Patient Identification in Interoperable Health Systems

A National Identifier is Only Part of the Answer

Several industrialized countries are investing heavily in a national health information infrastructure (NHII), including a national healthcare identifier, to support electronic health systems, with the goal being safer, more efficient and improved healthcare.

> “Achieving a complete view of a person’s healthcare history requires integrating data captured over time from the disparate processes, systems, architectures and frameworks of numerous providers and provider organizations.”

Executive Summary

The timely and successful implementation of a national healthcare identifier can be impeded by the lack of attention to three critical issues:

- **Ensuring legacy interoperability and accessibility**
- **Managing compliance, governance and privacy concerns**
- **Maintaining the highest level of information quality**

A national identifier, while important, is not the complete solution for health system interoperability and data exchange in clinical settings and across administrative domains. Four key challenges must be addressed for the successful implementation and maintenance of a national identifier that will also deliver interoperability:

- **Immediate return on investment (ROI)** – An identifier system can only be immediately useful when accurate data can be sought, found and used from all participating applications.
- **Transition support and migration strategy** – Interoperability and ongoing information quality must be ensured during the migration process, providing seamless access to all data, no matter where it is.
- **Data integrity** – Trust in the identification system is vital for its success, and nothing undermines trust more than inaccurate data.
- **Data governance framework** – Establishing and maintaining the permitted levels of access to sensitive information requires a governance framework to ensure data sharing, modification, security and privacy policies are harmonized across jurisdictions.

A national healthcare identifier must enable unique identification within a national interoperability framework suited to many stakeholders, systems and administrative domains. The critical success issues and challenges outlined are satisfied by integrating the national identifier with an enterprise master person index (EMPI), which is a specialized form of master data management (MDM). The EMPI is used to create an accurate, complete view of patient information from data dispersed across multiple facilities, application systems and databases to deliver a comprehensive picture of each patient in real time at all clinical settings. Integrating an EMPI with a national healthcare identifier will provide more effective management, reduce costs and risks associated with the identification of patients, and provide immediate ROI during the timely roll-out of the identifier and relevant framework while providing seamless interoperability across health delivery organizations. Overall, an EMPI bridges the gap between a national identifier and true clinical interoperability in healthcare.

Introduction

Several countries in the industrialized world are making substantial investments to deploy a national health information infrastructure (NHII). The infrastructure is designed to support electronic health systems such as an interoperable electronic health record (EHR), with the goal being safer, more efficient and improved healthcare, all of which are predicated on the ability to locate, exchange and share patient information accurately and quickly in the clinical environment.

With a more centralized health information infrastructure approach, a unique national healthcare identifier is issued to identify each patient in the system. Traditionally, national identifiers were only used by administration systems for such activities as claiming payments. Extending the use of the national identifier to support patient care functions requires specific considerations based on lessons learned from countries around the globe.

Critical Issues in Implementing a National Healthcare Identifier

The timely implementation of a national healthcare identifier supporting both clinical and administrative initiatives can be hampered by the lack of attention to critical issues, including ensuring legacy interoperability and accessibility, managing compliance, governance and privacy concerns, and maintaining the highest level of information quality.

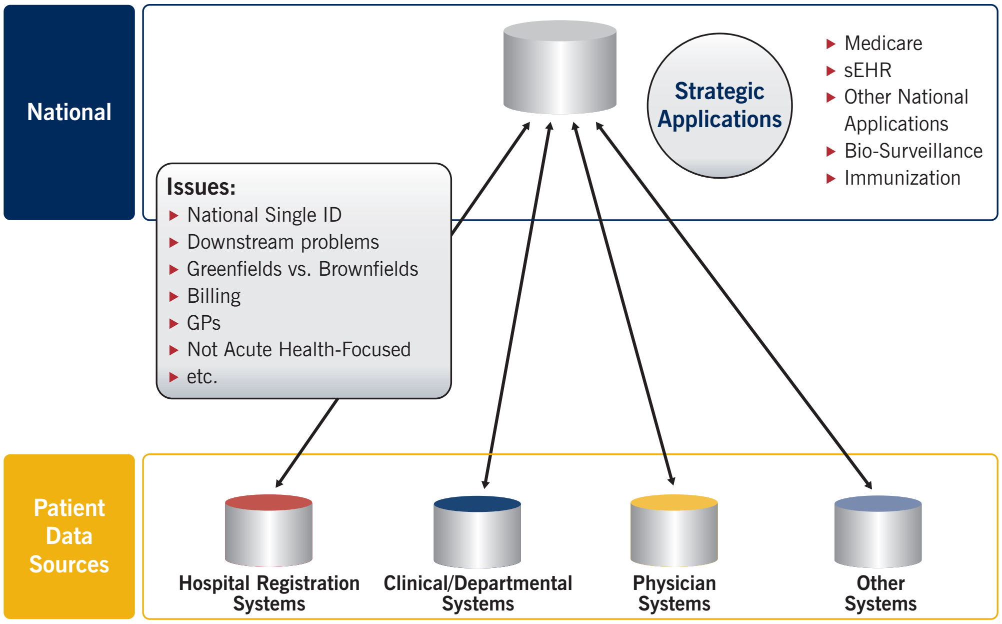
Legacy Interoperability and Accessibility

Achieving a complete view of a person's healthcare history requires integrating data captured over time from the disparate processes, systems, architectures and frameworks of numerous providers and provider organizations. There are millions or possibly even billions of existing medical records already indexed using current facility-level or regional identifiers. Migrating the data and processes employed by these existing systems while simultaneously maintaining the ongoing full operation of the existing systems poses the most significant challenges of actualizing the national identifier infrastructure.

For the new identifier system to be immediately useful and thus widely accepted, records from the myriad of systems need to be linked via each individual's identifying information. The national identifier must encompass incorporating services associated with the data record life cycle, namely the creation, update and retirement of patient data through the national infrastructure. All of this must take place while the existing systems continue to support ongoing healthcare delivery!

At the very least, all participants must:

- Modify their numerous systems to synchronize directly with the national identifier framework
- Replace all existing identifiers with the newly assigned national IDs, or augment records with the new ID
- Update systems so that the life-cycle functionality is aligned with the national ID infrastructure, which could include new data fields
- Integrate data quality management processes to support the needs of the federated community.

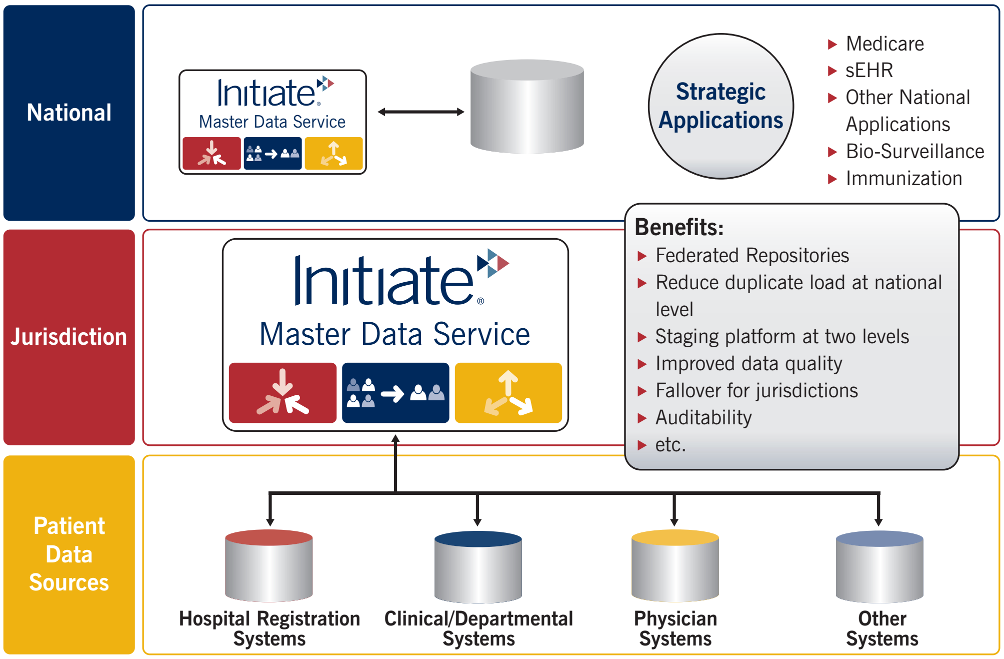


The impact of these tasks and their potential cost to existing operational systems is staggering. Creating and issuing a new identifier without planning for this enormous transition will lead to the same kinds of issues that drove the introduction of the national identifier in the first place. And during this transition, what will ensure that all the data that is available is actually accessible? And do the participants need to wait until the long transition is completed before any of the benefits of the national identifier can be realized? Employing MDM technology provides a framework that can immediately realize the benefits of the national identifier while providing a scalable and configurable environment for a smooth transition.

It should also be noted that not all legacy health information systems will be able to store and manage the new identifier. However, since these systems will likely not be "ripped and replaced" they still need to participate in data sharing, and they need a mechanism for obtaining the national identifier from either existing identifiers (a crosswalk) or demographic identification.

A successful migration to a national identifier depends on coordinating continued operations with the transition to the national infrastructure, requiring that:

- The use of an identifier must be complemented with additional identifying data and technology that facilitates search and use of all relevant data across all systems and data sets
- Existing records must be accurately correlated and assigned the correct new ID, ensuring that local systems are synchronized with the national identifier. This is best managed in a hub-style federated registry system architecture that reflects the underlying organizational network hierarchies in a way that does not force the owners of thousands of legacy systems to make costly (or perhaps even impossible) changes to their existing structures.
- Access to legacy information must be supported even in environments that may be destabilized by changing the underlying data models.
- During the transition period, current processes and applications that rely on existing identifiers must coexist with the national identifier to prevent duplication of effort and lost information.



Policies, Compliance and Governance

Creating a national identifier requires carefully examining the relevant policies governing privacy, security, sharing and distribution to ensure compliance. These policies, defined at the national, jurisdictional and facility levels, coupled with privacy and confidentiality laws, oversee how and what information may be collected, and to whom it may be disclosed. Of course, the combination of policies and their implications differs significantly across jurisdictional boundaries. Further complicating the matter, for example, when data originally from jurisdiction A is displayed at jurisdiction B, which jurisdiction's policies take precedence?

To ensure authentication and authorization, the use of a unique individual or provider identifier is not sufficient to guarantee against misuse or unauthorized access. Trust, quality, privacy, security, opt-in/ opt-out and linkage – all of these are aspects of healthcare information whose governance requires monitoring and oversight of role-based authentication and authorization.

Auditing of identification data is critical: knowing where records are created, by whom, the validations that were performed, the data's provenance, and quality checks all contribute to traceability. Also, the absence of the audit capability poses significant challenges to exception management and issue resolution.

A national identifier program is not sufficient to govern compliance to the numerous policies defined across a federated landscape. It must be bolstered by methods and capabilities that can document, manage, enforce, govern and report compliance to all defined policies. This requires that:

- The national solution must have a framework for managing the hierarchy and prioritization of policies as they exist across all administrative domains
- Security and access management must be fully integrated at the national level including mechanisms for identifying, authenticating and authorizing individuals while enabling role-based access to sensitive or private data
- Traceability and activity logging are needed to provide viable audits and to support reporting and analysis

- The national identifier system should be the logical repository for access information and must provide compliance services along with patient identification
- Corresponding application systems supporting the national identifier must be flexible to adapt rapidly to support and conform to policy changes

Information Quality

Trust in the system is vital for success. Nothing undermines this trust faster than poor or inaccurate data. The process for issuing identifiers must guard against duplicates and provide robust search capabilities against normal data variations. The system must have a mechanism for propagating new or modified information and must rely on high quality information while imposing data quality requirements. The very objective of a national healthcare identifier is to access current and accurate health information associated with the correct person – nothing less should suffice.

The consolidation of healthcare information within a national identification framework hinges on the ability to confidently locate and match patient information in sub-second response times. Yet as specific data elements are stripped and coalesced into a single identifier, the opportunities for introducing flaws into the system increase, ultimately leading to less safe and effective healthcare.

Relying on a number that is intended to act in the role of both identification and authentication leads to a false sense of security. The larger the number of processing points, the more difficult it becomes to isolate the introduction of data flaws. *The quality of information is best managed at its origin; replication of identifying information is impacted by the inherent lack of synchronization across copies, leading to missing, inconsistent and potentially the kind of inaccurate data that may jeopardize lives.* Considering the critical healthcare dependence on high quality information introduces these implications for any national identifier framework:

- The framework should not solely rely on one data item for identification; instead, a collection of identifying attributes should contribute to unique identification
- Reducing the copying or replication of data from its source will reduce opportunities for introducing error and inconsistency
- Problem resolution often requires manual intervention; the infrastructure must provide operational and production tools that streamline and monitor the workflow for manual correction processes

Implementation of a National Identifier Combined with an EMPI Can Deliver Interoperability

A national identifier is a critical component of nationwide interoperability and data exchange, but it is not the complete solution. Global experience points to four key challenges that must be addressed to achieve interoperability. These challenges include:

- **Immediate ROI** – For a new identifier system to be immediately useful and thus widely accepted, millions, or even billions, of existing medical records need to be identified and linked.
- **Transition support and migration strategy** – Not all legacy health information systems are able to store and manage new identifiers. Quickly sharing health information or an EHR across a network of participants requires knowing which systems store the data, along with enough identifying information to locate the requested data within legacy systems that cannot accept the new identifier.

- **Data integrity** – Trust in the identification system is vital for its success. Nothing undermines trust more than inaccurate data. The processes for issuing identifiers must guard against compromising unique identification of an individual. In the clinical environment, search capabilities must be robust against normal data variation, including missing data, and the system must be able to propagate new or modified information immediately. Processes must also exist to notify downstream systems of changes to the national identifier and demographic data.

- **Data governance framework** – Establishing and maintaining the permitted levels of access to sensitive information requires a governance framework. The national system needs to maintain and enforce data sharing and data modification policies that are harmonized across multiple jurisdictions.

To ensure a national identifier actually functions as desired, the central authority must have the power to assign and maintain identifiers across the network of participants, at facility, regional, or national levels. In doing so, accurate data can be sought, found and used from all sources while supporting the integrity of the identifier. A central authority can also ensure security and access management controls are in place – along with supporting processes – to protect sensitive data.

All of these requirements can be satisfied by integrating the national identifier framework with an enterprise master person index EMPI, which is used to create an accurate, complete view of patient information from data dispersed across multiple facilities, application systems and databases to deliver a comprehensive picture of each patient in real time at all points of service. The use of an EMPI also offers additional benefits, including increasing the percentage of payment transactions that can be processed without manual intervention, delivering new capabilities to detect fraud and abuse, and providing a foundation for research and analytics which can be the basis of pay for performance and proactive health management plans which reduce healthcare costs over time.

Addressing these issues and integrating these suggestions will provide more effective management while reducing costs and specific risks associated with the identification of patients in the health system. In addition, these suggestions will ensure the timely roll-out of the identifier and relevant framework so that initiatives such as the EHR and interoperability across health delivery organizations do not have to wait ten or more years for the foundations to be in place.

About Initiate Systems

Initiate Systems, Inc. enables organizations to strategically leverage and share critical data assets. Its Master Data Management (MDM) software and experience as an information exchange leader provide organizations with complete, accurate and real-time views of data spread across multiple systems or databases, even outside the firewall. This allows agencies to unlock the value of their data assets for competitive advantages or operational improvements. Initiate Systems operates globally through its subsidiaries, with corporate headquarters in Chicago and offices across the U.S., and Toronto, London and Sydney.

For more information, visit www.InitiateSystems.com.

United States

Chicago
+1 312 759 5030

Initiate Systems - Austin
+1 512 634 5111

Initiate Systems Government Operations
+1 703 904 4344

Initiate Systems - New York
+1 646 673 8551

Asia Pacific

Initiate Systems Australia Pty. Ltd.
+61 (0) 2 8061 3800

Canada

Initiate Systems Canada Inc.
+1 416 213 8999

Europe, Middle East and Africa

Initiate Systems UK Ltd.
+44 (0) 118 925 3322

Initiate | Know your data.
Trust your data.