Important Considerations When Planning a National Healthcare Identifier

Barry Hieb, M.D., Global Patient Identifiers, Inc.

Introduction

In June 2019 the U.S. House of Representatives passed an amendment overturning a 21-year-old prohibition on federal funding in support of a unique patient identifier for healthcare. The amendment, co-sponsored by representatives Bill Foster (D-IL) and Mike Kelly (R-PA), deletes the text that prevents the U.S. Department of Health and Human Services from providing any resources to support the implementation of a unique healthcare patient identifier. This legislation must now be approved by the Senate and signed by President Trump prior to taking effect. However, just the fact that this legislation was passed by the House of Representatives ensures a renewed debate over the appropriateness of a unique healthcare identifier solution and specific approaches which might deliver the best solution.

Predictably, the initial focus of these discussions will be on how to make patient identification as accurate and cost-effective as possible. This is fitting since the proper choice of a unique healthcare identifier strategy will be key to achieving this primary goal. But the discussion cannot stop there. The choice of a specific implementation approach for a healthcare identifier will have a dramatic impact on many associated healthcare requirements. In this paper, we list many of those requirements. Some are obvious, others not; but all are important and must be addressed in order to ensure that any unique healthcare identifier project delivers maximum efficacy and value to all stakeholders. More details on specific topics can be found in the references at the end of this document.

Disclosure

In the interests of full disclosure, the author is the founder of and Chief Scientist for a not-for-profit company, Global Patient Identifiers, Inc (GPII). This company has developed a solution to the problem of patient misidentification, a solution that addresses each of the requirements listed in this paper. The author was also the primary contributor to two ASTM standards that were developed in the 1990s regarding the attributes of a National Patient Identifier and guidelines for its implementation.

Contents

Context

When the original Health Insurance Portability and Accountability Act (HIPAA) of 1996 was passed it included a mandate for the creation of an individual healthcare identifier. The goal of this feature was to make accurate identification of each individual possible for healthcare operations. Two years later Congress reversed itself and passed a prohibition preventing the expenditure of any federal resources toward this goal{[i]} based largely on concerns about privacy. For the past 21 years that prohibition has been included in annual federal legislation.

Based on this prohibition, healthcare has used a variety of other methodologies to help identify individuals who are presenting for medical care. By far the most common has been probabilistic matching based on patient demographic data. But a variety of other techniques including "referential" matching and biometrics-based approaches (fingerprints, facial scans, genetics, palm vein scans) have also been employed. Despite over two decades working to solve this patient identification problem, the results have been less than satisfactory. A recent article{[ii]} estimates there is a 20% patient identification error rate within an organization and as much as a 60% error rate between organizations. We must do much better than this.

The author believes that the best solution to the problem of patient misidentification is a hybrid of several existing and proposed solutions. No one solution will fully meet the challenges of our complex healthcare information management and technology infrastructure. For example, variations in identity proofing and authentication must be offered to engender essential trust of both patients and providers. There are many issues to be addressed; perhaps the most critical of which are patient privacy rights, recovery from inevitable identity theft episodes and data breaches, and support of current and future legislation like the European Union General Data Protection Regulation.

Requirements

Each of the requirements described below briefly documents issues that must be considered in the design of a national healthcare identification system. We maintain that these requirements must be addressed regardless of what implementation strategy is chosen for the final deployment of a unique healthcare identifier. For that reason, the analysis of each issue attempts to focus on the requirements to solve that issue rather than the solution that is incorporated into any particular solution. Additional information concerning the specific GPII solution is provided by the references.

Accurate identification

Providing patient identification with the potential for 100% accuracy is the foundational requirement for any proposed healthcare identifier system. It is widely acknowledged that many patient identification strategies, such as demographic data matching and biometrics, cannot ever achieve 100% accuracy due to realities such as errors in demographic data capture, "collisions" where two individuals have identical or similar data, technology constraints, and situations where needed data is not available. One of the key advantages of a unique healthcare identifier strategy is that it is largely immune from such problems. In an analysis conducted by the RAND Corporation in 2018{[iii]}, eleven approaches to improving record matching were reviewed. Only for the unique identifier approach did RAND assert "If adopted and used as intended, this solution would match records used by the same individual perfectly." This 100% accurate capability is the bedrock on which any solution must be based.

Errors

Any identification system, no matter how well designed, must deal with the potential for errors. Humans are fallible and they can cause errors to occur, whether intentional or accidental. There are many instances of unintentional errors such as typographical mistakes or insufficient available data. In addition, any patient identification system must deal with intentional errors such as impersonations, identity theft, and data breaches. The healthcare identification system must be designed to minimize these events but it must also acknowledge that no known system can prevent errors entirely.

Resilience

Because of the existence of errors, a critical requirement of any proposed national healthcare identifier system is its resilience. From an identity perspective, resilience is defined as the ability to *completely* recover from an identity error and restore the affected person's identity to wholeness. The ability to achieve this recovery must be simple, automated, inexpensive, under the control of the affected individual and able to be completed quickly to ensure delivery of healthcare is minimally impacted{[iv]}.

Privacy

One of the critical objections to the creation of a national healthcare identifier is that it might represent a threat to patient privacy. However, a properly implemented national healthcare identifier system must substantially strengthen currently available privacy capabilities. Properly implemented, an identifier system will empower each individual patient to create whatever privacy paradigm meets their current medical situation needs and then evolve that privacy as their clinical situation changes{[v]}. It is also possible to design such a system in a way that it eliminates the need for patient privacy consent documents – an approach that leads to dramatic improvements in simplicity, cost, error reduction, and patient trust.

Break the glass and BTG recovery

There are numerous examples in healthcare where the patient's desire for privacy must be balanced against the healthcare system's commitment to patient safety. A properly designed unique healthcare identification system will contain functionality such as "break the glass" (BTG) that permits approved medical personnel to override patient privacy constraints in instances of a medical emergency{[vi]}. In addition, the system must contain capabilities to terminate a BTG episode once the associated emergency has ended.

Anonymity

Paradoxically, a unique healthcare identifier must fully support the needs of the US healthcare system for anonymity. This is essential not only to support patient privacy but also for activities such as research, education, public health, etc.{[vii]}. Full support for anonymous operation will be a key characteristic that promotes patient trust and hence patient utilization of the unique identification system.

Longitudinal medical record

One of the primary goals of healthcare automation is to enable the creation of a longitudinal medical record that includes all relevant information concerning an individual patient, no matter where that information was generated or where it is stored. This implies that the system must have the ability to track all locations where information concerning an individual resides. Given a unique identifier system that can achieve 100% identification accuracy, it is possible to design an automated data location capability that directly supports the creation of a longitudinal medical record{[viii]}.

Interoperability

The current industry focus on interoperability requires a key supporting patient identification technology that makes the creation of a longitudinal medical record feasible by supporting accurate information exchange among independent healthcare sites. The unique healthcare identifier system must be aware of all the locations that have information on that individual. This in turn implies that the system must be equipped with a completely accurate data location function which, operating in conjunction with the healthcare system's interoperability capabilities, permit a longitudinal medical record or portions of a patient's medical record to be assembled in either batch or real time modes{[ix]}.

Voluntary and mandatory operation

Certain segments of the healthcare industry (e.g. finance) will wish to use a unique healthcare identifier in a mandatory fashion – each participant must be assigned an identifier. Other segments (e.g. healthcare practitioners) may wish to use a voluntary approach where each patient makes the decision whether to participate based on their understanding of the value the system offers in their particular situation. A properly designed unique healthcare identification system must be able to concurrently support both these voluntary and mandatory modes of operation{[x]}. This flexibility will enable each healthcare segment to choose a voluntary or compulsory deployment strategy based on its own unique needs.

Enrollment authentication

There is an emerging consensus that NIST IAL2 is the minimal level of authentication required to assign a healthcare identifier that enables its owner to access their own patient information. It must therefore be possible to incorporate this level of identity assurance in the (theoretically once-in-a-lifetime) enrollment process for a patient. However, there are many circumstances which may require a higher level of authentication or which may prevent achieving IAL2. The anticipated unique healthcare identifier system must be able to reliably support these varying authentication levels{[xi]}.

Registration

One of the most appealing aspects of a unique healthcare identifier is its ability to make patient registration fast, convenient, and error-free{[xii]}. Through the choice of appropriate patient-managed identifier tools, it is feasible to establish a uniform methodology for patient registration that is consistent across all healthcare entities but can work with whatever registration system(s) that site is using.

Not-for-profit

The unique healthcare identifier project must be dedicated to the goal of improving the entire U.S. healthcare industry. The project must be financially viable. But it must not be driven by profit motivations. Decisions within the system must be based on what is best for healthcare rather than what makes for the most profitable mode of operation.

Governance/stewardship

An important decision concerning the unique healthcare identifier project concerns how it will be governed. What organization or entity can be counted on to act solely in the best interest of healthcare over the next century? How will decisions be made and sustained in a manner that ensures that all participants in the healthcare system can maintain confidence that the system is being managed properly, effectively, and solely for the benefit of those who are participating in the system{[xiii]}?

Simplicity

In order to ensure correct and efficient operation, the entire healthcare identification approach must be as simple as possible. Not only does this dramatically improve the chance for success of the identification system, it also plays a significant role in helping patients and healthcare workers trust the integrity of the system. It must be completely clear to each individual participating in the system – as a patient or as a healthcare professional – how the identifier system operates to support their needs.

Abstract

The requirement that each healthcare identifier be unique argues strongly that each identifier must be abstract. Creation of a specific identifier cannot depend on any properties of the individual linked to that identifier. This “abstract” approach makes it possible to ensure that each identifier is unique and that the identifier can remain valid despite any changes in the information associated with that individual{[xiv]}. Once generated and assigned to a person, the unique ID can remain associated with that individual for life despite changes in address, changes in name, gender reassignment, etc.

Fraud

The design of the healthcare identification system must include the ability to eliminate fraud as much as is possible. It must not be feasible for a counterfeiter to create a counterfeit identifier that is accepted by the system as being valid. There must be no need for identifier validation software (e.g. a check digit algorithm) that must be distributed to client sites and hence be at risk of reverse engineering{[xv]}.

Security

Due to the sensitive nature of healthcare information, security must be a high priority in the design of the identification system. All communications within the system must be encrypted. Data at rest should be encrypted. *There must be no centralized database of patient identifiable information.* Even if the system were to be hacked, patient privacy must not be threatened and there must be no risk of a data breach{[xvi]}.

Rapid deployment

Creating a national unique patient identification system represents a major project for the nation. It must be possible for multiple healthcare organizations to participate in parallel implementation efforts, each at its own pace. Similarly, within an individual organization, individual patients should be able to easily subscribe whenever they need to obtain services from their healthcare provider. Medical staff effort required to enroll each patient must be kept to a minimum. Similarly, the effort required to repair an identity theft or a data breach must be minimal.

Scope creep management

A major problem with existing identification systems is that they are susceptible to "scope creep" – where a system designed to solve one problem is borrowed, adapted, stolen or expanded to address a different problem. Because of these activities, the identifier may not address the new problem adequately and may lose its ability to effectively solve the original problem it was designed to meet. The social security number (SSN) is a classic example of this. The new healthcare identifier system must contain capabilities to limit, manage, or otherwise address issues of scope creep. Specifically, it must be possible to ensure that the ability of the system to achieve accurate patient identification can be maintained over time.

Synergy with existing identification methodologies

Healthcare organizations have spent enormous amounts of time and money attempting to achieve accurate patient identification. It is critical that whatever new unique healthcare identifier system is deployed, it should not compete with these efforts but rather should synergistically enhance them in order to achieve a net result of completely accurate operation. The new identity paradigm must be able to work in conjunction with existing identification capabilities including demographic matching, referential matching, and biometrics{[xvii]}.

Missing (or erroneous) patient data

One of the Achilles' heels of the current demographics-based approach to patient identification occurs when portions of that demographic data are either missing or in error. This can lead to significant uncertainty about the accurate identity of the individual and this can result in both false negative and false positive matching errors. The design of a unique identifier solution for healthcare must include provisions that make it as robust as possible in the light of these problems. The use of an abstract identifier can be critical in this situation because it does not have any direct dependencies on patient data that may not be accurate or that may change over time{[xviii]}.

Longevity

The design of the entire healthcare unique identifier system must ensure that it can successfully operate for hundreds of years. The capacity of the identifier must be sufficient to ensure that, if desired, the world's population can be accommodated for many generations. The database structure must be sufficiently compact to permit permanent storage of identifier information concerning tens of billions of individuals. Equally important, the governance and management of the system must be able to remain focused on proper operation of the system for the long term. Once created, the unique identifier system should be permanently available to serve healthcare.

Language independence and international capability

A properly designed healthcare identifier must avoid dependency on alpha characters as part of the identifier{[xix]}. By using a numeric only design, the system can avoid ambiguities (e.g. the number zero versus the letter "o") and prevent confusion for clients who might be more comfortable with non-Roman alphabets. This promotes maximum clarity for those using the system and helps it to effectively serve clients for whom English is not their native language.

EUGDPR compatibility

The European Union General Data Protection Regulation represents a security and privacy rule that is having a significant impact on U.S. organizations{[xx]}. Care must be taken to ensure that any U.S. identifier project is fully compatible with the EUGDPR. It must be able to implement the "right to be forgotten" requirement. There appear to be many open policy questions about how the EUGDPR should be implemented within U.S. healthcare but the identifier implementation must be sufficiently flexible to be compliant with whatever policy is eventually adopted.

A new, standardized approach

Whatever implementation strategy is chosen for a unique U.S. healthcare identifier, it should be compatible with existing principles and standards{[xxi]}. This will help ensure a consistent and successful deployment across the widest possible spectrum of different healthcare organizations. If the chosen strategy represents a "new" approach this will help ensure a consistent and successful deployment, because there are no “legacy” installations that will need to be retrofitted to participate in the new system.

Flexible authentication

The primary function of the healthcare unique identifier system is, not surprisingly, identification. In order to fulfill its mission, that identification function must be uniform and consistent across all healthcare organizations. Authentication, however, is an allied function that may vary from location to location based on the capabilities and needs of each healthcare organization. Each organization must be able to make full use of whatever authentication techniques it trusts and has available{[xxii]}.

Support for children, infants, and fetuses

Regardless of the technique used to implement a unique healthcare identifier, it is critical that the chosen approach be universal. It must be possible to assign an identifier to <u>any</u> biologic entity that requires healthcare services. In particular, this means that the system must be able to serve children, infants, fetuses, and potentially individual zygotes{[xxiii]}. An inability to assign identifiers to members of any of these groups will risk failure of the entire project because of the need to create and maintain a separate identification methodology to operate in parallel with the healthcare identifier system.

Surrogates

There are many populations, notably the very young, the very elderly, and the very ill, where the assignment of a healthcare identifier may need to be accomplished using the assistance of a surrogate. In such instances it must be possible for the surrogate to fulfill all the identity and authentication requirements that would normally be directed towards a specific patient. It is also important to note that the need for a surrogate may include “temporary” situations such as a patient being incapacitated by a serious illness.

Sparse uniqueness

An important property of a unique healthcare identifier system is that the identifiers must exhibit “sparse uniqueness”{[xxiv]}. Any valid identifier must differ from any other valid identifier by at least three digits. This helps eliminate errors by making it impossible for a single typographical error to accidentally yield a different, but valid, identifier. Instead, such typographical errors will yield an invalid identifier which will be flagged by the system as invalid as soon as someone attempts to use it.

Identifier invalidation

There must be a mechanism for a patient or an authorized healthcare user to designate that a given healthcare identifier is no longer valid. This action must occur instantaneously and must be effective across all locations where that identifier has ever been used. This capability is particularly critical in situations that deal with identity theft and data breaches{[xxv]}. It is particularly useful if it can be paired with a “replace” function that allows an invalidated identifier to be replaced with a new one.

No identifier reuse

The requirement that each healthcare identifier be unique implies that no healthcare identifier must ever be reused. If, for any reason, an identifier must be terminated or replaced (for example, in the event of identity theft) then that identifier must be permanently disabled. Once an identifier has been disabled, any subsequent attempt to use it for healthcare services must be rejected{[xxvi]}.

Patient empowerment

Every patient that participates in the national healthcare identification system should do so because they believe it is in their own self-interest. Features such as the ability to choose whether to participate, tools to enable the creation of a longitudinal medical record, the opportunity to design and enhance an individual-specific privacy approach, and the ability to make changes (including disenrollment from the system) will all be critical to attracting and retaining participants. The entire identification system must be designed and maintained with a focus on patient empowerment. The ability to establish and maintain this focus will be one of the most important factors in ensuring the long-term success of the identification system.

Future-proofing

It is not possible to completely foresee the future requirements that might be placed on a unique healthcare identifier. Consequently, the design of the identifier and its supporting infrastructure must include the ability to expand and modify the operation of the system to meet unanticipated future requirements. The goal of this “future proofing” capability is to enable the maximum degree of flexibility for the system to accommodate requirements that are not currently foreseeable{[xxvii]}.

Conclusion

The recent action by the House of Representatives to rescind the prohibition for HHS to support a national healthcare identifier represents a significant inflection point. There is undoubtedly a long road ahead before such a system can be deployed. However, now there is at least hope that significant evaluation and planning discussions can begin. At GPII we believe that our experience developing a unique healthcare identifier system can be of great value in helping others understand some of the issues that must be addressed if the federal project is to be successful. We hope that the issues outlined in this document and the resources we have identified can contribute significantly to this discussion. We look forward to the opportunity to contribute to the dialog on this topic as the national discussion accelerates.

Summary

For over ten years Global Patient Identifiers, Inc. (GPII) has been dedicated to the challenge of developing a patient identification approach that could serve as a fully functional national healthcare identification system. The existing GPII system addresses all the requirements listed in this document and provides novel solutions for many of them. Documentation on how the system achieves those requirements is provided in a series of white papers that are included in the reference section. GPII hopes that this analysis eventually leads to the creation of a robust, durable, and effective healthcare identifier implementation for the country.

References

External references are listed in bold text. GPII materials are listed in plain text.
Most of the GPII materials are 3-7 page white papers that provide a brief discussion of the indicated topic. To obtain a copy of any of these white papers please contact Barry Hieb, M.D., bhieb@vuhid.org, or 520-320-6220.

[i] In 2014 the prohibition language read: **Sec. 510.** ***None of the funds made available in this Act may be used to promulgate or adopt any final standard under section 1173(b) of the Social Security Act providing for, or providing for the assignment of, a unique health identifier for an individual (except in an individual's capacity as an employer or a health care provider), until legislation is enacted specifically approving the standard.***

[ii] **Why the movement toward a patient identifier is only a start, Dan Cidon, Health Data Management, https://www.healthdatamanagement.com/opinion/why-the-movement-toward-a-patient-identifier-is-only-a-start.**

[iii] **Defining and Evaluating Patient-Empowered Approaches to Improving Record Matching, Rudin, et. al., RAND, August, 2018.**

[iv] Error and Fraud Mitigation using ***<prTag>*** Services, GPII Identity Theft and Data Breach Remedies, GPII Privacy Resilience, How to Deal with Identity Theft and Data Breaches, Resilience: The Story of Susie Smith

[v] Privacy Paradigm, GPII Privacy Implementation, GPII Privacy Classes, GPII Privacy Resilience, GPII Defined Privacy classes

[vi] Balancing Privacy and Safety, Ensuring Patient Safety Using GPII Capabilities

[vii] Anonymity in Healthcare, GPII Privacy Classes, GPII Privacy Resilience, Resilience: The Story of Susie Smith

[viii] The GPII Data Location Function, The role of GPII Patient Identification in Supporting Interoperability

[ix] The GPII Data Location Function

[x] Voluntary and Mandatory GPII Deployment Options

[xi] Security considerations in the GPII Patient Identification System, GPII Privacy Classes

[xii] "Identity First" Registration, GPII Identification Token, The role of GPII Patient Identification in Supporting Interoperability

[xiii] GPII Stewardship

[xiv] ***<prTag>*** Identifiers

[xv] Error and Fraud Mitigation Using ***<prTag>*** Services

[xvi] ***<prTag>*** System Technical Architecture

[xvii] GPII Synergy with Emerging Technologies

[xviii] Misidentification in Healthcare

[xix] ***<prTag>*** Identifiers

[xx] **https://www.google.com/search?client=firefox-b-1-d&q=general+data+protection+regulation+usa&sa=X&ved=2ahUKEwjvkbaenoPjAhWjMX0KHcJUDFcQ1QIoA3oECAsQBA&biw=1383&bih=770**

[xxi] **https://www.astm.org/Standards/E1714.htm**

[xxii] Biometrics and Patient Identification, “Identity First” Registration

[xxiii] Managing Children, Infants and Fetuses

[xxiv] Sparse Uniqueness in ***<prTags>***

[xxv] Error and Fraud Mitigation Using ***<prTag>*** Services, How to Deal with Identity Theft and Data Breaches

[xxvi] How to Deal with Identity Theft and Data Breaches

[xxvii] GPII Privacy Classes