DATA QUALITY REQUIREMENTS FOR HEALTHCARE IDENTITY MANAGEMENT AND MASTER VETERAN INDEX FUNCTIONS

1. REASON FOR ISSUE. This Veterans Health Administration (VHA) Directive establishes the business authority for the Healthcare Identity Management (HC IdM) Program and defines HC IdM enterprise and business requirements throughout the information systems lifecycle, including: the Master Veteran Index (MVI) and HC IdM operations at Department of Veterans Affairs (VA) health care facilities.

2. SUMMARY OF MAJOR CHANGES. This VHA Directive:

a. Changes the system title from Master Patient Index (MPI) to MVI and reflects establishment of MVI as an enterprise system.

b. Updates references to reflect involvement in activities such as the Nationwide Health Information Network and current versions of software systems and applications.

c. Updates guidance on entry and maintenance of data related to gender consistent with direction provided by Patient Care Services (see Att. A par.4).

3. RELATED ISSUES. VHA Handbook 1907.05.

4. RESPONSIBLE OFFICE. The Office of Informatics and Analytics (10P2) is responsible for the contents of this Handbook. Questions may be addressed at 202-554-3497.

5. RECISSIONS. VHA Directive 2006-036, Data Quality Requirements For Identity Management And Master Patient Index Functions, dated June 1, 2006, is rescinded.

6. RECERTIFICATION. This VHA Directive is scheduled for recertification on or before the last working day of May 2018.

Robert A. Petzel, M.D.
Under Secretary for Health

DISTRIBUTION: E-mailed to the VHA Publications Distribution List 4/30/2013

DATA QUALITY REQUIREMENTS FOR HEALTHCARE IDENTITY MANAGEMENT AND MASTER VETERAN INDEX FUNCTIONS

1. PURPOSE: This Veterans Health Administration (VHA) Directive establishes the business authority for the Healthcare Identity Management (HC IdM) Program and defines HC IdM enterprise and business requirements throughout the information systems lifecycle, including: the Master Veteran Index (MVI) and HC IdM operations at Department of Veterans Affairs (VA) health care facilities. The MVI is the authoritative identity service within VA maintaining and synchronizing identities for VA clients, Veterans, and beneficiaries (see subpar. 5g).
AUTHORITY: Title 38 United States Code (U.S.C.) 7301(b).

2. BACKGROUND

a. In fiscal year (FY) 2000, VHA established a HC IdM Program, now within the Office of Informatics and Analytics, Health Information Governance, Data Quality Program, as the national business owner and data steward for MVI and the services and activities needed to maintain and ensure the integrity of a patient or beneficiary's longitudinal health record and unique person identity for health care. The MVI and the activities performed by HC IdM are based on national standards (e.g., American Society for Testing and Materials (ASTM)) and link all records about one patient in multiple VHA, VA, Department of Defense (DOD) and other external systems to provide that patient/beneficiary's complete electronic health record (see subpars. 5h and 5i). This ability is essential to seamless care coordination and data sharing and interoperability with health care partners such as DOD and the Nationwide Health Information Network (NwHIN) and with VA lines of business such as the Veterans Benefits Administration (VBA). HC IdM information and functionality resident in the MVI are on the critical path for all patient, Veteran, and beneficiary-centered clinical and administrative information technology (IT) applications.

b. The MVI contains an entry and unique identifier for all patients who have had an active record in any Veterans Health Information Systems and Technology Architecture (VistA) PATIENT file (#2) since 1996. Today the MVI provides the capability to link a patient's records through matching of traits such as name, social security number (SSN), date of birth (DOB), gender, address, etc., from multiple VA health care facilities' national databases and other VA systems that support health care, such as MyHealth***e***Vet (MHV). In FY 2013-2014, VA is expanding this capability to all of VA's systems legacy and new systems as part of the Veterans Relationship Management (VRM) Major Initiative supported by a mandate from the Assistant Secretary of the Office of Information Technology (OIT).

c. Current HC IdM Program activities include: establishing business policy and rules; overseeing core identity management product implementation; and monitoring, identifying, and resolving record and identity integrity issues and conflicts in the MVI, VA systems such as MHV and local VA health care facilities related to identity data. This includes the resolution of duplicate records, mismatches, and overwrites (catastrophic edits) of patient identity that affect patient care and safety. In FY 2013-2014, the program activities are expanding to other VA lines of business which include the implementation, monitoring, identification and resolution of identity integrity issues and conflicts on the MVI with line-of-business systems.

d. Clinical, administrative, billing, and intra-departmental processes within VA, such as eligibility data sharing between VBA and VHA and with external partners, depend on accurate patient health care information and identity management and have implications to patient safety and the provision of health care. In order to ensure that individuals are correctly identified by VA staff during patient selection and entry and to prevent catastrophic edits to identity, extreme care must be exercised when entering and editing identity information. The HC IdM Program supports field efforts relating to the data entry into the patient health record with a team of highly-skilled specialists who understand VHA's health care records and can guide the resolution of duplicate entries, overlaps, overwrites, and other mis-identification of patient identity data that could impact patient care and safety.

e. HC IdM is dependent on the correct identification of unique individuals, but it is distinct from Security, and Identity and Access Management (IAM), which involves managing persons seeking access to VA resources based on national security standards (Homeland Security Presidential Directive 12 (HSPD12), Federal Information Security Management Act (FISMA), National Institute of Standards and Technology (NIST), etc. (e.g., authentication, authorization, and access control).

f. **Definitions**

(1) **Catastrophic Edit.** A Catastrophic Edit means changes have been made to a patient's electronic health record in a local VistA system that result in the record being changed inappropriately to that of another patient, caused by, but not limited to, edits to patient identity data (such as name, SSN, date of birth, gender) and/or erroneous merging of two or more distinct patient records into a single record within VistA.

(a) These errors can occur as a result of improper due diligence by staff using the Duplicate Record Merge software when two potential duplicate patient records are not properly reviewed and screened. This results in two different patient entries being merged into one.

(b) All types of errors affect the longitudinal patient entry (record) at other facilities that have treated the patient and they specifically affect patient care. These errors are considered a significant patient safety risk.

(2) **Enumeration.** Enumeration is an assignment of a universal health identifier by the authoritative identity management service to an individual. For VA, this service is provided by the MVI and the identifier is known as the Integration Control Number (ICN) (see subpar. 2f(4)).

(3) **Healthcare Identity Management (HC IdM).** HC IdM is comprised of the set of business processes and a supporting infrastructure for the creation, maintenance, and use of digital identities within a legal and policy context.

(a) The HC IdM Program is the national business owner or steward for patient identity data within VHA.

(b) The HC IdM Team ensures the integrity of patient identity data within the MVI and the associations to the systems that contain electronic health record information about the patient, which provides the longitudinal health record.

(4) **Integration Control Number (ICN).** ICN is VA's enterprise unique person identifier which is based on the conformance standard from ASTM E 1714-00, assigned and maintained by the MVI to each unique patient within the VHA systems and provides the key to linking the patient electronic health record across the enterprise.

(5) **Master Veteran Index (MVI).** MVI is the authoritative identity service within VA, establishing, maintaining and synchronizing identities for VA clients, Veterans and beneficiaries. The MVI correlates a patient's identity across the enterprise, including all VistA systems and external systems, such as DOD, and the NwHIN. Legacy systems from other VA administrations, e.g., National Cemetery Administration's (NCA) Burial Operations Support System (BOSS) and Automated Memorial Application System (AMAS) and VBA's Corporate Database are being integrated with the MVI. The MVI includes authoritative sources for health identity data and contains over 18 million patient entries populated from all VHA facilities nationwide. The MVI facilitates the sharing of health information, resulting in coordinated and integrated health care for Veterans by providing the access point mechanism for linking patient's information to enable an enterprise-wide view of patient information; it uniquely identifies all active patients who have been admitted, treated, or registered in any VHA facility, and assigns a unique identifier to the patient.

(6) **Primary View**. A Primary View is the VA enterprise profile of an identity indicated by an ICN. An identity is represented by one ICN, and each ICN has one Primary View Profile. The Primary View Profile provides the most authoritative identity traits known about a person's identity within VA. The Primary View Profile is referenced in VA information systems by an associated ICN.

3. POLICY: It is VHA policy that information systems and databases, including the MVI, maintain accurate and complete person-identifying information, and that vital processes related to resolving identity data quality issues be performed.

4. RESPONSIBILITIES

a. **Chief, Office of Informatics and Analytics, Health Information Governance, Data Quality, HC IdM Program, VHA Central Office.** The Chief, Office of Informatics and Analytics, Health Information Governance, Data Quality, HC IdM Program, VHA Central Office is responsible for:

(1) Serving as the business owner and data steward to ensure that the correct patient or beneficiary longitudinal, electronic health record is available.

(2) Managing the integrity of health care identities required to provide health care services, treatment and health care operations.

(3) Serving as the business function owner and steward for HC IdM systems such as the MVI and other related HC IdM efforts and/or other applications that require Identity Management (IdM) functionality.

(4) Providing the authoritative business input about and monitoring compliance with HC IdM functions, requirements and policy on behalf of VA to ensure that HC IdM business requirements are provided, understood and addressed within VA information technical efforts throughout product lifecycles.

(5) Promoting HC IdM best practices and developing and disseminating information and training to improve the understanding of HC IdM and related systems.

(6) Resolving patient and other non-patient (e.g., provider) identity issues (e.g., duplicates, mismatches, patient catastrophic edits), working with local facility staff to maintain the integrity of the longitudinal record and ensure that policies and procedures are followed.

(7) Participating in the development of national HC IdM standards.

(8) Ensuring VA information systems adhere to health care identity management requirements as documented in the Identity Management Business Requirements Guidance located on the Data Quality (DQ) homepage: http://vaww.vhadataquality.va.gov . ***NOTE:*** *This is an internal VA Web site and is not available to the public.*

b. **Facility Director.** Each Facility Director is responsible for:

(1) Ensuring that the entry of person identity data into VA applications is accurate and complete.

(2) Ensuring that local duplicate patient records are reviewed and merged in VistA using the Duplicate Record Merge software in an accurate and timely manner.

(3) Designating individuals as points-of-contact (POCs) responsible for processing MVI and Patient Demographic (PD) Exceptions, resolving ICN issues on a daily basis, as well as merging local duplicate patient records and resolving any other data quality issues brought to their attention by the national HC IdM Program staff.

(4) Ensuring that personnel are assigned to resolve, in a timely manner, issues with exceptions, data quality, communication links, infrastructure, and applications that support data communications. This includes assigning staff members to the following roles (including alternates for each of these categories):

(a) Administrative POC, and a Health Information Management (HIM) staff member;

(b) OIT POC; and

(c) Health Level 7 (HL7) POC.

NOTE: *POC information for Master Veteran Index/Patient Demographics (MVI/PD) is updated using the Add/Edit Point-of-Contact [RG UPDATE POINT OF CONTACT] option on the MPI/PD Patient Admin Coordinator Menu [RG ADMIN COORD MENU]. A current listing of facility MVI POCs can be found on the Data Quality Web site: http://vaww.vhadataquality.va.gov/index.php?option=com_joodb&view=catalog&Itemid=240&lang=en. This is an internal VA Web site and is not available to the public.*

(5) Ensuring that national HC IdM staff are apprised of staffing changes.

(6) Ensuring that management and staff are made aware of policies and procedures related to catastrophic edits to patient identity. This includes ensuring that all staff members with the ability to enter, edit, and merge patient identity data (such as name, date of birth, SSN and gender) specifically, those individuals who have been given the privilege of being assigned the VistA "DG REGISTER PATIENT," "DG LOAD EDIT" key or a local equivalent, are required to complete and document the required training module "Preventing Catastrophic Edits to Patient Identity." ***NOTE:*** *The required training,"Preventing Catastrophic Edits to Patient Identity," can be found at VA Learning University Talent Management System (TMS) under Item Number: VA 7861, www.tms.va.gov*. This training is required prior to the assignment of the key to these individuals.

(7) Ensuring that the appropriate supervisors are responsible for ensuring this training is successfully completed and documented by the employee, as this is a key competency for patient selection. Any individual who does not demonstrate competency of this skill must re-take the training until core competency is established. Any individual who mis-selects a patient record and generates a catastrophic edit to a patient record must re-take the training and provide evidence of successful completion to the individual's supervisor and the HC IdM Team.

(8) Ensuring that supervisors monitor employee work quality and ensure that employees achieve and maintain core competency of this skill; failure to achieve competency can lead to patient safety issues.

(9) Ensuring the VistA DG CATASTROPHIC EDIT security key is assigned to the responsible Chief Business Office (CBO) Program Application Specialist (PAS) or Automated Data Processing Application Coordinator (ADPAC), their alternates, and supervisor, so they are recipients of the "Potential Catastrophic Edit of Patient Identifying Data" alerts. Designated staff reviews these alerts on a daily basis to ensure that catastrophic edits are reported and resolved and that any issues with staff performing catastrophic edits are addressed.

(10) Ensuring the VistA DG SUPERVISOR security key is assigned and a daily review of the Report – Patient Catastrophic Edits option is conducted and all potential catastrophic edits listed on the report have been reviewed, and resolved in a timely and accurate manner (see VHA Handbook 1907.05 for detailed procedures and timelines in correcting health and demographic information within the electronic health record and other electronic databases when health or administrative data are erroneously associated with a patient as a result of a catastrophic edit to patient identity).

(11) Ensuring that all facility staff involved in the editing or alteration of the electronic health record exercise care and caution when making changes to identity traits of patients and report any suspected catastrophic edits to the designated facility MVI POC.

(12) Ensuring that staff directly involved with identity data entry into information systems are aware of the guidelines contained within this Directive and are aware of their responsibility for entering complete identity data elements in a consistent and accurate format. This also includes staff at facilities with outpatient clinics and community-based outpatient clinics assigned to their jurisdiction.

(13) Ensuring that each supervisor involved in the activities of entering demographic data follows the guidance on data quality of the non-identity elements provided by the VHA CBO.

(14) Ensuring that staff members responsible for data entry of administrative and demographic information are informed of these requirements mandated by the CBO. ***NOTE:*** *Links to up-to-date guidance on data quality are posted on the HC IdM team's Web site*: *https://www.tms.va.gov/learning/user/login.jsp,*

(15) Ensuring that the audit trail of the PATIENT File (#2) for all electronic health records is maintained and never purged as this is critical in the identification and resolution of catastrophic edits to patient identity and other identity integrity issues.

c. **Facility MVI POC.** Each facility MVI POC, who is considered to be the liaison between the facility and HC IdM, is responsible for:

(1) Working with their counterparts and national HC IdM staff in correcting anomalies and addressing issues related to identity data for shared patients.

(2) Processing MVI-PD Exceptions, data quality and other ICN issues in VistA and merging local duplicate patient records, to ensure accuracy and completeness of identity data.

(3) Taking appropriate action to resolve exceptions, data quality and other ICN issues in VistA, and merge local duplicate patient records within 5 business days. ***NOTE:*** *Specific information regarding these processes can be found in Attachment A of this Directive.*

(4) Responding to requests from HC IdM staff to resolve catastrophic edits that overwrite the original patient entry with another patient. These must be completed within 1 business day.

(5) Using electronic mail (i.e., Outlook) to facilitate communications.

(6) Obtaining and maintaining Public Key Infrastructure (PKI) encryption certificates that must be utilized when transmitting and receiving patient identifiable information.

(7) Ensuring that facility contact information maintained by the HC IdM team is current.

(8) Obtaining the necessary VistA access to verify information.

(9) Making appropriate changes to patient data in the respective facility's VistA system and perform POC functions, such as processing MVI-PD Exception Handling, data quality, and ICN issues.

d. **Facility OIT and HL7 POCs.** Facility OIT and HL7 POCs are responsible for:

(1)Working with their counterparts and OIT Product Development (PD) Product Support (PS) staff to maintain communication links, infrastructure, and applications supporting data communications. Responses to inquiries and requests for assistance must be addressed within 1 business day;

(2) Ensuring that the audit trail of the PATIENT File(#2) for all electronic health records is maintained and never purged as this is critical in the identification and resolution of catastrophic edits to patient identity and other identity integrity issues; and

(3) Facilitating the resolution of any catastrophic edits to patient identity, which must be completed within the timelines designated in VHA Handbook 1907.05, Repair of Catastrophic Edits to Patient Identity.

5. REFERENCES

a. VHA Handbook 1601A.02, Eligibility Determination.

b. VHA Handbook 1601A.01, Intake Registration.

c. VALU TMS Item Number 7861 Preventing Catastrophic Edits to Patient Identity.

d. VHA Handbook 1907.05, Repair of Catastrophic Edits to Patient Identity.

e. VHA Handbook 1605.1, Privacy and Release of Information.

f. Identity Management Business Requirements Guidance, Version 2.5, October 2012 http://vaww.vhadataquality.va.gov/index.php?option=com_phocadownload&view=file&id=123:identity-management-business-requirements-guidance&Itemid=153&lang=en. ***NOTE:*** *This is an internal VA Web site and is not available to the public.*

g. VA Identity Management Policy Memorandum.

h. ASTM. Standard Guide for the Properties of a Universal Healthcare Identifier. E1714-00; E31 reference: http://www.astm.org.

i. Object Management Group (OMG) Person Identification Service (PIDS) Specification Version 1.1, April 2001, http://www.omg.org/spec/PIDS/1.1/PDF.

PROCEDURES FOR DATA ENTRY AND MAINTENANCE RELATED TO HEALTH CARE IDENTITY MANAGEMENT

It is imperative that staff take the utmost care when entering identity data for patients and other persons. Incomplete or inaccurate data (including typographical errors) are the leading cause of duplicate entries in the Master Veteran Index (MVI) and the failure to link records via the Integration Control Number (ICN). The following guidelines are intended to increase the accuracy and completeness of the essential identity data traits and to clarify practices that need to be followed when data are not available or duplicate entries exist. These guidelines emphasize the intended use of some identity fields within Veterans Health Information Systems and Technology Architecture (VistA). It is important that identity data for patients be reviewed for accuracy and completeness and updated, as necessary, each and every time contact is made with the individual.

1. NAME: The NAME field is an important element in the unique identity of a person. Sites need to ensure that the name entered is the complete legal name, and includes a full middle name, when available. Nicknames or ambiguous information are not to be used. Additional guidance for the entry of the name field includes the following procedures:

a. All data must be entered using uppercase letters.

b. No parenthesis may be used.

c. Commas, apostrophes, and hyphens are the only punctuation that may be used.

d. Enter full middle names. Do not use only an initial unless an initial is the person's given middle name. No punctuation will be used if the middle name is only an initial. The middle name will be left blank if one does not exist; NMI (no middle initial) or NMN (no middle name) will not be used.

e. Multiple last name components must be separated by spaces. Individuals with hyphenated names are to be entered with the hyphen included.

f. When entering a full name, it must contain a comma (i.e., LAST NAME, FIRST NAME). Individuals with a legal name as a single value must be entered with the name followed by a comma.

g. Suffixes must be used for junior (JR), senior (SR) and birth positions. Numeric birth position identifiers must be entered in Roman numeral values (i.e., I, II, III, etc.). Suffixes must be entered without punctuation.

h. If entering a Prefix, (such as MR, MRS, MS, and MISS), no punctuation must be used.

i. The Degree field may be used to denote the degree or profession (such as MD for Doctor of Medicine, PHD for Doctor of Philosophy, REV for Reverend), and must be entered without punctuation.

j. Legal Spanish names must be entered with the father's last name first, a hyphen and then the mother's maiden name all in the LAST NAME field.

k. Alias names must be entered in the ALIAS NAME field for any previously used names (including maiden names). An entry in this field is automatically cross-referenced and the record can be accessed using the alias name.

l. To enter another patient record with the same name as an existing person in the file on VistA, use quotes when entering the full name and a new entry will be created (i.e., "LASTNAME,FIRSTNAME MIDDLE").

m. TEST patient records must be designated by the last name being prefixed by ZZ (i.e. ZZLASTNAME, FIRSTNAME MIDDLE).

n. A legal name change requires a written request and supporting documentation from the Veteran. Requests to change static administrative data are considered to be a Privacy Act amendment requests and may be made only by the Veteran or by a personal representative of the Veteran as defined in Veterans Health Administration (VHA) Handbook 1605.1. Official supporting documentation for a name change are the following: letter from the Social Security Administration (SSA) stating that all required documentation has been received and they will be issuing the requestor a new SSA card, a State Driver's License (based on new regulations enforced by the Department of Transportation whereby a name will not be changed until SSA provides the preceding letter or the new SSA card), new SSA card reflecting the name change, an official name change court order, amended birth certificate or passport. Marriage licenses or certificates are no longer sufficient stand-alone documents for a name change, as not all who apply for a marriage license or marry actually change their name. The Privacy Officer must review all documentation supplied by the Veteran to ensure it meets the criteria and to transmit this information to the MVI POC.

2. SOCIAL SECURITY NUMBER (SSN): Enter the patient's official SSN issued by the SSA. No other value will be entered into this field. If a valid SSN is not known, then a "P" must be entered into the field for the calculation of a pseudo SSN. SSNs are not to be created and no other numbers may be entered in this field, including prison-issued numbers or Canadian SSNs. SSNs beginning with five leading zeros are considered TEST patients and are not be used for any other purpose.

3. MOTHER'S MAIDEN NAME: Enter the last name only of individual's mother at the time of her birth. Leave blank if unknown or not provided. Values such as "deceased," "unknown," and other inappropriate responses are not to be used.

4. GENDER (ADMINISTRATIVE)

a. Male or Female must be entered. In case of gender reassignment, a written request and supporting documentation are required from the Veteran and is considered to be a Privacy Act amendment request. One of the following is required as supporting documentation: legal documentation (i.e., amended birth certificate or court order), passport or a signed original statement on office letterhead, from a licensed physician. Sexual reassignment surgery is not a prerequisite for amendment of gender.

b. The licensed physician's statement must include all of the following information:

(1) Physician's full name.

(2) Medical license or certificate number.

(3) Issuing state of medical license/certificate.

(4) Drug Enforcement Administration (DEA) registration number assigned to the physician or comparable foreign designation, if applicable.

(5) Address and telephone number of the physician.

(6) Language stating that the physician has treated the patient or reviewed and evaluated the medical history of the applicant. Also, the physician has a doctor-patient relationship with the applicant which is evident in having one or more clinical encounters between doctor and patient.

(7) Language stating that the patient has had appropriate clinical treatment for gender transition to the new gender (specifying male or female).

(8) Language stating "I declare under penalty of perjury under the laws of the United States that the foregoing is true and correct."

5. DATE OF BIRTH (DOB): Day, Month, and Year of Birth must be entered, whenever available. Imprecise (month/year or year only) can be entered, but only if the full DOB is not available. If DOB is unknown 1/1/1910 must be entered.

6. PLACE OF BIRTH [CITY]: Enter the birth city only. For persons born outside of the United States, enter the city, province, or other designated area.

7. PLACE OF BIRTH [STATE]: Enter the birth state only. For persons born outside the United States, choose FOREIGN COUNTRY from the list of state options.

8. PLACE OF BIRTH [COUNTRY] (not yet available)**:** Enter the birth country only (future implementation in VistA). The default country must be the UNITED STATES.

9. MULTIPLE BIRTH INDICATOR (Patients only): Enter YES in the Multiple Birth Indicator field only if the patient is part of a multiple birth (i.e., is a twin, triplet, etc.). This field assists in the unique identification of patients who are part of a multiple birth and may have identity traits similar to other patient entries. Leave blank if unknown or not provided.

10. DATES OF DEATH: Death certificates are generally required to enter a Date of Death. Dates of Death must not be entered from newspaper obituaries, phone calls, or other unofficial sources. Information from these sources may be used as a mechanism to further research the death information. However, they must not be entered unless they have been verified by an official source. Medical facilities are required to use the following as authoritative sources in order of precedence:

a. VHA facility is an authoritative source for date of death if the person died in the VHA facility or while under VA auspices,

b. Death Certificate, and

c. National Cemetery Administration (NCA) is an authoritative source for the date of death if the Veteran has received NCA benefits.

11. MOTHER'S NAME and FATHER'S NAME: The patient's mother's and father's complete legal names need to be entered in the appropriate fields, when known. Values such as "deceased," "unknown," and other inappropriate responses in lieu of the name or in addition to the name are not to be used.

12. INCAPACITATED, UNIDENTIFIED, OR UNRESPONSIVE PATIENTS (for whatever reason): Records for incapacitated patients must be entered with a pseudo SSN, 1910 for the DOB, and name entered as UU-UNRESPONSIVE, PATIENT. Subsequent patient records must be entered as UU-UNRESPONSIVE, PATIENT A, UU-UNRESPONSIVE, PATIENT B, etc. Records must be completed with appropriate identity data trait fields once the patient has been identified.

13. TEST PATIENTS: It is essential that TEST patients who exist in local VistA production systems be designated with a SSN containing five leading zeros (i.e., 000001111) and the last name prefixed by ZZ (i.e., ZZTESTPATIENT, FIRSTNAME MIDDLE). Test entries not to be used for categories of persons outside of patients, or for patients that are other than those used exclusively for testing purposes. Any deviation must be approved by the Healthcare Identity Management (HC IdM) Program Manager.

14. RESEARCH PATIENTS: Research patients must have all valid information (i.e., legal name, real SSN, DOB, etc.) collected and entered.

15. SSN, DATE OF BIRTH, MOTHER'S MAIDEN NAME, PLACE OF BIRTH [CITY], PLACE OF BIRTH [STATE] and PLACE OF BIRTH [COUNTRY]: The SSN, DATE OF BIRTH, MOTHER'S MAIDEN NAME, PLACE OF BIRTH [CITY], PLACE OF BIRTH [STATE] and PLACE OF BIRTH [COUNTRY] identity trait fields are important and are to be collected for the unique identification of individuals, since these are fields that do not generally

change over time. If these fields are inaccurate or incomplete, it is difficult to ensure that duplicates are not being created and that the record is being linked to the correct ICN on the MVI.

16. PATIENT RECORDS INVOLVED IN MEDICAL IDENTITY THEFT: Records for a patient that is determined to be an "imposter," where staff are unable to obtain the true identity of a patient, need to be edited to reflect the NAME field of THEFT, IDENTITY A (where the trailing letter would be incremented for each subsequent entry that exists in the local VistA PATIENT File (#2)). The record needs to be edited to use a pseudo SSN and have the DOB recorded as 1910. Any facility staff suspecting for any reason, that a person may be fraudulently receiving VA health care benefits, must immediately notify their supervisor, the Chief of Health Information Management (HIM) and the Business Office Manager, or equivalent. These individuals are responsible for notifying the HC IdM Team, facility management staff, police, local Information Security Office, local Privacy Officer, appropriate Regional Counsel, and the Office of Inspector General (OIG). Edits to the patient record are not to be made until after the OIG investigation has been completed. Any electronic documentation that is determined not to belong to the real patient (if identified) must be retracted in the same manner that any document found to be erroneously attributed to a patient is removed.

17. ALIAS FIELDS: The ALIAS fields are only to be used to enter previously-used names and SSNs. Name changes due to marriage, divorce, etc., are to be entered into the ALIAS field.

18. MVI EXCEPTIONS IN VISTA: Exceptions processing must be performed on a daily basis to ensure that inconsistencies are addressed in a timely manner. Failure to resolve data quality issues may result in incorrect operation of the Remote Data View, VistA Web, and Inter-facility Consult functions for facility clinicians. When processing MVI exceptions in VistA, if potential enterprise duplicate records, data quality, or other ICN issues are identified, a request for assistance is to be sent by an e-mail message to the VHA HC IdM Team distribution group on Outlook. PKI encryption must be utilized when transmitting patient identifiable information. A request for national support can also be entered using the OIT national problem management system (Remedy©). When submitting requests for assistance using Remedy©, do not include the individual's identifying information (name, SSN, etc.). The specialist assigned to the request must obtain this information directly from the MVI Point of Contact (POC). ***NOTE:*** *Additional information regarding MVI VistA User and Exception Handling manuals can be found on the VistA Documentation Library at: http://www.va.gov/vdl/application.asp?appid=16.*

19. DUPLICATE PATIENT ENTRIES: Merging of local duplicate patient records in VistA is to be performed in an accurate manner and merge process initiated within 5 business days of identification. When more than one record exists for the same patient a treating clinician may not see a complete view of the care provided to a patient and make treatment decisions based on a fragmented record. All proposed merges must be reviewed and approved by the ancillary package experts and the Chief HIM, or equivalent. ***NOTE:*** *To merge the data from one record to the other, use the process outlined in the DUPLICATE RECORD MERGE: Patient Merge User Manual located on the VistA Documentation Library at: http://www.va.gov/vdl/.*

20. MULTIPLE BIRTHS: Extreme caution must be taken when merging duplicate records to ensure the records are for the same individual. Many identity fields for individuals of multiple birth (e.g., twins) will be the same or similar. Once patients are identified as part of a multiple birth, the Multiple Birth Indicator needs to be set to "Yes" on all applicable records. It is essential that appropriate clinical ancillary staff and Chief HIM or equivalent, review potential duplicate records, to verify whether or not they should be merged.

21. ADDITIONAL INFORMATION: Information regarding the HC IdM Program, along with a current staff listing and the VHA facility POC can be found on the HC IdM Web page on the Data Quality Web site at: *http://vaww.vhadataquality.va.gov*. ***NOTE:*** *This is an internal VA Web site and is not available to the public.*