5 Tips for Successful Patient Identity Management in Government Agencies

Valuable lessons on how government agencies successfully automate and integrate patient-centric systems

HEALTHCARE INSIGHT SERIES
About this Report

**Patient Identity Management** is a critical function for healthcare-related federal and state government agencies.

Through the tips in this report, administrators and practitioners will gain key insights into how state and federal government agencies successfully automate and integrate patient-centric systems while building effective and efficient healthcare-related operations.

**NorthPage Research** produces independent publications and online guides to help strategic decision makers.
5 Tips for Successful Patient Identity Management in Government Agencies

➢ Don’t Reinvent the Patient Identity Management Wheel
➢ Automate Patient Identity Management Integration and Delivery
➢ Align your Patient Identity Management Architecture with your Agency’s Needs
➢ Find and Fix the Sources of Compromise to Patient Data Quality
➢ Make Data Integration the Enabler of Patient Identity Management
EXECUTIVE SUMMARY

Federal and state government agencies pay over half of US formal health-care costs as employers and through Medicare, Medicaid and state-level programs. Through policies, regulation, direct involvement and budget allocation, government agencies increasingly shape the US health-care system. Additionally, as employers and health-care providers, government agencies build and implement healthcare systems, employ vast numbers of healthcare practitioners and treat millions of patients.

Central to all government agency healthcare activities are patients and the requirement to accurately and appropriately identify, handle, treat and track them. To do this well, Patient Identity Management is critical to agencies’ ability to link all patient-related information within and across systems and the healthcare ecosystem.

Given the size and complexity of public sector patient-centric information requirements, government agencies face challenging Patient Identity Management deployment scenarios because the agencies:

- rarely have control of the patient identity data capture process,
- receive data generated by many different provider master patient indexes containing data filled with inconsistencies, and
- have no control of the interfaces through which provider databases deliver patient record data.

Since an important function within healthcare-centric government agencies involves the exchange of patient information between independent entities, these issues create significant additional points of stress on each agency’s ability to effectively maintain their systems and provide required levels of patient data integrity.

A solid identity management foundation produces a range of benefits to patients, healthcare providers, payers, regulators and other stakeholders. These benefits include reducing the risk of medical errors, lowering healthcare costs, reducing fraud and limiting healthcare identity theft. For these reasons, a Patient Identity Management infrastructure needs to become a foundational element of every patient-related agency information system.
## Government Agencies with Significant Patient Identity Management Requirements

<table>
<thead>
<tr>
<th>Federal</th>
<th>State/Local</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administration on Aging</td>
<td>Behavioral Health Programs</td>
</tr>
<tr>
<td>Center for Disease Control and Prevention</td>
<td>Children’s Health Insurance Program</td>
</tr>
<tr>
<td>Child Welfare - Administration for Children &amp; Families</td>
<td>Department of Health and Social Services</td>
</tr>
<tr>
<td>Department of Agriculture</td>
<td>Fiscal Agents</td>
</tr>
<tr>
<td>Department of Justice</td>
<td>Medicaid</td>
</tr>
<tr>
<td>Federal Health IT Initiative: NHIN (National Health Information Network)</td>
<td>Special Supplemental Nutrition Program for Women, Infants and Children</td>
</tr>
<tr>
<td>Food &amp; Drug Administration</td>
<td></td>
</tr>
<tr>
<td>Health and Human Services</td>
<td></td>
</tr>
<tr>
<td>Health Resources and Services Administration</td>
<td></td>
</tr>
<tr>
<td>Indian Health Service</td>
<td></td>
</tr>
<tr>
<td>Internal Revenue Service</td>
<td></td>
</tr>
<tr>
<td>Medicare and Medicaid Services (CMS)</td>
<td></td>
</tr>
<tr>
<td>Military Health Systems</td>
<td></td>
</tr>
<tr>
<td>National Cancer Institute</td>
<td></td>
</tr>
<tr>
<td>National Health Information Network</td>
<td></td>
</tr>
<tr>
<td>National Institutes of Health</td>
<td></td>
</tr>
<tr>
<td>National Vaccine Program Office</td>
<td></td>
</tr>
<tr>
<td>Office of Managed Care</td>
<td></td>
</tr>
<tr>
<td>Office of Personnel Management</td>
<td></td>
</tr>
<tr>
<td>Social Security Administration</td>
<td></td>
</tr>
<tr>
<td>Veterans Affairs</td>
<td></td>
</tr>
<tr>
<td>Women, Infants and Children (USDA)</td>
<td></td>
</tr>
</tbody>
</table>
The Top Reasons Why Patient Identity Management has become a Critical Success Function for Government Agencies

1. There continues to be explosive growth in the amount of patient data that is being produced and exchanged electronically.

The amount of healthcare data and the number of patient information systems that provide and consume patient-centric data double every eighteen months.

2. The significant increase in the number and types of Patient Identity-related laws and regulatory requirements.

Government agencies must comply with, implement and in many cases oversee mandates for patient information-related transparency, privacy, disclosure, handling and documentation.

3. The tremendous potential for dramatic gains that can be achieved by all constituents in the healthcare ecosystem by implementing patient identity-centric systems, policies and processes.

The Patient Identity “Multiplier Effect”, the impact of one accurate and accessible patient record successfully distributed and leveraged throughout a healthcare ecosystem, is profound. Information can now follow the patient, while artificial obstacles including technical-, bureaucratic- and business-related need no longer act as barriers to the seamless exchange of information.

4. The need for agencies to demonstrate progress on patient-centric programs to justify current and proposed levels of funding.

Patient-centric programs are highly visible and represent key components of every healthcare-related agency’s objectives and measures of success.
The Top Reasons Why Patient Identity Management has become a Critical Success Function for Government Agencies, continued


Stakeholders have expanded beyond traditional healthcare providers; they now include payers (government, private and self-insured), employers, consumers, and the broadest reaches of the public and private health sectors.


Increasing scrutiny and pressure continues to mount for government agencies to securely and effectively manage, share and secure patient identity information.
Don’t Reinvent the Patient Identity Management Wheel

**WHY**

A vast collection of Patient Identity- and agency-specific resources, tools and knowledge exists and is available to help agencies more rapidly deploy effective Patient Identity Management models, methodologies, processes and systems. While no two agencies are exactly the same, taking advantage of core Patient Identity Management principles, best practices and lessons learned allow for accelerated implementations, reduced levels of project risk and greater functional success.

Agencies cannot afford to start Patient Identity Management implementations from scratch. By adopting an iterative Patient Identity Management approach that builds on a solid system and process foundation, agencies will deliver currently needed functionality while providing the extensibility required for supporting future projects and initiatives.
Don’t Reinvent the Patient Identity Management Wheel (continued)

HOW

Leverage the vast collection of Healthcare- and agency-specific Patient Identity Management resources to efficiently provide reliable, high-quality patient identity functionality in your agency:

- Adopt best practices and proven business processes
- Establish efficient organizational and staffing models
- Mandate Provider, Exchange and Agency integration
- Adopt and integrate standards
- Leverage established architectural, data and deployment models
- Implement rigorous patient data security, compliance and governance models
- Require Data Quality and Master Data Management integration including using pre-built patient data transformation maps
- Study and leverage the Patient Identity Management use cases of peers and other agencies
- Engage proven Patient Identity Management-focused experts and solution providers
TIP

Automate Patient Identity Management Integration and Delivery

WHY

Automation is critical to government agencies’ ability to successfully handle the explosive growth in the amount of patient data being produced and exchanged. Patient information is fragmented across many independent databases that use different identifiers.

The primary agency-centric Patient Identity Management-related functions that hold substantial automation potential are:

- Integration of internal and external patient data
- Use and delivery of original, aggregated and processed patient data

Automation enables high volume, secure data transfer and integration while lowering maintenance costs and enabling efficiencies.
Automate Patient Identity Management Integration and Delivery (continued)

HOW

Typical “must have” Patient Identity Management functionality for government agencies.

STEP 1 – INTEGRATION

- When data is created and stored across disparate health information systems and databases, data validation, transformation, integration, and cleansing must all play critical roles in and across your effective patient data management initiatives.
- Build to obtain a single view of patients across large data volumes and distributed providers.
- Centralize data management and access across stovepipe applications and information sources.
- Implement defined cross-referencing functionality to map identities across different domains.
- Implement integrated data repositories to integrate with the broad government initiatives including the Nationwide Health Information Network.
- Patient record matching is challenging but critical for uses including:
  - Public Health/Administrative reporting
  - Outcomes management
  - Vital status determination
  - Research
  - Clinical care
- Ensure that integrated patient data supports the broadest set of inter- and intra-agency applications and administrative systems.
- As policy makers, ensure integration and access to patient data are broad in scope to ensure optimal decisions are made during the build, deploy, run and upgrade system lifecycles.
Automate Patient Identity Management Integration and Delivery (continued)

STEP 2 – DISTRIBUTION

- Securely and reliably deliver patient-centric data to employees, citizens, first responders, healthcare providers, and other agencies.
- Standardize patient data for public health information networks including regional providers, exchanges and inter-agency networks.
- Deliver trusted patient data to support better decision making and planning.
- Provide the data delivery infrastructure necessary to disseminate and distribute data in an efficient and reliable way.
Align your Patient Identity Management Architecture with your Agency’s Needs

WHY

Creating an open and accessible data sharing architecture that is patient-centric is crucial to the success of computerizing healthcare-related applications in government agencies. The following Patient Identification Challenges have created a reliance on demographic information to clearly differentiate and properly identify patients:

- Lack of State and National Unique Patient Identifiers
- Provider reluctance to store and share Social Security numbers and other patient-specific information
- Lack of biometric data collected and transmitted that uniquely identifies patients

As a provider or aggregator of patient information, government agencies must put considerable emphasis on implementing a sound Patient Identity Management architecture to enable successful patient information flow and usage.

Accurately identifying patient records becomes exponentially harder as the size of the patient population and the number of patient information sources grows.
Align your Patient Identity Management 
Architecture with your Agency’s Needs 
(continued)

HOW

• An agency’s underlying Patient Identity Management platform must be flexible and secure while enabling seamless links to clinical and administrative documents and images across heterogeneous source systems.

• Invest heavily in your agency’s design, choice and implementation of Patient Identity Management architecture. Agencies’ operational and analytical systems that are developed without due consideration for Patient Identity Management become virtually impossible to re-architect after the fact for patient identity-centric capabilities.

• Architectural flexibility is critical. Patient Identity Management systems in government agencies must allow for a variety of architectures, including a database model, a federated model and those using record locator services. The system must support multiple frameworks as the agencies’ ecosystems have a variety of constituents with vastly different systems and evolving patient identity frameworks.

• Evaluate the need for real-time patient data integration and monitoring at the architectural level. While not currently a requirement for most agencies, real-time functionality is achievable and increasingly valuable for patient-centric operations, reporting and analyses.

• There are no ideal patient identity architectures, only best principles and practices for specific use cases.
TIP

Find and Fix the Sources of Compromise to Patient Data Quality

WHY

Poor Patient Identity Management processes cannot be offset by the best of technology. Failure to establish accurate patient identity at the original point of information capture results in all subsequent business processes being seriously hindered. Establishing incorrect medical record associations compromises all associated systems and data and ultimately requires correction.

Failure to identify and remediate the causes and sources of “dirty” patient data – whether introduced by the patient data producer or facilitator – compromises agency effectiveness.

Effects of “Dirty” Patient Data

- Incorrect association of patient medical record data to a different patient’s record
- Intermingling of two or more different patients’ records
- Health jeopardizing treatments administered to the wrong patients
- Electronic health records becoming fragmented and polluted by conflicting data
- The ability to accurately analyze patient-centric information and trends is compromised
Find and Fix the Sources of Compromise to Patient Data Quality (continued)

HOW
Agencies must avoid or remediate the following sources of compromise to patient data quality:

ORGANIZATIONAL
- Lack of priority given to Patient Data Quality
- Lack of understanding and appreciation for how compromised patient records negatively impact all associated electronic data, services and transactions
- Lack of organizational commitment to accurate patient identification
- Entrenched impressions of the difficulties associated with accurate patient identity as being ‘unsolvable’ problems
- Unclear or improperly implemented patient information confidentiality and privacy policies

IMPLEMENTATION
- Costs of sufficient Patient Identity Management systems, training and resources
- Poorly defined Patient Identity Management business processes
- Insufficient capture and analysis of patient identity errors including failure to perform Master Patient Index data reconciliations
- Lack of patient data quality standards
Make Data Integration the Enabler of Patient Identity Management

WHY

The patient data integration function is responsible for patient data acquisition from clinical, operational and reference systems in addition to the corresponding transformation of source data into actionable, reliable data for specific use within an agency.

Government agencies are often at the mercy of the quality of data delivered by sending organizations including healthcare providers, exchanges, insurers and other government agencies. Integrating and adapting to the challenges inherent in properly handling external patient data sources is a function-critical requirement for successful agency operations.

HOW

Proper patient data integration design is critical, starting with the types of integration needed to run an agency’s application. Patient data integration models in government agencies are typically applied in one of two ways:

1 – Deterministic Integration

Pursuing answers to known questions through available data sets. In this type of integration, finding reliable sources from which to pull needed fields into a database designed for the application is of principle importance. Operationally-related projects such as payment, patient eligibility and status are typically approached in this way.
Make Data Integration the Enabler of Patient Identity Management (continued)

2 – Probabilistic Integration

Probabilistic integration aims at understanding the power of data “at large” when a number of data sources of varying reliability are to be utilized. For projects requiring this approach, goals can be vaguely defined as “find correlations” and “discover new knowledge” via various data mining techniques. Projects of this kind are focused on determining what data exists, how reliable the available data are, and what additional data are required to enable systems to answer complex interdisciplinary questions. Broad projects such as epidemic outbreak studies are typically approached in this way.

The patient data integration model and the processes and tools used by your agency depend greatly on the type of data integration required.

Patient Data Sources

Pay great attention to the quality, availability and reliability of patient data sources. Profile each data source to determine

- Levels of trust: Can the source be considered authoritative?
- Acquisition: What data acquisition methods can be used?
- Integration: How can source data be meaningfully integrated with other source data?
- Source environment: Federated, Centralized or Hybrid?
- Meta-information: Security model, availability, usage rights and restrictions
- Levels of Data Quality: What are the source’s error / problem rates?

Patient data integration “nirvana” is approached when integrated data sources have no dependencies, no limitations and no need for manual intervention.
WORKS CITED


AHIMA e-HIM Work Group on Regional Health Information Organizations (RHIOs). “Using the SSN as a Patient Identifier.” Journal of AHIMA 77, no. 3, March 2006

AHIMA. "Managing the Integrity of Patient Identity in Health Information Exchange", Journal of AHIMA 80, July 2009


TERMS AND CONDITIONS

While the information is based on best available resources, NorthPage Research LLC disclaims all warranties as to the accuracy, completeness or adequacy of such information. NorthPage Research LLC shall have no liability for errors, omissions or inadequacies in the information contained herein or for interpretations thereof. Opinions reflect judgment at the time and are subject to change. All trademarks appearing in this report are trademarks of their respective owners.