an emerging system of healthcare that requires access to patient information across geographically dispersed provider organizations. To uniquely identify an individual across such multiple organizations, a reliable unique patient identifier is needed.

Industry Initiatives

Since the beginning of the decade, healthcare organizations have been addressing this critical issue. These efforts include:

- In 1993, the Computer-based Patient Record Institute (CPRI) created a work group to address the need for a unique patient identifier

- Organizations such as the Workgroup for Electronic Data Interchange, the American Medical Informatics Association, and the American College of Medical Informatics have called for action and published position papers

- In 1994, the American National Standards Institute-Healthcare Informatics Standards Planning Panel (ANSI-HISPP) created a task force to review options in this area

- In 1995, the American Society for Testing Materials released its "E1714 Standard Guide for Properties of a Universal Patient Identifier"

- Other organizations have worked to develop identifiers relating to providers, employers, health plans, and payers

- Twelve state governments and a number of private initiatives have emerged to develop a suitable unique patient identifier methodology

- AHIMA recommends the inclusion of UPI in the core data elements of the MPI

- Industry-wide initiatives such as MPI workshops, consortia initiatives such as OMG/CORBAMed Patient Identification Service, and standards organizations initiatives such as HL7 MPI Mediation highlight both the significance of a unique patient identifier and the industry's efforts to achieve it

In 1997, the author prepared, on behalf of the ANSI-Healthcare Informatics Standards Board (HISB), an inventory of available unique health identifier options for the use of the Department of Health and Human Services (HHS).

"An Analysis of Unique Patient Identifier Options"

In 1997, HHS commissioned a study to analyze the various patient identification systems available. The author conducted this nationwide study, which was released in December 1997.[1]

The study consisted of an analysis of the various unique patient identifier options available for use in healthcare. It aimed to be an objective analysis, examining industry requirements, analyzing different options, and looking at the needs of the industry as a whole. The study used four levels of criteria to analyze existing options, examining conceptual, operational, component, and functional aspects.

Finally, instead of recommending one particular option, the study concluded that the healthcare industry had two choices—to choose one option or create a new one. It did, however, conclude that an identifier of some kind was needed—an identifier that was simple enough for computers and humans to use easily.

This article presents a brief overview of the analysis described in the study.

Unique Patient Identifier Options

A number of unique patient identifier options already exist. They include:

1. *Enhanced Social Security Number* (ESSN)—Proposed by CPRI, ESSN adds several security features to the existing SSN, such as check digits, cleanup of existing errors, and customization for use in healthcare

2. *ASTM Sample Universal Healthcare Identifier* (UHID) Implementation—The sample UHID consists of a 16-digit sequential identifier, a "." that serves as a delimiter, a six-digit check digit, and a six-digit encryption scheme. Altogether, it consists of 28 numeric digits and a period

3. *Patient Identification Number based on Bank Card Method*—The initial proposal consisted of a 13- to 15-digit identifier with a set of digits to identify the practitioner or the medical group, another set of digits to identify payers, a

third set of digits to identify an individual, and check digits to control errors. The use of separate additional digits to identify conditions such as allergies or disease was also suggested

4. *Model Universal Patient Identifier based on Personal Immutable Properties*—The model consists of three universal immutable values plus a check digit. The three values are a seven-digit date of birth field, a six-digit place of birth code, a five-digit sequence code (to identify the individual born on the same date in the same geographic area) and a single check digit

5. *Lifetime Human Service and Treatment Record (LHSTR) Number based on the Birth Certificate*—This number would consist of a set of seven core demographic data elements, another set of longitudinal data elements to corroborate over time to protect against error or fraud, and a third set of data to identify the medical or social service record

6. *Biometric Identification*—Biometric identification consists of the patients' personal physical characteristics such as fingerprint, retina scan, iris scan, and voice and DNA analysis

Non-unique Patient Identifiers

These options are not unique identifiers in that they are only specific to the organizations that issue them.

1. *Medical Record Number*—This represents the current method of identifying patients and patient information. Each provider organization maintains an MPI, and a medical record number is issued and maintained through this index.

2. *Medical Record Number with a Provider Prefix*—This option adds a provider ID as a prefix to the medical record number discussed above.

3. *Cryptography-based Identifier*—Cryptography, the use of two keys that allow arbitrary messages to be encoded and decoded, plays a key role in this option. The two keys contain mathematical functions that are inverses of each other. The patient holds a patient private key and the provider organization holds an organizational (provider) public key. The two keys together generate IDs that are both organization-specific and unique to individuals.

Alternatives to Unique Patient Identifiers

These methods offer alternatives to unique patient identifiers, but they do not meet all the necessary criteria.

1. *Manual Process*—This process will require manual searching and verification of records and information; for many organizations, this is not feasible

2. *CORBAMed Person Identification Service*—Common Object Request Broker Architecture (CORBA) is the industry standard for object-oriented interoperability among disparate computer systems. This approach includes multiple levels of MPIs, using the interface definition language technology, which allows a program in one language to communicate with another program in an unknown language, to search and match patient information

3. *HL7 MPI Mediation*—Like CORBAMed, HL7 Mediation uses HL7 transaction standards to manage the searching and matching of patient information

4. *Directory Service*—A directory service system proposes to interactively reconcile the proper association of patient identification data at the current point of care with any one of the other prior points of care

5. *FHOP's Standard Data Set as Common Patient Identifier*—The University of California-San Francisco Family Health Outcomes Project (FHOP) recommends the use of standard data sets for the identification of patient information. FHOP's identifying data elements consist of two sets, namely core data elements and confirmatory data elements. Using object-oriented software technology, a string value is derived from these data elements, which is used as an identifier for searching and matching patient information

Method of Analysis

The HHS study analyzed each option using a two-step process. In the first step, the requirements for a unique patient identifier, including its characteristics, capabilities, components, functions, and use were analyzed. In the next step, each available option was analyzed individually. Four sets of criteria were used to analyze these options at four different levels:

- conceptual level—comparison with the 30 conceptual characteristics from ASTM's UHID standards guide
- operational level—5 operational characteristics
- component level—6 component requirements
- functional level—11 basic functional requirements

What We Learned

While it aimed to be an objective analysis, the study did offer several conclusions for the requirements of the universal patient identifier. These included:

A patient identifier is an integral part of patient care. The use of reliable patient identifiers is required for sensitive procedures, such as blood transfusion, invasive testing, surgical procedures, and medication administration. Identifiers are also routinely used for ordering and reporting the results of tests, procedures, and medications; coordinating multidisciplinary patient care delivery processes; and managing all administrative functions, such as scheduling, billing, or coordination of benefits.

A patient identifier is an integral part of patient information. Clinical documentation, including observations, results, diagnosis, procedures, medication, progress, and outcomes are based on the patient identifier. An identifier is vital for the management of automated information and manual medical record functions (e.g., compilation, filing, storage, retrieval, and communication). It is mandated as an integral part of the medical record by regulatory authorities.

Privacy, confidentiality and security do not preclude the use of unique patient identifier. In fact, a unique patient identifier can help enforce security by standardizing and strengthening access control and eliminating the repeated use of personal identification information. Additional measures to fully and effectively address privacy concerns include federal legislation, appropriate organizational policies and procedures, access control, audit trails for tracking access, public education, and continuous evaluation and improvement of these protective measures.

A unique patient identifier prevents exposure and protects patient privacy. A UPI eliminates repetitive use and disclosure of an individual's personal identification information (name, age, sex, race, marital status, place of residence) for routine internal and external communications (orders, results, medication, consultation) and protects the privacy of the individual. It also helps preserve patient anonymity while facilitating communication and information sharing.

Unique patient identifiers help standardize methods of accessing patient care information and protect its privacy and confidentiality. A UPI helps standardize methods of accessing patient care information and enables organizations to use a single point of access. The use of patient demographic information for identification increases the level of exposure and subjects patients to unnecessary privacy risks. Such nonstandard access methods are difficult to control and monitor and increase the potential for the violation of privacy and confidentiality of patient information. The single point of access and the standard access method enable organizations to plan and implement necessary access controls. A valid UPI provides the required focused control as well as timely and reliable access.

A judicious design can protect a patient's privacy and confidentiality. A UPI requires a design architecture that will keep the identification of patient care information and its access two distinct and separate functions within healthcare. The identifier's role is merely to identify the patient record, accessing only the identification segment of the patient record and not its content. Access control deals with the authentication of the user (e.g., validation of user ID and password), verification of access privileges, audit trails, physical security, etc. Organizational policies and procedures and federal legislation must supplement it.

Ongoing organizational measures are required to support patient identification and confidentiality. The judicious design discussed above must be supplemented by appropriate ongoing organizational measures to protect patient information. Fail-safe access control mechanisms, including software security, physical access security, encryption protection, and an authentication mechanism must be in place to prevent unauthorized access and ensure legitimate access. The recommended HIPAA security

measures include audit trails for tracking inappropriate access and preventive steps against possible misuse. These mechanisms must be evaluated on an ongoing basis and improved continuously.

Uniform federal/state legislation is required to protect the privacy and confidentiality of healthcare information. To ensure the privacy and confidentiality of patient information beyond organizational boundaries, uniform federal and state privacy and confidentiality legislation is necessary. Such legislation must protect the UPI from misuse and prevent unauthorized access to patient care information, illegal linkages, and discrimination based on patient information.

Multiple identifiers inhibit timely access. When multiple identifiers are used for the same patient, the information is fragmented and isolated and timely access to it is difficult for care providers in other locations—impairing timely delivery of care.

A UPI is made up of six critical components. These components work together as a system and support the UPI's basic functions:

- an identifier—can be based on a numeric or alphanumeric scheme

- identifying information—identifies a patient by matching his or her identification information. It usually contains permanent (unchanging) personal data such as name, date of birth, place of birth, mother's maiden name, etc.; a longitudinal data segment that contains corroborating information that occurs over the lifetime of a person such as address, SSN, profession, spouse, etc; a health service data segment with information that helps locate the individual's previous health records

- index—links the UPI and the identification information of the patient. It serves as the directory of UPIs

- mechanism to hide or encrypt the identifier—protection of the identity of a patient can be accomplished with the use of technology, such as encryption. Encryption provides protection when communicating sensitive information, such as HIV tests or other similar information

- technology infrastructure—in order to issue, maintain, and manage the UPI, a robust technology infrastructure that includes computer systems, a communication network, and powerful software applications is necessary

- administrative infrastructure—an administrative infrastructure to manage and control various functions relating to the issue, use, and maintenance of the identifier and the demographic database is necessary

The six identifier components are critical to the basic functions of a unique patient identifier. By itself, the identifier scheme can neither protect the privacy and confidentiality of patient information nor assure its accurate identification. These functions depend on the maintenance of current identification information, security measures such as access security and secure communication, and appropriate technology infrastructure. The remaining identifier components provide these capabilities and, in essence, give functionality to the identifier.

Development of technology infrastructure requires direction, support, and coordination. Alternatives to the UPI, namely CORBAMed, HL7, and Directory Service address the technology infrastructure, which is one of the five identifier components. The industrywide adoption of a UPI will help its development and capabilities.

Critical functions are independent of identifier scheme/value of the identifier. Critical functions such as access control, identification information, administrative and technology infrastructure, etc., are independent of the identifier's numbering scheme (i.e., the choice of UPI). These functions are not unique or proprietary to any particular UPI (numbering) scheme or value. They can be implemented with any one of the UPI options.

Check digits and encryption are common to all options. Check digits protect against transcription errors and ensure accuracy. They can support any numeric identifier. Encryption ensures storage and communication in a secure format. All identifier options discussed in this report can make use of this feature.

The Final Analysis

After the four-level evaluation of the possible methods, the study reached these conclusions:

- Non-unique patient identifier options (medical record number, medical record number with provider prefix, and cryptography-based identifier) do not adequately meet ASTM conceptual characteristics

- Alternatives to the UPI (CORBAMed, HL7, Directory Service, FHOP Standard Data Set, and Manual Process) are significantly noncompliant with the ASTM conceptual characteristics

- Options that did not comply with the conceptual characteristics also did not comply with the rest of the requirements, including operational characteristics, component requirements, and basic function requirements

- Of the five UPI options that fared well at the conceptual level, enhanced SSN is the only option that complied with operational characteristics and component requirements. The remaining four are not operational and remain as concepts. In addition, they did not meet the ASTM criteria "concise" and only partly met "usable"

- All of the UPI options (ESSN, ASTM Sample UHID, LHSTR number, personal immutable characteristics-based identifier, bank card method, and biometrics) are in general compliance with the ASTM conceptual characteristics, with the exception of the biometrics method, which does not meet seven of the 30 characteristics

- Of the remaining four, the sample UHID is a well-developed concept, followed by the LHSTR number and personal immutable character-based identifier. Even as a concept, the bank card method requires a significant amount of additional development

- The SSN is used for about 20 percent of the population as a UPI, and the Social Security Administration is evaluating options to enhance the SSN and fix its current problems

- The Florida Veterans Integrated Service Network is piloting a modified sample UHID as an internal control number (ICN). It is being used in conjunction with the SSN. The SSN continues to be the patient identifier (embossed, bar coded and included in the magnetic stripe of an ID card), since the ICN is too long for users to handle

- The medical record number with provider prefix proposal directs the focus away from patient identification to information identification. It designates the primary care physician as curator to track previous sites of care for an individual. Therefore, it neglects some of the basic functions of the UPI

- Alternatives to UPI address only one of its necessary components (e.g., technology infrastructure and identification information). CORBAMed, HL7, and Directory Service address the technology infrastructure/software solution and the FHOP option addresses data standardization

An Ideal Unique Patient Identifier

Examination of the available options reveals that, in general, they focus more on the identifier scheme component and less on other components. A careful overall analysis, however, reveals that in fact it is the remaining components, namely identification information, index, security protection, technology infrastructure and administrative infrastructure that give functionality to the identifier.

Critical functional elements, such as access control, identification information, and administrative and technology infrastructures, are independent of the numbering scheme (i.e., the choice of UPI). They can be implemented with any of the options. Therefore, a simple, user-friendly UPI that is suitable for use by both humans and computers constitutes an ideal choice for the UPI.

In addition, these critical functions do not depend on the identifier scheme but on other components. As a result, we can separate the identification scheme from all the other components. We can choose a simple and reliable identification scheme and equip it with all of the required functionality by adding the remaining five components.

Recommendations for the Adoption of Standards

HHS and the Health Care Financing Administration published a notice of intent in 1998 to address the UPI issue. However, the initiatives came to a halt when Congress passed legislation prohibiting HCFA from using any funds in 1999 to address the need for a UPI.

The issue continues to be controversial and in 1998 sparked numerous concerns from privacy advocates. It is unfortunate that those who are opposed to the use of UPI were unable to see that it actually protects the privacy, confidentiality, and security of patient information.

Non-unique patient identifiers are already in widespread use, and access to patient information is possible even without an ID. In fact, access through means other than a standard UPI presents a dangerously serious level of exposure. An unauthorized user can gain access to confidential patient information if access is not restricted to a nationally accepted standard method and if a patient's personal information is allowed for identification and access instead of an UPI. A UPI, on the other hand, can facilitate the elimination of all other nonstandard access methods and limit access only through a valid identifier. This, in turn, will allow provider organizations to focus on a single access point and strengthen its security with the appropriate authentication, audit trails, and controls.

Ultimately, a UPI eliminates the disclosure of an individual's personal information and helps preserve patient anonymity while facilitating patient care and communication. It is critical that the original intent of HIPAA, namely the adoption of a UPI standard, is not abandoned due to lack of understanding of the UPI, wrong perceptions, or misplaced priorities.

AHIMA's Position

The Health Insurance Portability and Accountability Act of 1996 mandates that the Secretary of Health and Human Services (HHS) adopt a unique health identifier for individuals. However, due to privacy concerns, the omnibus appropriations bill (HR 4328) for fiscal year 1999 contained a provision prohibiting funds to be used "to promulgate or adopt a final standard providing for a unique health identifier for an individual until legislation is enacted specifically approving the standard." As a result, there has been no activity within HHS on the selection of a unique health identifier.

A number of potential candidates for consideration exist, as this article outlines. AHIMA supports the use of the master patient index (MPI).

An accurate MPI, whether on paper or in electronic format, may be considered the most important resource in a healthcare facility because it is the link tracking patient, person, or member activity within an organization (or enterprise) and across patient care settings. The MPI identifies all patients who have been treated in a facility or enterprise and lists the medical record or identification number associated with the name.

AHIMA recommends that the following core data elements be included in MPIs:

- internal patient identification
- person name
- date of birth
- date of birth qualifier
- gender
- race
- ethnicity
- address
- alias/previous name
- social security number
- facility identification
- universal patient identifier
- account number
- discharge or departure date
- encounter or service type patient disposition

For definitions regarding these core data elements, see the practice brief "Master Patient Index—Recommended Core Data Elements" in the July-August 1997 Journal of AHIMA.

It is anticipated that these data elements should:

- accurately match persons being registered for care with their MPI record
- minimize duplicate records within a facility and across patient care settings
- facilitate merging MPIs to create enterprise MPIs
- facilitate access to longitudinal patient records

This will speed access to patient information, resulting in significant benefits for patients and healthcare providers.

Soloman I. Appavu is Director of Systems Planning at Cook County Bureau of Health Services in Chicago. He is also chairman of the ANSI-HISB Publicity, Education, and Information Standing Committee, co-chair of ANSI-HISB Ad hoc Committee on Unique Individual Identifier, and Chairman of the CPRI Committee on Unique Patient Identifier. He is also the author of the HHS report "Report on the Analysis of Unique Patient Identifier Options" and a consultant to NCVHS/HHS. He can be reached at Soloman_Appavu@compuserve.com*.*

Article citation:

Appavu, Soloman I. "Unique Patient Identifiers--What Are the Options?" *Journal of AHIMA* 70, no.9 (1999): 50-57.

Driving the Power of Knowledge