

A high priority for improving the quality of healthcare delivery is development of effective Electronic Health Records (EHR) systems. Already in progress for many healthcare organizations is the initial step of digitizing and aggregating information from a variety of sources. A significant challenge exists in creating accurate and manageable information stores from scores of data sources: automating the determination of whether two sets of medical records are in fact referring to the same person before they are added to a master patient index (MPI). False positives and false negatives during this process can hinder effective treatment and even cause preventable medical errors.

Patient Master Identity Management (PMIM) is an identity-focused solution based on patented technology selected by the U.S. Department of Homeland Security to screen domestic airline passengers for terrorist threats. PMIM aggregates information from multiple disparate data stores to form a clear, composite depiction of the identity of an individual. It applies sophisticated Similarity Search™ and clustering techniques to resolve identities and establish an index from multiple sources without requiring the extensive cleansing required by other approaches.

BUILDING ON MASTER DATA MANAGEMENT (MDM)

Healthcare IT departments are attempting to address EHR challenges with MDM, but MDM platforms need to be extended to effectively manage identity information about people and other entities involved in healthcare systems.

Identity resolution enhances MDM with the ability to apply, update, reuse, and retain resolved identities. As traditional MDM solutions seek to cleanse and normalize data, they remove data that either is valuable or may become valuable in the future. PMIM manages identity information by providing a single view of an identity without the need to combine and destroy data. As new identity information becomes available, PMIM's active repository will be able to unlink identities that were once linked and/or create new linkages that were previously undetectable.

PMIM EXAMPLE

Two individuals with exactly the same name and address are likely to be combined by current MDM/CDI solutions, in effect "losing" one of the records. PMIM scores these two records as having a very high likelihood of being the same identity but does not discard either record. Later, when subsequent data about the identity is added to the data record that shows that one individual has a birth date of 1-23-64 and the other has a birth date of 2-5-88, it becomes clear that the two identities represent two separate individuals with a likely parent-child relationship.

Enriching MDM for Patient Master Identity Management

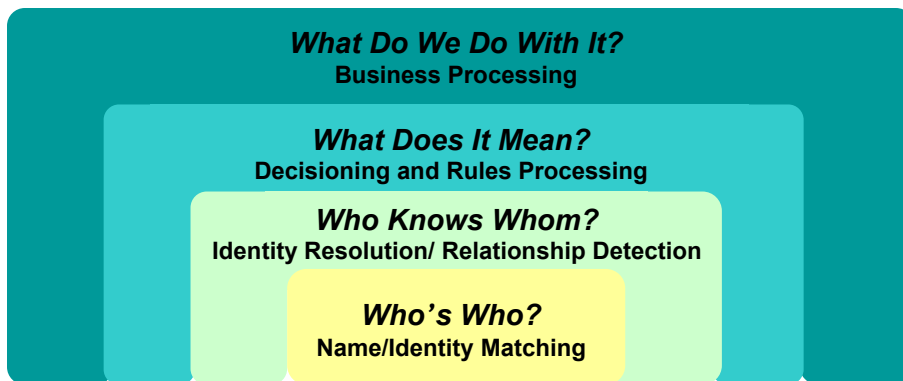
PMIM adds the following identity-focused capabilities to MDM:

- **Context Building** – Saves resolved identity information across time, preserving all information about that identity, including multiple instances of attributes (e.g., names and addresses) and references to source records.
 - Provides a persistent identity to which additional information can be related.
 - Provides persistent relationships to which additional information can be related.
- **Annotation** – Adds and retains incremental information about a resolved entity. Preserves history and enables information sharing and collaboration.
- **Scalability** – Scales to handle data sources representing in excess of 300 million records while maintaining high standards for performance.
- **Linking/Relationships** – Automatically detects relationships among data sources of interest and persists them. Authorized users can enhance them or add new relationships generated from external sources.
- **Secondary Searching** – Discovers hidden or indirect relationships among entities. Automated discovery graphically depicts relationships for easy decision-making.
- **Federated Identity Management** – Manages entities across various departments as well as across organizations.
- **Audit Log and Reporting** – Provides a comprehensive audit and report of all identity resolution transactions in order to comply with HIPAA privacy and compliance requirements.
- **Collaboration** – Allows teams to share information through integration with leading software packages such as Microsoft SharePoint.
- **Integration** – Allows easy integration into existing infrastructures and new solutions through open interfaces based on web services standards and message queues.

PMIM LEVERAGES IDENTITY RESOLUTION ENGINE™ (IRE) SECURITY

Balancing the need to resolve identities is the need to ensure that the information is used responsibly so that each individual's right to privacy is protected as prescribed by HIPAA regulations. IRE was designed to protect the privacy of data and to ensure its secure transmittal. IRE's security features support privacy protection policies while allowing an organization to maintain responsibility for enforcement (e.g., allowing or denying the secure transmittal of confidential information). Like other features within IRE, users are able to configure security features to control their actions based upon the requirements for a specific implementation:

- ◆ Search can be configured to return a similarity score without returning the associated data.
- ◆ Search can be configured to return top scores by target type with full document details and scores, document locators and scores only, or top scores only.
- ◆ Details used to derive relationships can be hidden while still exposing valuable information (e.g., this record should be combined with another identity previously encountered).
- ◆ Organization-specific decisioning rules/policies can be written and incorporated into the decision-making process.



Resolving identities quickly and accurately using identity resolution has already led to better decision-making in multiple industries, including financial services and insurance, government, retailing, and transportation. Now the same identity resolution technology is being applied to solve challenges in healthcare.

Unique Capabilities

Similarity Search

- Patented Similarity Search algorithms far exceed exact match/fuzzy logic capabilities to uncover previously hidden identity relationships
- Detects misspellings and typos or intentional data manipulations to reduce false negatives
- Unique ability to apply Similarity Search across multiple attributes to disregard irrelevant matches and reduce false positives

Multi-Database Access

- Identity analysis performed across multiple, disparate data sources
- Expand the breadth of analysis by uncovering matches and relationships within data regardless of the type or physical location of the data source
- Ability to incorporate commercial data sources and also validate identities

Flexible Integration

- Designed to quickly integrate with MDM solutions to provide advanced identity-focused analysis and results

Infoglide Software Corporation

6500 River Place Blvd. Building II, Suite 101, Austin, Texas 78730
512.532.3500 • Fax: 512.532.3505 • www.infoglidsoftware.com