Department of Veterans Affairs

Health Information Governance

Data Quality/Business Product Management

IAM Identity Management Business Requirements Guidance

Version: 2.6

May 2013

Revision History

Date	Revision	Description	Author
10/14/2009	1.01	Initial draft, incorporating April 2006 version 1.0	Business Project Management Team
11/10/09	1.02	Made additions per additional PSIM research and discussion with Pat and Colleen. Mapped enterprise requirements to use cases, began fleshing out pattern descriptions, added references and applicable regulations.	Business Project Management Team
12/17/2009	1.03	Added more information about Primary View.	Business Project Management Team
1/2010	1.04	Added information about Person Search.	Business Project Management Team
2/2010	1.05	Added additional information about Person Search.	Business Project Management Team
3/2010	1.06	Made changes per Jill Scheppler review.	Business Project Management Team
3/15/2020	1.07	Additions for guidance on displaying identity data. Also added placeholders for additional sections in this document.	Business Project Management Team
5/21/2010	1.08	Added guidance to ENTR listing (section 3), also made the table into an appendix.	Business Project Management Team
7/2/2010	1.09	Team review changes	Business Project Management Team
7/12/2010	2.0	Completed team review changes; added contact info for readers who have additional questions.	Business Project Management Team
1/5/2011	2.1	Began editing document to refer to VA and not just VHA; corrected list of requirements; clarified required search traits.	Business Project Management Team
2/2/2011	2.2	Minor corrections to list of requirements.	Business Project Management Team
3/17/2011	2.3	Included updated instructions on accessing the ERR	Business Project Management Team
7/21/2011	2.4	Additional guidance on local searches; replaced search grid with updated authority scores.	Business Project Management Team
7/01/2012	2.5	Reviewed/clarified materials on search; added update to reference UAT SOP; checked links; clarified document text and sample screens.	Business Project Management Team
5/9/2013	2.6	Added new search grids and updated pattern information.	Business Project Management Team

Table of Contents

1 Introduction

1.1 Purpose

The purpose of this document is to provide overall guidance on Veterans Administration (VA) Identity Management enterprise implementation requirements. This document provides a "road map" to be used by application development teams to help them understand, plan for, and implement identity management requirements so that their projects can proceed and make their deliverable dates, confident in having met these important requirements.

VA Identity Management business requirements are managed by the VHA Office of Health Information Governance (HIG) Data Quality/Business Project Management (BPM) team. The BPM team acts as the IdM business sponsors along with Healthcare Identity Management (HC IdM). For further information, please contact:

- Sara Temlitz, Manager, Business Project Management, sara.temlitz@va.gov
- Alice Cave, Program Analyst, Business Project Management, alice.cave@va.gov

Please contact Sara and Alice if you see anything that can be improved in this document. We consider this to be a "living" document and continually strive to improve it.

1.2 Audience

This document is written for requirements analysts, program and project staff, and developers responsible for projects where identity management functionality is used.

1.3 Definition of Key Terms

Refer to Identity Management Service (IdMS) Master Glossary for key identity management terms and concepts.
http://tspr.vista.med.va.gov/warboard/ProjectDocs/CommonServices_PS_v2.0/Identity_Management_Service_Master_Glossary.pdf

1.4 Identity Management Guidance and Legislative Background

The following regulations and laws are applicable to identity management applications:

- VA Identity Management Policy, VAIQ 7011145, June 28, 2010
- VHA Directive 2009-021 Data Entry Requirements for Administrative Data
- VHA Directive 2006-036 Data Quality Requirements for Identity Management and the Master Patient Index Functions (currently in review)
- VHA Directive 2007-037 Identity Authentication for Health Care Services
- VHA Handbook 1050.01 National Patient Safety Improvement Handbook
- VHA Handbook 1907.1 Health Information Management and Health Records
- VHA Handbook 1907.05 Repair of Catastrophic Edits to Patient Identity
- Joint Commission National Patient Safety Goals- Goal 1- Improve the accuracy of patient identification

1.5 References

The following documents were consulted during the development of this document:

- Identity Management Direction for HealtheVet VistA, Version 1.0, Identity Management Data Quality, VHA OI Health Data Informatics, April 2006 (http://vaww.vhaco.va.gov/dataquality/identitymgmt.htm
- Master Patient Index (MPI) Austin User Manual, Version 1.0, original publication April 1999, Updated October 2011 http://www.va.gov/vdl/application.asp?appid=16

- Identity Management Data Quality Enterprise Use Cases (http://vaww.vhaco.va.gov/dataquality/identitymgmt.htm)
- All Identity Service (IdS) Use Cases, Supplementary Specifications, and other Requirements documents http://tspr.vista.med.va.gov/warboard/anotebk.asp?proj=1385&Type=Active
- Healthcare Identity Management Compliance Request #20071102, Business Requirements Document, June 2011, http://tspr.vista.med.va.gov/warboard/ProjectDocs/MVI/VA%20IAM%20BRD%20v1.pdf
- Identity Management Services (PS/MPI) Business Rules Document, Version .3, June 2012 http://tspr.vista.med.va.gov/warboard/ProjectDocs/MVI/Common_Business_Rules_Document.pdf
- Identity Management Enterprise Level Requirements http://tspr.vista.med.va.gov/warboard/ProjectDocs/MVI/Enterprise-Level%20Identity%20Management%20Requirements.pdf

2 Identity Management Requirements in the Software Development Lifecycle

2.1 Statement of Problem

All legacy and new development projects must implement VA Identity Management functionality consistently. Failure to do so will potentially result in serious consequences such as patient safety issues, delays in claims processing, and application re-work and schedule delays.

Initially, some applications were released that did not meet the approved Identity Management requirements. There were a number of reasons for this: some project teams were unaware of the requirements, or did not have an adequate understanding to appropriately or consistently include the specific Identity Management functionality as stipulated in the requirements.

This document is a roadmap to identity management requirements compliance in the hopes of avoiding these problems in the future.

2.2 Importance of Proper Identity Management Requirement Implementation

It is imperative to have the correct, authoritative identity data to ensure the integrity of Veteran information as well as to avoid patient safety and claims issues. Patient safety issues that can arise when a patient's identity is mistaken include:

- Improper treatment provided
- Incorrect medications administered
- Incorrect medical decisions made
- Incorrect eligibility/enrollment actions taken

Claims issues that can arise in the case of mistaken identity can include:

- Payments going to the wrong persons
- Processing delays and/or lost benefits

Note that under no circumstances can the Identity Management data be proxied by any system other than the Identity Service (IdS).

2.3 Which Projects Need Identity Management Functionality?

Projects need identity management functionality when the project will:

- Provide person search capability
- Add a new person record

- Add a correlation for a person to a site or system of interest
- Update person records
- Respond to Link messages (to resolve duplicates)
- Change a person correlation (resolve mismatch)

The BPM Team is available to consult on these requirements and guide this process throughout the development cycle.

2.4 What is the Identity Service (IdS)?

The Master Veteran Index (MVI) is the Identity Services product comprised of the Master Patient Index (MPI) and Person Service Identity Management (PSIM).

The Master Veteran Index (MVI) holds over 18 million unique patient identity entries, populated from all VA facilities nationwide. The MVI matches/links system records together across the VA systems. The MVI also establishes a unique Enterprise Identifier for each of the VA unique person records; the identifier is called Integration Control Number (ICN).

Master Patient Index (MPI) is a component within Master Veteran Index (MVI) that supports Legacy data quality activities. It is the national VA patient index located at the Austin Information Technology Center (AITC) composed of a unique list of patients and a current list of Veterans Affairs Medical Centers (VAMCs) where each patient has been seen. This enables the sharing of patient data between operationally and regionally diverse systems. Each record (or index entry) on the MPI contains a small amount of patient data used to identify individual entries.

MVI's mission is to uniquely identify a person and to "link" that person's data throughout the VA facilities and corporate databases using the Integration Control Number (ICN). The MVI is the authoritative source of a person's ICN, the enterprise-wide identifier for a veteran and the key to accessing a patient's record. The accuracy of patient information and patient identification directly affects clinical, administrative, billing, and interdepartmental processes such as eligibility data sharing between Veterans Benefits Administration (VBA) and Veterans Health Administration (VHA).

PSIM enumerates and maintains person identities of patients, synchronizes identities with VistA during transition from Legacy VistA to HeV; maintains a history of ID changes; correlates the Integration Control Number (ICN) to internal and external identity domains; provides duplicate prevention and resolution tools; initiates identity link and unlink activities; and provides a data quality management user interface.

3 Identity Management and the Software Development Lifecycle

Identity Management requirements need to be considered from the very beginning of the software development lifecycle, and continuing through user acceptance testing. This applies equally to new development, Class III to Class I conversions, and COTS projects, across any and all software development lifecycle frameworks.

3.1 Requirements Phase

Identity Management requirements need to be considered from the very beginning of the software development lifecycle. This applies equally to new development, Class III to Class I conversions, and COTS projects, across any and all software development lifecycle frameworks. For example, during the VHA Requirements Analysis and Engineering Management (RAEM) New Service Request (NSR) lifecycle, Identity Management requirements are called out in the appendix to the template of each

Business Requirements Document (BRD). Use of this Identity Management Business Requirements Guidance document expands on the instruction provided in the BRD appendix.

3.1.1 Accessing the Enterprise Requirements Repository

Cross-cutting enterprise requirements are managed by VHI SE&I Enterprise Requirements Management, using an IBM Rational ReqPro Repository. Identity Management requirements are stored in this repository. Guidance documents and information on how to access the repository are located at: http://sharepoint.vista.med.va.gov/sites/enterprise_requirements_management/default.aspx To access Identity Management Data Quality requirements, follow the instructions to log in to ReqPro, and then follow these steps:

1. Log in to Rational Requisite Pro.
2. Go to 01-Enterprise -> views -> Stakeholder Views.
3. Right click on Stakeholder Views.
4. Select Create View.
5. Select Attribute Matrix and select Row Requirement Type as 'ENTR: Enterprise-level Requirement.
6. Click on Filter.
7. Enter a name for the view.
8. Select 'Save View' if you'd like to save it; otherwise, the view will not be saved for viewing at a later time.
9. Enter the number of rows per page; by default, 10 rows are displayed per page.
10. Under 'Export View to CSV', uncheck requirement name (if it is checked).
11. Select the 'Show' check box for attributes 1 through 21.
12. For the Keywords attribute, select 'Includes' from the drop down list; enter Person Identity Management in the text box next to it.
13. For the Submitter Name attribute, leave blank.
14. For the RM Status attribute, select 'Selected Values' from the drop down list; enter REVIEWED in the text box next to it.
15. For attributes Traced-From & Traced-To, select Requirement Types as 'ENTR: Enterprise-level Requirement.
16. Click the 'Submit' button to see the requirements.
17. The applicable requirements will be listed and can be exported as needed.

3.1.2 Roadmap to Further Requirements Detail

The requirements as listed in the repository are very high-level requirements. Appendix A maps the requirements to further instruction toward meeting those requirements. Use cases developed for use in the IS development process should be reviewed by project teams for background. IdMS use cases are located on this link:

http://tspr.vista.med.va.gov/warboard/anotebk.asp?proj=1385&Type=Active

Studying these use cases will provide insight on IdMS enterprise requirements and processes.

3.2 Design Phase

Design artifacts for projects employing the IdMS should be reviewed and approved by the IdMS technical staff.

3.3 Testing Phase

Identity Management business users expect to perform user acceptance testing after development testing is accomplished. The BPM team will need to take part in test case development and user acceptance

testing efforts in these cases:

- Implementation of a new integration with Identity Services
- Implementation of new features to Identity Services
- Implementation of any new use of Identity Services

Complete details are published in the BPM Team's standard operating procedure for user acceptance testing. This standard operating procedure is published at this link:
http://vaww.vha.vaco.portal.va.gov/sites/HDI/DQ/WebDQPublicFolder/Business%20Product%20Management/SOP%20-%20BPM%20User%20Acceptance%20Testing_May2013_updated.pdf

4 Identity Management Patterns

VA has implemented standard methods for integrating applications and systems with Identity Services. The standard methods preserve the integrity of the identity, as well as VA's ability to maintain the identity and record linkages in support of the longitudinal person record.The Identity Management implementation pattern is identified collaboratively by the IdS technical team along with input from the business and from consuming application project staff, based on technical, architectural, and business concerns. The pattern is important for determining the implementation plan necessary for successful integration with IdS. The pattern defines the data elements to be stored, messaging required, testing requirements, etc. Identification of the IdS pattern must be completed and approved by IdS before any development related to identity management takes place. There are several patterns that can be employed when integrating with IdS.
Patterns are fully documented in the MVI Service Description document at http://tspr.vista.med.va.gov/warboard/ProjectDocs/MVI/MVI_Service_Description.pdf.

5 Primary View Business Rules

Some of the use cases discussed in section 3.1.2 reference Primary View business rules. These are enforced by the MVI when user updates are received via HL7 messages. The following is a brief overview of what analysts and developers need to know about primary view rules. A flowchart that outlines the Primary View Update process follows at the end of this section.

5.1 What is the Primary View?

The Primary View is considered to be the enterprise "gold copy" of a Veteran's identity record, that is, it is the best collection of identity traits known about a Person among all the sites at the VA where that Person has been seen. The Primary View Profile is referenced in VA information systems by an associated ICN. The Primary View can be utilized by consuming applications to provide the most accurate identity data about a Person.

When an update is made to Primary View traits, the changes are promulgated to every system of interest to which the identity record is correlated. The term "systems of interest" refers to VA facilities that have seen patients and entered them as entries onto the MVI.

5.2 Why does a Project Team Need to Know about the Primary View?

Project teams working on an application that adds, updates, or otherwise manipulates data about patient or non-patient person identity will need to ensure that their application does not allow any conditions that will violate the Primary View rules. If the rules are violated, the IdMS will reject the addition or update. For identity data, these rules govern conditions about how identity can be added or updated, for example,

the following are some of the update rules for Last Name:

- If the incoming Last Name is blank then reject
- If Last Name contains numbers then reject

For applications that have a user interface, project teams would need to ensure that the interface does not allow Last Names to contain numbers or to be blank.

Primary View rules are maintained by the Data Quality Business Product Management group. Note that these rules also take into account authority scoring, as described in section 5.4.

5.3 What is a Catastrophic Edit?

One of the conditions MVI checks for when it receives an update, is whether an update would be considered a potential erroneous or catastrophic edit. A potential catastrophic edit is when two of the following attributes about a person are changed, thus possibly changing the identity of the person:

- First Name/Last Name
- Date of Birth
- Social Security Number
- Gender

Changes to the Name component (Last Name and/or First Name) are considered one edit for purposes of the Catastrophic Edit rules.

The following types of edits are exceptions to the rules for the SSN and Date of Birth fields in which they are not flagged as Potential Catastrophic Edits:

- **SSN:** Changing from a Null or Pseudo SSN to an SSN does not constitute a catastrophic edit.
- **Date of Birth:** Changing an imprecise to a (more) precise Date of Birth does not constitute a catastrophic edit. Examples of Imprecise and Precise Date of Birth values include the following:
  - Imprecise—Only the year (e.g., 1956)
  - More Precise—Include month and year, (e.g., 01/1956)
  - Precise—Include month, day, and year (e.g., 01/07/1956)

If MVI receives an edit it determines to be potentially catastrophic, an exception will be generated and manually processed. If it is determined that a catastrophic edit has occurred, the HC IdM team will work with the consuming application to correct the data issue, notify management of the occurrence and ensure staff has received the mandatory catastrophic edit training.

5.4 What is the Primary View Authority Score?

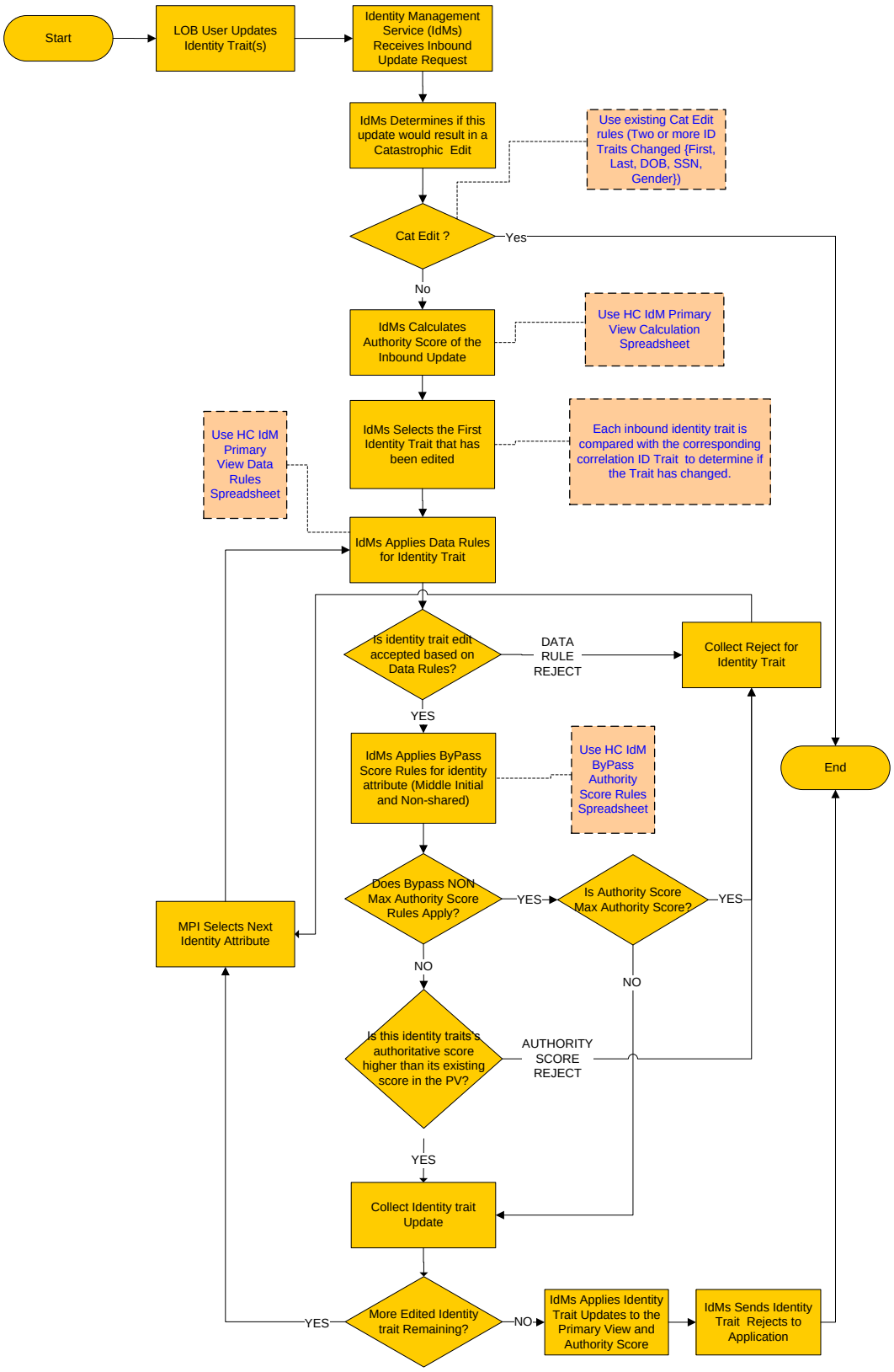
The concept of the Authority score is to ensure that the Primary View is updated with the most accurate, authoritative, and up to date data. Using data context and content, scores are calculated to determine whether or not updates should be applied to the Primary View.

- All fields in Primary View are compared to the inbound data sent for that correlation.
- If there are differences, a series of computations begin to "score" the data to determine if it meets the criteria for acceptance. The Primary View score is currently based on data captured from a patient encounter with a Veterans Affairs facility (e.g., active prescriptions, admission or registration in the last year, lab test, or radiology exam in the last year).

- The score is then calculated from the data update coming from the site.
- Each field is then evaluated against any fields that are different in the current Primary View to see if the score is equal to or greater than the existing Primary View field's score and that the data update meets the business rules for data validity and integrity.
- Any of the fields, all of the fields, or none of the fields may be updated based upon the scoring and the business rules.

Primary View Authority Score rules are maintained by the Data Quality Business Product Management group.

Primary View Update Process
7/13/2010



6 Requirements for Enterprise Person Search

This section describes the requirements applications using the Identity Management Service need to follow in order to perform enterprise person searches. This section will describe the information required to perform searches both at the local and enterprise levels, the order in which that information needs to be entered, the characteristics of the patient data, and requirements for attended and unattended searches. It is required to perform an enterprise search to ensure a person does not have an existing record in MVI before adding a new person record.

6.1 Search vs. Retrieve

If an application is using a unique identifier, such as the ICN, EDI-PI, or local source id, that identifier can be used to directly retrieve a person record. If no such identifier is available, a trait-based search will need to be performed.

6.2 Types of Searches

The VA has used Deterministic matching in the past, but the current direction is to use a Probabilistic matching algorithm.

6.2.1 Probabilistic

The VA has upgraded to an Enterprise Probabilistic matching algorithm from the former Deterministic (exact) matching. The change in matching algorithms was made because the probabilistic method allows for a greater chance of getting a correct match. For example, if a search supplies a first name of "Joe" instead of "Joseph," the match might return both records, as both are probable matches. In Deterministic matching, only the "Joe" record would return (missing a possible "Joseph" match) as the values in a deterministic search must match exactly to what is in an existing record, or no match will be found. Probabilistic matching has a greater possibility of detecting potential matches and therefore helping prevent potential duplicate records being added to the system for a person who already exists.

Probabilistic searching is used for enterprise person searches for both attended and unattended.

When searching using the probabilistic method, the following rules apply:

- The entire field value must be entered; for example, the whole first name as presented must be entered and not just the first initial.
- No wildcards (such as "*") are allowed in the search.
- Search criteria should be entered in the order listed in the grid below.
- A minimum of three traits must be supplied (last name and two others not including first and middle name). It is highly recommended to use as much data as is available (even if it is more than the minimum traits needed). Matching success is dependent on what traits are provided and any application developing search capabilities must collaborate with IdM business to ensure optimum results are achieved.

Note: Probabilistic searching is available in VistA with the Enterprise Person Lookup. See Appendix B for more information.

Table 1.
VA Identity Service Attended Search Sample Scenarios, Person - Probabilistic

29-Jan-13

	Person Id Traits / Criteria	Sample Scenario Number														
		1	**2**	**3**		**4**	**5**	**6**		**7**	**8**	**9**		**10**		**11**
1	Name															
a	First Name	X	X	X		X	X	X		X	X	X		X		X
b	Middle Name	X[1]	X[1]	X[1]		X[1]	X[1]	X[1]		X[1]	X[1]	X[1]		X[1]		X[1]
c	Last Name	R	R	R		R	R	R		R	R	R		R		R
2	Social Security Number (SSN)	X				X	X	X						X		
3	Date Of Birth (DOB)					X				X	X	X				X
4	Gender	X	X	X						X						
5	Home Address (Street, City, St. , Zip)		X				X				X					
6	Home Phone			X				X				X				
7	Place of Birth (POB)															X
a	City															
b	State															
8	Mother's Maiden Name (MMN)															X

Legend	
Results	Candidate Persons returned from search based on the search criteria supplied
R	Denotes required search criteria
X	Denotes required for optimized results
X[1]	Denotes recommended if available for optimized results
blank	Denotes optional search criteria
Maximum Results	Maximum number of results / None will be returned if more than 10 results

`

Table 2.
VA Identity Management Service
Match (unattended search) Sample Scenarios Person - Probabilistic
27-Mar-13

		Primary	Address in place of SSN		Use of POB, MMN	
	Person Id Traits / Criteria	**1**	**2**	**3**	**4**	**5**
1	Name					
a	First Name	X	X	X	X	X
b	Middle Name	X[1]	X[1]	X[1]	X[1]	X[1]
c	Last Name	R	R	R	R	R
2	Social Security Number (SSN)	X			X	
3	Date Of Birth (DOB)	X	X	X		X
4	Gender	X	X	X	X	X
5	Home Address (Street, City, St. , Zip)		X	X[1]		
6	Home Phone		X[1]	X		
7	Place of Birth (POB)					
a	City				X	X
b	State				X	X
8	Mother's Maiden Name (MMN)				X	X

Legend

Results	Candidate Persons returned from search based on the search criteria supplied
R	Denotes required search criteria
X	Denotes required for optimized results
X[1]	Denotes recommended if available for optimized results
blank	Denotes optional search criteria

Maximum Results

10	Maximum number of results / None will be returned if results are more then 10

6.2.2 Deterministic

In deterministic matching, either a unique system identifier is used in a search to find a match (VistA DFN_Station Number for instance) or an exact comparison is used between identity traits (Name, DOB, SSN for instance) in a search to find a match. System identifiers are very reliable in deterministic searching to find a match. However, deterministic searching using identity traits only produces a match when those identity traits match exactly. So, for example, a deterministic search for Pat Smith would not find Patrick Smith and other possible matches. Address is another trait likely to have small variations that would prevent a match when searching deterministically. Deterministic matching should only be used for a lookup when an exact unique system identifier is being used, not with identity traits. Any exceptions to this would need to be coordinated with IdM business to ensure searches are successful.

6.3 Search Methods

Enterprise person searches can be either attended or unattended searches.

6.3.1 Attended

An attended search is a manual search done by a user. In an attended search, there is direct user involvement from the point of view of the Identity Service. For an attended search, the Identity Service displays a maximum 10 results of potential matches from the probabilistic search algorithm. Table 1 above presents sample scenarios for achieving matches with various combinations of traits in an attended search.

6.3.2 Unattended

Unattended searches are automated searches done during application processing. In an unattended search, there is no direct user involvement from the point of view of the Identity Service. The probabilistic search algorithm applies the Match Threshold Tie Breaker rules to narrow the results down to one result for an unattended search. Unattended searches will return either one match or no match. Table 2 above presents sample scenarios for achieving matches with various combinations of traits in an unattended search.

Match threshold rules are maintained by the Data Quality Business Product Management group.

6.4 Enterprise Person Search Requirements

Applications that need to search for persons within the VA may require a search throughout all the records contained in the MVI. This is considered an enterprise search. When this type of search is needed, Identity Service recommends using as much identity data as is available to an application, and collecting it in the order presented in the grids in Tables 1 and 2 above. These grids present sample scenarios for achieving matches with various combinations of traits.
Note: For local searches, see section 7.

6.4.1 Search Order

Add search traits in the order shown in the grid in Table 1 above.

6.4.2 Identity Management Data Format

Application teams need to be aware of the characteristics of the identity trait data elements in order to ensure search strings are in the appropriate format. The following table lists each trait along with its data type and size.

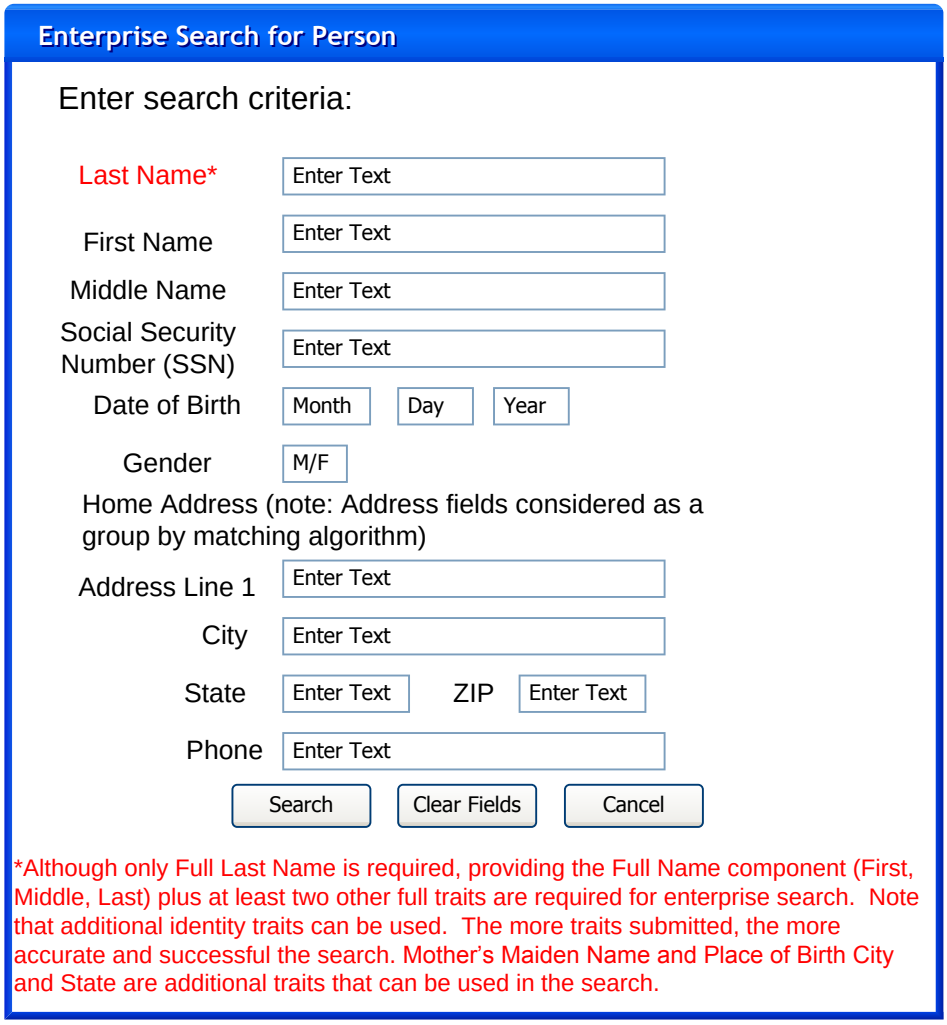
Trait Name	Data Type	Data Size	Comments
First Name	Varchar2	1 to 25	Wildcards not allowed for name components; may diminish quality of results
Middle Name	Varchar2	1 to 25	Providing Middle Name increases the success of the search but is not mandatory.
Last Name	Varchar2	1 to 35	
Date Of Birth (DOB)	Date		Imprecise dates allowed; however, may diminish quality of results
Social Security Number (SSN)	Varchar2	9	All nine digits required if used in search
Gender	Varchar2	1	M or F
Street Address (i.e. Address Line 1)	Varchar2	3 to 35	
City	Varchar2	3 to 28	
State	Varchar2	2	
ZIP Code	Varchar2	5 to 10	
Home Phone	Varchar2	4 to 23	

6.4.3 Can 1U4N Searches Be Used?

Veterans Health Administration (VHA) Office of Health Information Governance (HIG) has recommended to discontinue use of the One Upper Case Letter (first initial of the last name) and the Last Four Digits of the Social Security Number (1U4N) as an option for patient lookup in VHA electronic medical record systems, and this option is not supported under enterprise Probabilistic Searching. Use of this convention has been shown to result in selection of an incorrect patient entry, which in turn can lead to the erroneous addition of information to that wrong patient entry. Due to the fact that searching at the enterprise level involves an extremely large data store, 1U4N is not a reliable search trait on its own and presents a high risk of the wrong patient being selected. This has a direct impact on patient safety; therefore HIG's recommendation is to discontinue these specific lookup conventions from all applications in use across the Department of Veterans Affairs (VA) and to require lookup with more robust identity traits, such as full SSN or full name.

6.4.4 Sample User Interface

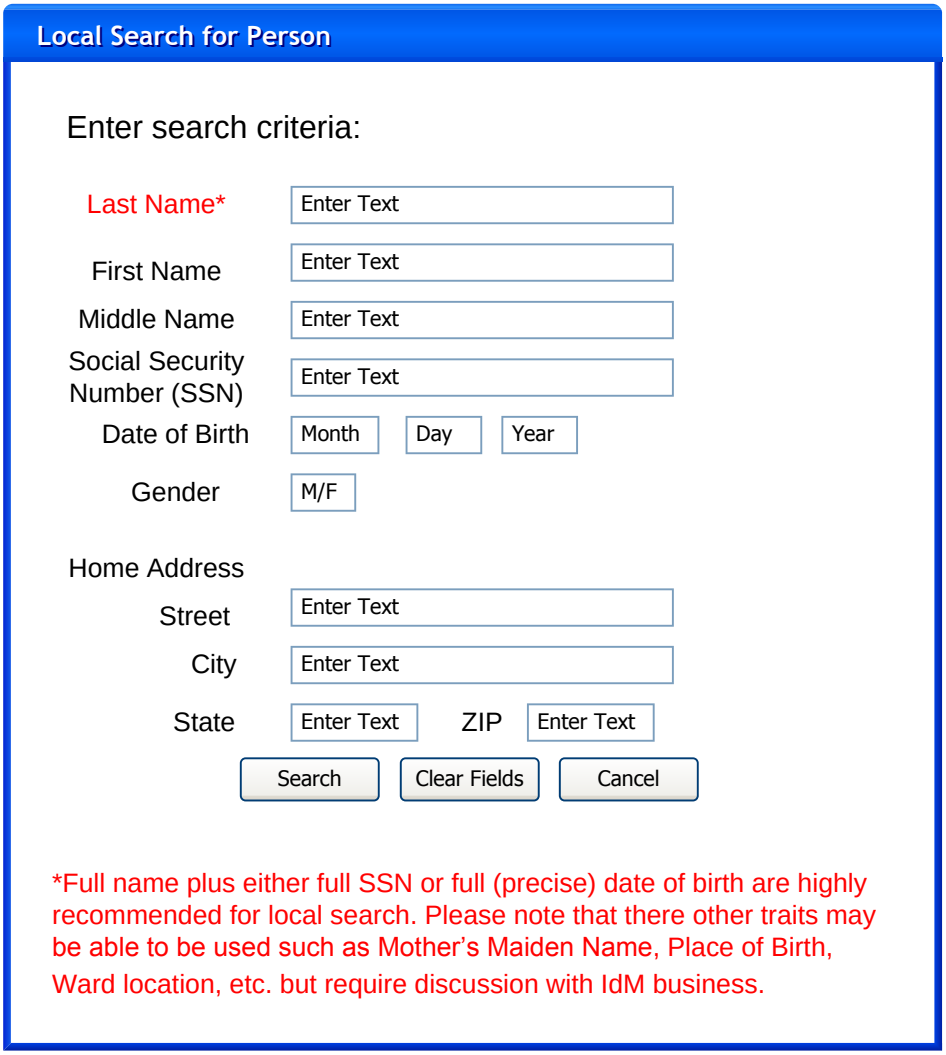
The following is a suggested design for an Enterprise Person Search screen.



7 Local Person Search Guidance

Applications that need to search for persons within the VA may require a search throughout all the records contained in the MVI. This is considered an *enterprise* search. However, some applications only need to search within just one VistA system; this is considered a *local* search. In local searches, it is allowable to use fewer search traits, because in general the search is enacted on a smaller population. However it is still important to ensure that applications find the correct person record with little user intervention and risk for error. The local search guidance is intended to expedite the search for a patient but without compromising patient safety issues that are associated with selecting an incorrect record.

An ideal local search would include a full name (First, Middle, Last) plus either a full Social Security Number (SSN) and a complete Date of Birth. Note that other identity traits can be used (see Table 1). When more traits are submitted, the returned results will be more accurate. The minimal local search criteria includes a full Last Name and either a complete SSN or a complete Date of Birth. Note that submitting the full Last Name and the complete Date of Birth may increase the number of potential twin records returned in the results. A partial SSN (i.e., last 4 digits) or imprecise Date of Birth should never be accepted in any search.



7.1 Search Standard Background

The Joint Commission (TJC), formerly the Joint Commission on Accreditation of Healthcare Organizations (JCAHO), accredits over 19,000 health care organizations and programs in the United States and maintains a number of standards regarding patient care. The local search recommendations in this document are based on the TJC's National Patient Safety Goal 1: Two Patient Identifiers, for use in hospitals:

> The purpose of this requirement is to reliably identify the individual's record as the target record who may require service or treatment from the VA medical center. Second, is to match a service or treatment to the individual. The requirement of searching using two full identifiers may also help prevent common "wrong patient" errors such as the recording of orders in the wrong patient's record. In most cases, the error is recognized by another caregiver; however, there are a significant number of such cases in which the error is not recognized and the patient receives an inappropriate treatment. Similarly, "wrong patient orders" can be an unintended consequence of using some CPOE systems that do not provide adequate safeguards to include at least two

identifiers to assure correct patient identification before accepting orders.[1]

8 Requirements for Displaying Identity Data

The purpose of this section is to provide requirements for displaying identity data in applications that use the Identity Management Service.

8.1 Displaying Search Results

Currently, for an Attended Enterprise search, IdM Service will return a maximum of 10 possible patient records that match based on the criteria submitted to the Enterprise Probabilistic algorithm. It is crucial that applications return and display the patient records in a way that will allow the End User to distinguish the correct patient record from the other possible matches. It is recommended that the application's default search display returns the potential matches in match threshold score order from highest to lowest. This order will provide the user with the best possible matches at the top of the list. The following guidance is to provide a standard, consistent format for applications to display the patient identity information after submitting a search for a patient. By following this guidance, application teams ensure the End User will have the necessary information to select the most accurate record (avoiding Patient Safety and other Identity Management issues).

The following identity trait elements will be returned with the result set of possible matches:

- Full Name
- SSN
- DOB
- Gender
- Home Address (Note that Home Address and Phone Number are currently not included in the Probabilistic Result set, but retrieving this information from the Authoritative source is a future requirement.)
- Phone Number
- Mother's Maiden Name
- Place of Birth City

Note that any other ancillary information that applications use in their business process that may help identify the correct patient record can also be included.

The threshold scores (i.e. match scores) returned with the search results should not be displayed.

The following is an example of how the result set might be displayed in a consuming application.

Full Name	SSN	Date of Birth	Gender	Street Address	City	State	Zip	Telephone
Jones, Joseph Lyle	XXX-XX-XXXX	3/11/1952	M	100 Ash Street	Newton	CA	55555	333-333-3333
Jones, Joey Lyle	XXX-XX-XXXX	3/11/1951	M	500 Oak Street	Newton	CA	55555	333-444-3333
Jones, Joe L	XXX-XX-XXXX	3/10/1952	M	100 Oak Street	Newton	CA	55555	333-444-4444

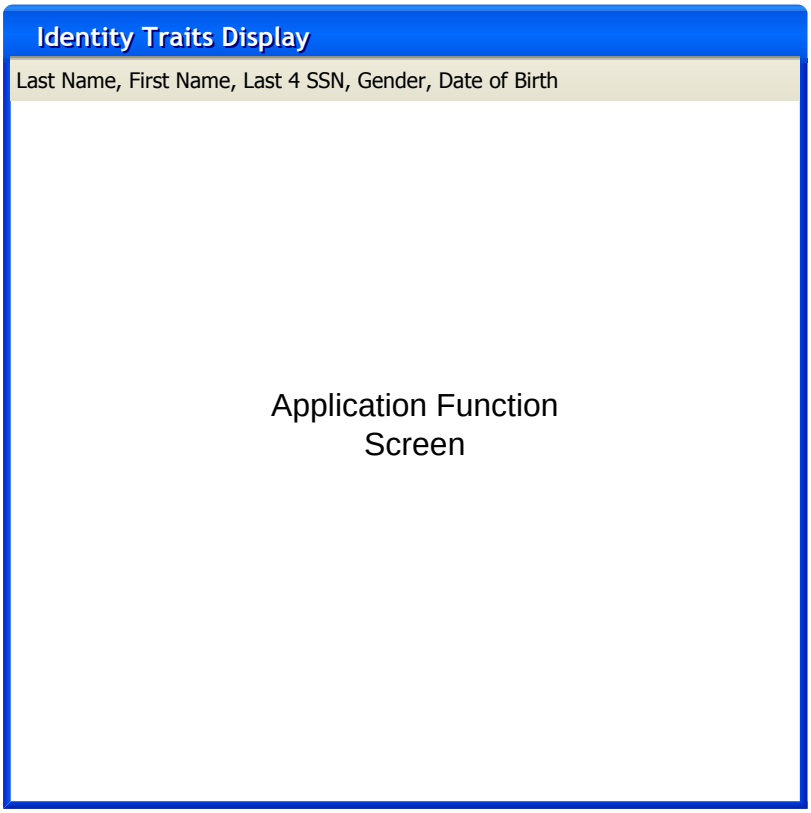
[1] Ross Koppel, PhD; Joshua P. Metlay, MD, PhD; Abigail Cohen, PhD; Brian Abaluck, BS; A. Russell Localio, JD, MPH, MS; Stephen E. Kimmel, MD, MSCE; Brian L. Strom, MD, MPH. Role of Computerized Physician Order Entry Systems in Facilitating Medication Errors. JAMA. 2005;293:1197-1203.

8.2 Displaying Identity Traits on Application Pages

Upon selection of the correct patient record, identifying information should be displayed consistently so that the End User has clear knowledge of which patient record he/she is accessing throughout the system. The following guidance is to provide a standard, consistent format for applications to display patient identity information throughout their application screens. This includes local, central and hybrid patterns as described in the References documentation, Section1.5. By following this guidance it will support the integrity of the patient record and will help prevent information from entering into an incorrect patient record (avoiding Patient Safety and other Identity Management issues).

The following patient elements are suggested to display throughout applications:

- Full Name
- Gender
- DOB
- Partial SSN (for security purposes in display)



Appendix A: Enterprise Requirements Roadmap

Please note that this list of requirements was downloaded from the Repository in June 2010; application teams should check the database as described in Section 3.1.1 for additional or changed requirements. Note that this use case column is "under construction" as use cases are continuing to be revised. Please see the link below for complete information on Identity Services use cases.
http://tspr.vista.med.va.gov/warboard/anotebk.asp?proj=1385&Type=Active

RM ID	Description	Checklist	Related Project Use Case
ENTR890	Applications/Services shall process update notifications to person identity traits received from the authoritative source for Identity Management.	❑ Patient Identity data updates from systems of record are sent and communicated to all systems of interest (patient Identity information updates to traits from MVI) (e.g., test with Updates and Overrides).	Enterprise Update Person
ENTR925	Person related applications/services shall be capable of processing a fully qualified Enterprise Person Identifier.	❑ Applications and services must be able to handle the full ICN, Checksum, Encryption key number without truncating (29 characters).	Enterprise Update Person
ENTR927	Applications/services that persist person related data shall register persons of interest with the authoritative source for Identity Management.	❑ For any new "Add" of a new patient record, ensure an ICN is assigned. Ensure the MPI has the correlation reference. ❑ Ensure the application/service receives and stores the ICN.	Enterprise Link Person
ENTR929	Applications/services that persist persons of interest-related data shall process person identity Link (Resolve Duplicate) notifications received from the authoritative source of Identity Management.	❑ Are patient record link requests from the IdM authoritative source sent and processed at the system of interest, see the 3 scenarios. ❑ Scenario 1) Perform a Link request when the system of interest is on	Enterprise Link Person

RM ID	Description	Checklist	Related Project Use Case
		the Surviving ICN. ❑ Scenario 2) Perform a Link request when the system of interest is on the Deprecated ICN. ❑ Scenario 3) Perform a Link request when the system of interest is on both the Surviving and Deprecated ICN. This turns into a local merge scenario. ❑ For all scenarios, ensure Enterprise, VistA, Hybrid and Downstream Systems (correlated to the secondary, HDR) are notified and communication is sent in the appropriate direction. •	
ENTR1097	Person related applications/services shall use Identity Management services as the authoritative source for maintaining person identities.	❑ Systems of interest should attempt to make updates to Patient Traits, ensure Enterprise IdM Business rules are enforced.	All
ENTR1098	Person related applications/services shall use Identity Management services as the authoritative source for creating Enterprise Person Identities.	❑ Are new person records added via the appropriate method in order to receive a Source ID and to correlate to the correct Enterprise Unique Identifier (e.g., test with add). ❑ Are existing/enumerated person records added via the appropriate method in order to receive a Source ID and to correlate to the correct Enterprise Unique Identifier.	Enterprise Add Person

RM ID	Description	Checklist	Related Project Use Case
ENTR937	Applications/services that consume person based transactions/messages from a source/input system that is correlated to an Enterprise Person Identifier shall persist the Source Identifier from the originating system along with the person data		Enterprise Update Person
ENTR930	Applications/services that persist persons of interest-related data shall support person identity Move Correlation (Resolve Mismatch) notifications received from the authoritative source of Identity Management.		Enterprise Move Correlation Person
ENTR941	Applications/services that consume person based transactions/messages from a source/input system that is correlated to an Enterprise Person Identifier shall include the Source Identifier within all messages containing person related data that are sent to other VA systems.		

Appendix B: VistA Enterprise Person Lookup

This appendix describes the VistA Enterprise Lookup, a tool used to interact with the VistA system in order to determine if a patient is known to VHA. The user begins by selecting the VistA option to search the VHA enterprise for a patient. The system prompts the user for a set of identity traits. The user supplies the identity traits and submits the search to the system. The system returns the results to the user. The system returns multiple results based on the success of the search. If no matching patients are found the system indicates such. If only "exact" matches are found then only a single list of "MEET THE MATCH CRITERIA" matches are returned. If only "MEET THE POTENTIAL MATCH CRITERIA" matches are found then only a single list of "MEET THE POTENTIAL MATCH CRITERIA" matches are returned. However, if both "MEET THE MATCH CRITERIA" and "MEET THE POTENTIAL MATCH CRITERIA" matches are found then the "MEET THE MATCH CRITERIA" matches are returned first followed by the "MEET THE POTENTIAL MATCH CRITERIA" matches. Both lists are in Match Score order. The user can select to see the details for any match returned by selecting that match number, a list of numbers or ALL.

Input Search Criteria

The following Identity Trait criteria are used to perform the search.

```
Enter Last Name (Required):
Enter First Name:
Enter Middle Name:
Enter DOB (Required-accepts imprecise dates.):
Enter SSN:
Enter Gender:
Phone Number:
Address Line 1:
Address Line 2:
Address Line 3:
City:
```

Search Output

For any search, a maximum of 10 rows will be returned.

If the search engine finds more than 10, no results will be returned, and an error message will be sent indicating that more identity traits are required to make a match".

The output from the search lists the identity traits from the MPI primary view.